TERRORISM

studies
analyses
prevention

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

Editorial team Damian Szlachter, PhD (editor-in-chief)
Agnieszka Dębska (editorial secretary, layout editor)

Translation Agencja Bezpieczeństwa Wewnętrznego

Cover design Aleksandra Bednarczyk

ISSN 2720-4383
e-ISSN 2720-6351

MEiN points: **20**

Articles published in the journal are peer-reviewed

Articles express the views of the authors

Declaration of the original version:
The printed version of the journal is the original version
The online version of the journal is available at www.abw.gov.pl/wyd/

The journal is available on the Jagiellonian University Scientific Journals Portal at: https://www.ejournals.eu/Terroryzm/

Articles for the journal should be submitted through the editorial panel available at: https://ojs.ejournals.eu/Terroryzm/about/submissions

Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia i Edukacji
im. gen. dyw. Stefana Roweckiego „Grota"
ul. Nadwiślańczykow 2, 05-462 Wiązowna, Poland

Contact
phone (+48) 22 58 58 671
e-mail: wydawnictwo@abw.gov.pl
www.abw.gov.pl/wyd/

Printed in September 2023.

Print
Biuro Logistyki Agencji Bezpieczeństwa Wewnętrznego
ul. Rakowiecka 2A, 00-993 Warszawa, Poland
phone (+48) 22 58 57 657

TABLE OF CONTENTS

AWARDED THESES

OTHER

Ladies and Gentlemen!

We are working hard to ensure that the journal "Terrorism - Studies, Analyses, Prevention" (T-SAP) meets the expectations of its audience - representatives of the entire counterterrorism community of the Republic of Poland and the community of researchers of the phenomenon of terrorism, as well as other people interested in one of the greatest security challenges of the countries of the European Union and NATO. Above all, we are committed to ensuring that the topics covered are significant and topical.

Artificial intelligence certainly is such a topic. In the ongoing public debate, much attention is paid primarily to the threats posed by its use. These indeed pose serious challenges. However, thanks to AI, we have also gained completely new opportunities to develop knowledge and implement solutions to improve various areas of life. Among other things, AI can help us take better and more effective care of security. In what ways? For example, as the authors of the articles point out, by using AI algorithms to increase the resilience of critical infrastructure to terrorist threats or to predict the victims of such attacks.

Nowadays we are also dealing with a rapidly growing market of virtual currencies. In this issue you can read about their use to finance criminal activities, including those of a terrorist nature. The authors of the text analyze this phenomenon from the side of legal regulation and the possibilities of counteracting it by law enforcement and law enforcement agencies.

The COVID-19 pandemic, which until recently we had to deal with, focused our attention on health issues. However,

the topic of food safety and agroterrorism using biological agents has rarely been addressed in the broader forum, and it is closely related to human health well-being. The author of one article analyzes the current challenges in the area of biosecurity and food security - compounded not only by the epidemiological situation, but also by the war taking place in Ukraine, which is among the world's top food producers.

The unstable geopolitical situation in the world increases the risk of acts of a terrorist nature also directed against diplomatic facilities. The author of an article on the architecture of the buildings of 22 embassies located in Warsaw, Berlin and Rome writes about how they are protected by zonal security.

Starting with this issue of T-SAP, we would like to offer you a new, additional formula. It will feature texts that are not strictly scientific. Our goal is to create conditions conducive to a substantive discussion on countering, combating and preventing terrorist threats also from the point of view of practitioners, taking into account their experiences and opinions. In this issue we publish an essay on the role of counterintelligence activities. Its author has devoted many years of service to the Polish anti-terrorist community. The next materials presented were compiled by EU terrorism experts. They described two important anti-terrorism initiatives run by the European Commission - the EU High Risk Security Network and the EU Protective Security Advisors. With a view to exchanging experiences at the international level, we interviewed an expert from the Stockholm police about ways to build resilience to terrorist attacks in Sweden. In this part of the issue, we also publish a commentary by an expert from the American George Washington University, one of the best-known researchers of terrorist threats, on the results of a survey on terrorism in Poland and the directions of its development, conducted by the ABW in 2022.

I have already written about the novelties. Now, traditionally, I would like to encourage you to read the 4th issue of T-SAP, including reviews of two interesting book items. At the same time, I hope that the content presented in

it will meet with interest and contribute to the development and improvement of the anti-terrorist system of the Republic of Poland at every level - operational, tactical and strategic.

Editor-in-Chief
Damian Szlachter, PhD

ARTICLES

https://doi.org/10.4467/27204383TER.23.029.18331

https://orcid.org/0000-0002-5288-0324
https://orcid.org/0000-0002-3907-2242
https://orcid.org/0000-0001-6390-1402

TOMASZ P. MICHALAK
MICHAŁ T. GODZISZEWSKI
ANDRZEJ NAGÓRKO

Protecting critical infrastructure with game theory, optimization techniques, and AI algorithms

Abstract

In light of recent geopolitical developments, Europe and Poland are acutely aware of the urgent importance of infrastructure security. Despite heightened interest and increased investments, our security resources remain severely limited, rendering continuous protection for every potential target unattainable. Consequently, the strategic allocation of security resources becomes an ongoing imperative. This paper presents a short introduction to the core principles behind advanced methods that facilitate automated decision-making in security resource allocation. These methods leverage artificial intelligence (AI), game theory, and optimization techniques, and have demonstrated their effectiveness through multiple real-life deployments in the USA. We also provide a concise overview of this exciting body of research and discuss the solutions and software developed by our team, "AI for Security" at the IDEAS NCBR research institute to protect critical infrastructure in Poland and in Europe.

Keywords:

optimization, security games, artificial intelligence, critical infrastructure

Introduction

Los Angeles International Airport (LAX) is one of the busiest and largest airports in the world, serving as a vital transportation hub for the city of Los Angeles and the surrounding region. In terms of the number of passengers, it is about four times larger than the Frederic Chopin Airport, Warsaw, which is the biggest Polish airport. The LAX airport encompasses a vast area and features four parallel runways and nine terminals each serving different airlines and destinations. The largest one is the Tom Bradley International Terminal dedicated to international flights. The Central Terminal Area serves as the focal point of the airport connecting all the terminals. It includes a complex network of roadways, parking structures, and transportation services, such as shuttles and taxis, to facilitate passenger movement around the airport.

Given its prominence and size, LAX is one of the prime targets on the West Coast of potential attacks. Safeguarding such a complex and sprawling facility requires a delicate balance between security measures and operational efficiency. Unfortunately, available security resources are limited, making it impossible to provide round-the-clock security for each and every place of interest. For instance, while the number of canines exceeds the number of terminals, there are only a handful of canines of particular expertise, such as explosive detection ones. It means that it is simply impossible to provide constant coverage of a single explosive detection canine patrol per each terminal at LAX. The same hold for other types of canine patrols, such as those specialised in drug detection.

Interestingly, however, in 2008, the drug sniffing canine patrols at the LAX airport turned out to be much more effective than it was previously believed possible. While in the 15 month period between April 2006 to July 2007, only 4 drug-related offences were recorded, in the 12 months of 2008 the number of cases grew to 30. The reason behind this significant improvement was ARMOR which stands for the Assistant for Randomized Monitoring over Routes. The ARMOR system was an innovative software tool developed by Milind Tambe and his colleagues at the University of Southern California (USC)[1], within the Department of Homeland Security's first University Center of Excellence.

[1] J. Pita et al., *Using game theory for Los Angeles Airport security*, "AI Magazine" 2009, vol. 30, no. 1, pp. 43–57.

The primary objective of the ARMOR system is to assist security personnel in making better and more efficient decisions by weighing risks against available resources. To this end, ARMOR leverages artificial intelligence (AI), game theory, and optimization techniques. The system makes it difficult for adversaries to plan how to avoid security forces during an attack. Even more importantly, it allows security forces to deploy their limited resources in the most efficient manner and achieve maximal effectiveness.

The implementation of ARMOR at LAX resulted in the improvement in security coverage, resource allocation efficiency, and deterrence against potential attackers. For example, Chart shows that the introduction of the ARMOR system at the LAX Los Angeles Airport resulted in more than threefold increase in the number of detected offences. The system serves as an exemplar of how advanced technology and AI-driven approaches can contribute to strengthening security measures and enhancing the safety of airports and their passengers.

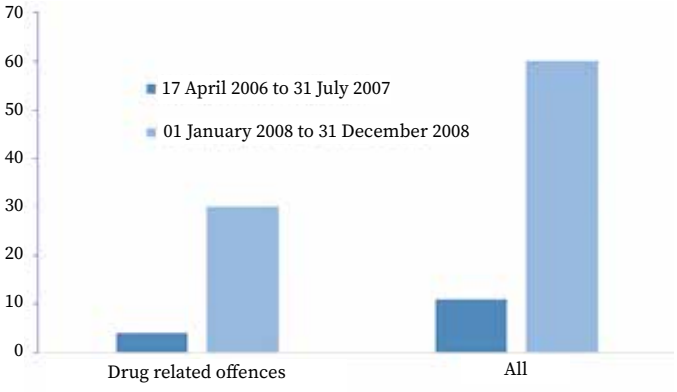


Chart. The number of offences in the period of 15 months before introducing ARMOR (dark blue bars) vs. the number of offences in the period of 12 months after introducing the system (light blue bars).

Source: own elaboration based on: Pita et al., *Using game theory for Los Angeles Airport security*, "AI Magazine" 2009, vol. 30, no. 1, pp. 43–57.

The success of ARMOR received significant attention in the context of security applications. A number of systems based on similar principles were deployed in the USA to protect other critical infrastructure sites. These include, in particular:

- IRIS system[2] – to optimize the routes and schedule of the security agents in the U.S. Air Marshals program;
- PROTECT[3] – to optimize the security of the Boston and New York ports;
- TRUSTS system[4] – to prevent fare evasion created for the railway transport system in Los Angeles.

Furthermore, it has been advocated in the context of cybersecurity[5]. There are also a growing number of civilian applications such as protecting endangered species in national parks (systems PAWS[6] and MIDAS[7]). In all these cases, it was possible to significantly improve security, not by adding many additional security resources but by better deployment of the available ones.

This is a very important lesson for Europe and Poland in particular. Given recent geopolitical developments, and the on-going Russian full-scale invasion in Ukraine that started in 2022, we are all well aware of the pressing concern of infrastructure security. Europe has already witnessed a few such attacks[8]. The question now is not if the next attacks will happen but when.

---

[2] J. Tsai et al., *Iris - a tool for strategic security allocation in transportation networks*, in: *Proceedings of the 8th International Conference on Autonomous Agents and Multi-Agent Systems* (AAMAS 2009), pp. 37–44 (the proceedings of the AAMAS conference series are available at: https://dl.acm.org/conference/aamas/proceedings – editor's note).

[3] E. Shieh et al., *Protect: A deployed game theoretic system to protect the ports of the United States*, in: *Proceedings of the 11th International Conference on Autonomous Agents and Multi-Agent Systems* (AAMAS 2012), vol. 1, pp. 13-20.

[4] Z. Yin et al., *Trusts: Scheduling randomized patrols for fare inspection in transit systems*, in: *Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence* (AAAI 2012), vol. 26, no. 2, pp. 2348–2355 (the proceedings from the AAAI conferences and symposia are available at: https://aaai.org/aaai-publications/aaai-conference-proceedings/ – editor's note).

[5] Y. Zhang, P. Malacaria, *Bayesian Stackelberg games for cyber-security decision support*, "Decision Support Systems" 2021, vol. 148, art. 113599. https://doi.org/10.1016/j.dss.2021.113599.

[6] R. Yang et al., *Adaptive resource allocation for wildlife protection against illegal poachers*, in: *Proceedings of the 13th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2014), pp. 453–460.

[7] W. Haskell et al., *Robust protection of fisheries with COmPASS*, in: *Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence* (AAAI 2014), vol. 28, no. 2, pp. 2978-2983.

[8] An example is the deliberate cutting of two optical fibers of the Deutsche Bahn communication system on October 8, 2022, which stopped rail traffic in northern Germany for approximately 3 hours.

Unfortunately, the problem is exacerbated by the growing technological sophistication of critical infrastructure. While modern communication, computation, and control technologies enhance the efficiency, they also make modern critical infrastructure systems increasingly complex and vulnerable to deliberate attacks and random failures. These attacks can manifest in various forms, severities, and magnitudes, ranging from acts of terrorism on local infrastructure to major kinetic strikes during times of war, such as the ongoing Russian invasion on Ukraine. New technologies, such as drones, also enhance the capabilities of the potential attackers.

Facing the evolving and expanding landscape of threats, despite increased interest and investments in infrastructure security, our security resources will remain limited, making it impossible to provide constant protection for everything. Thus, the need to strategically allocate security resources becomes a perpetual necessity. The example of the LAX airport as well as other aforementioned examples from the USA show that such well-designed strategic decision making is beneficial and delivers significant improvement in security.

In this paper, we discuss the fundamentals behind these advanced methods of protecting critical infrastructure, briefly review this body of research, and present the solutions and software which is developed by our team "AI for security" at the IDEAS NCBR research institute.

Defender–Attacker Security Games

Game theory studies interactions between intelligent entities like individuals, companies, or countries. In the context of security, these entities can represent "the defenders", e.g., security forces, police, military, and "the attackers", e.g., criminals, terrorists, and state actors. Game-theoretic approaches help us understand how these intelligent actors interact, assuming they can anticipate and respond to each other's actions. By using game theory, we can develop a strategy to efficiently distribute scarce security resources for infrastructure protection. This approach considers the importance of different targets and how adversaries may react to specific protection strategies.

A non-cooperative game is defined by the set of players, the set of strategies for each player and the payoff function that assigns each

player the utility for any possible combination of strategies. Each game is also associated with some set of rules, e.g., we may require the players to move simultaneously or sequentially.

Table 1 presents a sample game from Pita et al.[9] In this case, we have two players, each having two strategies: {*A*, *B*} and {*C*, *D*}, respectively. The values of the payoff function are given by the pairs of numbers in the matrix, where each cell corresponds to a given combination of strategies, also known as a 'strategy profile'. For instance, if Player 1 plays strategy and Player 2 plays strategy then the Player 1 earns the payoff of 2 while Player 2 the payoff of 1.

Sometimes it is possible to stipulate how the rational players (where the notion of rationality is explicated with a precise mathematical formula) actually would play the game given its rules. Such a collection of players' strategies is called an equilibrium of the game. Perhaps the most well-known equilibrium concept is the Nash equilibrium. A combination of strategies is a Nash equilibrium if any player would not like to change their strategy, given the strategies chosen by the opponents. For instance, in Table 1, the combination of strategies (*A*, *B*) is not a Nash equilibrium, because Player 2 would like to change their strategy from D to C, assuming that Player 1 sticks to strategy A. Conversely, the combination of strategies (*A*, *C*) is a Nash equilibrium, because, for Player 1, *A* is the best strategy if Player 2 plays *C*, and, for Player 2, *C* is the best strategy if Player 1 plays *A*.

Table 1. A payoff matrix for a sample game.

		Player 2	
		C	*D*
Player 1	*A*	(2,1)	(4,0)
	B	(1,0)	(3,2)

Source: J. Pita et al., *Using game theory for Los Angeles Airport security*, "AI Magazine" 2009, vol. 30, no. 1, pp. 43–57.

Players in a non-cooperative game do not have to focus on particular strategies. Instead of choosing a single strategy with certainty, a player can choose one strategy with some probability, other strategy with other probability, and so on and so forth. That is, a player can assign

[9] Pita et al., *Using game theory for Los Angeles Airport*...

probabilities to each available strategy. For instance, Player 1 may choose to play strategy A with a certain probability, denoted by p, and strategy B with a probability of $1 - p$. Similarly, Player 2 can assign probabilities to strategies C and D. By using mixed strategies, the players introduce randomness into their decision-making process. The concept of the Nash equilibrium also extends to the mixed strategies.

Consider the game with the payoff matrix defined in Table 2.

Table 2. An example of payoff matrix for a game with no Nash equilibrium in pure strategies, but with a Nash Equilibrium in mixed strategies.

		Player 2	
		C	*D*
Player 1	*A*	(2,1)	(1,2)
	B	(1,2)	(3,1)

In this game, there is no pure strategy Nash equilibrium, since for every strategy profile, it is beneficial for one of the players to switch their strategy, if the other player's strategy is fixed, but there exists a mixed strategy Nash equilibrium, namely the following:

- Player 1's mixed strategy: A with probability $\frac{1}{2}$, B with probability $\frac{1}{2}$;
- Player 2's mixed strategy: C with probability $\frac{2}{3}$, D with probability $\frac{1}{3}$.

The expected payoff for Player 1 in the equilibrium is:

$$\frac{1}{2}\times\frac{2}{3}\times 2+\frac{1}{2}\times\frac{1}{3}\times 1+\frac{1}{2}\times\frac{2}{3}\times 1+\frac{1}{2}\times\frac{1}{3}\times 3=\frac{5}{3}$$

and the expected payoff for Player 2 is:

$$\frac{1}{2}\times\frac{2}{3}\times 1+\frac{1}{2}\times\frac{1}{3}\times 2+\frac{1}{2}\times\frac{2}{3}\times 2+\frac{1}{2}\times\frac{1}{3}\times 1=\frac{3}{2}$$

The above model is, of course, simplified. In particular, in the case of protecting critical infrastructure, one may argue that the players do not move simultaneously. This is because, an attacker may be able to observe the defensive measures (strategies) employed by a defender. To address this problem, let us consider a seminal economic model proposed by Stackelberg[10], a game is played between two players: a leader and a follower.

[10] H. von Stackelberg, *Marktform und Gleichgewicht*, J. Springer 1934.

That is, in contrast to the previous ex-ample, the Stackelberg game is played sequentially rather than simultaneously. Specifically, the leader selects their strategy first, and this choice is observed by the follower, who subsequently determines their own move accordingly.

The Stackelberg model has garnered substantial attention within the realm of security applications due to its inherent ability to capture the dynamics of defender-attacker interactions. In this context, Stackelberg games are often called security games.

The model encompasses the following aspects:

- the defender, who assumes the role of the leader in the Stackelberg game, allocates limited security resources to protect a designated set of targets. Recognizing that adversaries possess the capability to observe defense strategies and exploit discernible patterns, the defender naturally opts for a mixed (randomized) strategy. For instance, in the case of LAX, the management of the canine unit determines the frequency of visits to each terminal by a specific type of patrol within a given week. In other words, they establish the probability distribution for each patrol type across all terminals;
- the attacker, acting as the follower in the Stackelberg game, observes the defender's chosen strategy, i.e., these probability distributions. This assumption embodies a prudent and realistic scenario, presupposing an intelligent attacker who thoroughly surveys critical infrastructure before devising and executing an attack;
- lastly, having acquired knowledge of the probabilities selected by the defender, the attacker strategically selects the optimal course of action for themselves and subsequently executes their move accordingly.

It is crucial to emphasize that the attacker has the capability to observe the probability distribution chosen by the defender but not the defender's actual move. As an illustration, let us consider an scenario involving the United States Coast Guard (USCG) responsible for patrolling the Mexican Bay to combat drug trafficking via boats. The smugglers can observe the frequency of patrols in specific sea areas and how frequently patrol boats alter their course, e.g., by changing the patrol direction to a different one. In other words, the attackers have knowledge of the probability distribution. Nonetheless, they lack the capacity to predict whether a patrol boat will change its course at a given moment or not. So they cannot simply wait until a patrol boat goes away as there is

a non-zero probability that it may immediately return. Interestingly, as we already mentioned in the introduction, the system called PROTECT, based on the Stackelberg game was introduced by the USCG to enhance port/coastal security.

One may say that the defenders of a critical infrastructure are at disadvantage as they move first (decide on the allocation of defense resource and the probability distributions) and their move is observed by the attacker. However, a more careful analysis reveals that the defender, as the first mover, may have a significant influence on the choices made by the attacker. Intuitively, the defender may push the attacker to choose one strategy not the others.

Table 3. A payoff matrix for a sample game.

		Player 2	
		C	*D*
Player 1	*A*	(1,1)	(3,0)
	B	(0,0)	(2,1)

Source: D. Korzhyk et al., *Stackelberg vs. Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness*, "Journal of Artificial Intelligence Research" 2011, vol. 41, no. 2, pp. 297–327.

As an example, let us assume that Player 1 in Table 3 is the leader in the Stackelberg game. Observe that if the players move simultaneously, then actually the only Nash equilibrium (in pure strategies - observe that, trivially, every Nash equilibrium in pure strategies is also a Nash equilibrium in mixed strategies) of this game is for Player 1 to play A and Player 2 to play C, which gives Player 1 the expected payoff equal to 1. Now, by the power of moving first, Player 1 can choose a uniform mixed strategy of playing A and B with equal probability of 1/2 , instead of A with probability 1 and B with probability 0 as in the case of the Nash equilibrium for a simultaneous game. The choice of the leader pushes the follower (Player 2) to choose strategy D instead of C[11]. In result, by being the leader, Player 1 can secure the expected payoff of 5/2 instead of 1, which is quite a significant difference.

[11] In Stackelberg Games, the assumption is that if the follower remains indifferent, the tie is resolved in favor of the leader, since otherwise the optimal solution is ill-defined.

In Appendix A we present a more formal introduction to security games. Let us now comment on the computational challenges posed by security games and then move on to the overview of approaches in the literature.

Challenges and approaches

The game-theoretic approach described in the previous section has been well-established in the literature for many years. However, it is only in the last two decades that these concepts have been effectively deployed in practice to protect critical infrastructure. The reason for this delayed implementation can be attributed to the computational challenges associated with security games. In this section, we will first discuss these challenges and explore how optimization and AI techniques have emerged as effective tools to address them. Furthermore, we will briefly review the existing lines of research on security games to shed light on the challenges involved in developing practical and feasible solutions.

Computational challenges

In real-life deployments, Stackelberg games pose significant computational challenges due to the following key factors:

- first and foremost, decision spaces in complex and large-scale environments of critical infrastructure are immense. The number of possible strategies and actions that can be taken by the players, such as defenders and attackers, can be truly enormous. For example, the New York City Subway system is one of the largest and busiest public transportation networks in the world, serving millions of commuters and visitors daily. The subway system comprises a vast network of tracks, stations, and interconnected lines, covering a total of 472 stations and over 800 miles (1,287 kilometers) of tracks. There are not only various layers of protective measures (i.e., enormous strategy space of the defender) but also very many attack options (i.e., enormous strategy space of the attacker). This requires efficient algorithms to explore and optimize such a vast decision spaces;
- this difficulty is further exacerbated by uncertainty and incomplete information regarding the intentions, capabilities, and actions

of adversaries. Bayesian security games (see the appendix) explicitly model this uncertainty using probability distributions. This, however, adds computational complexity to the problem;

- next, real-life situations are often dynamic and they constantly evolve. Adversaries may adapt their strategies, and defenders need to respond accordingly. Modeling and optimizing strategies in such dynamic environments require solving repeated or sequential games, which further increase the computational challenge.

The scientific literature took a few routes to deal with the computational challenge posed by security games. One approach is to employ mathematical optimization methods to solve these games efficiently. Researchers have developed algorithms and optimization techniques that can handle large-scale game models and provide solutions within reasonable time frames. These optimization methods exploit the structure of the game to reduce the computational burden and improve computational efficiency. They leverage mathematical programming, linear programming, integer programming, and other optimization frameworks to find optimal strategies and resource allocations.

Due to the inherent complexity of these games, finding exact solutions for large-scale scenarios is often infeasible. Therefore, researchers and practitioners often resort to developing approximation algorithms and heuristics to tackle computational challenges while maintaining a reasonable level of accuracy.

Furthermore, AI techniques may play an important role in enhancing the performance of the optimization algorithms. Using AI to optimize algorithms in general and optimization solvers in particular has led to improvements of the state of the art in the solving of hard computational problems for many years. AI allows existing approaches to scale better, and can be applied in many different contexts, for example the one we consider here, i.e., games and optimization[12]. On the other hand, AI models can approximate the result of expensive computational processes quickly and reliably, allowing to do more with the same amount of resources. For example, when deciding what intervention to use to improve resilience and security, some alternatives will be obviously inferior. AI models can help to identify such inferior interventions quickly and cheaply, even accounting

[12] F. Hutter et al., *Boosting Verification by Automatic Tuning of Decision Procedures*, in: *Proceedings of the 19th International Conference on Computer Aided Verification* (CAV 2007), pp. 27–34.

for the uncertainty of the approximation. The same kind of techniques allow systems like AlphaGO to explore a vast space of possible actions in seconds, used for example to deter wildlife poachers[13].

Another option is to resort to parallel computing and distributed computing techniques. By distributing the computational workload across multiple processors or machines, much larger-scale game models can be handled. Here, advancements in hardware technology that improve parallel computing capabilities, are especially important.

Approaches in the Literature

A brief overview of the Stackelberg games with a couple of illustrative examples can be found in the work by Sinha et al.[14] A major and very recent literature review concerning security games can be found in the paper by Hunt and Zhuang[15]. The review examines the present state-of-the-art in game-theoretic modeling for attacker-defender scenarios and analyzes the literature based on common application areas, modeling approaches, and solution methods, additionally addressing significant gaps in the existing body of research and providing a comprehensive discussion on future directions. Other extensive surveys concerning security gams can be found in the work by Fang and Nguyen[16] and in the one by Nguyen et al.[17], where it is demonstrated that security agencies regularly employ decision aids based on game theory to optimize the allocation of limited security resources against strategic adversaries, and that the unique characteristics of these applications demand innovative solutions from AI systems.

---

[13] S. Gholami et al., *Adversary models account for imperfect crime data: Forecast-ing and planning against real-world poachers*, in: *Proceedings of the 17th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2018), pp. 823–831.

[14] A. Sinha et al., *Stackelberg security games: Looking beyond a decade of success*, in: *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence* (IJCAI 2018), pp. 5494–5501.

[15] K. Hunt, J. Zhuang, *A review of attacker-defender games: Current state and paths forward*, "European Journal of Operational Research" 2023, in press. https://doi.org/10.1016/j.ejor.2023.04.009.

[16] F. Fang, T.H. Nguyen, *Green security games: Apply game theory to addressing green security challenges*, "ACM SIGecom Exchanges" 2016, vol. 15, no. 1, pp. 78–83. https://doi.org/10.1145/2994501.2994507.

[17] T.H. Nguyen et al., *Towards a science of security games*, in: *Mathematical Sciences with Multidisciplinary Applications*, B. Toni (ed.), Springer Cham 2016, pp. 347–381.

Two already classical monographs have emerged as prominent references in the intersection of game theory and security. Tambe's book[18] centers around algorithmic advancements and the adoption of game-theoretic software by government stakeholders. On the other hand, Bier and Azaiez's monograph[19] presents a compilation of works that combine game theory and risk analysis within the realm of security.

The Stackelberg games have been increasingly employed to examine a wide array of security issues, spanning from scenarios like missile defense systems[20], terrorism[21], policing[22], to computer network security[23].

Sometimes the models of security games are being referred to as attacker-defender games. They have been a subject of extensive research for the past years and there is a large body of literature concentrating on variety of different problems. An example, again, might be a resource allocation model where e.g., a government wishes to allocate defensive resources among a set targets (e.g., airports or train stations) in an optimal way, and an adversary seeks to attack some of these targets. In the paper by An et al.[24], the authors present an overview of the aforementioned game-theoretic system PROTECT, utilized by the USCG for scheduling patrols in the Port of Boston and New York (see Image). Importantly, the successful evaluation of PROTECT in the Port of Boston has led to its further deployment in the Port of New York. The foundation of PROTECT lies exactly in the attacker-defender Stackelberg game model. However, the development and implementation of the system involved significant contributions in theory as well as comprehensive evaluations. What

[18] M. Tambe, *Security and game theory: algorithms, deployed systems, lessons learned*, Cambridge 2011.

[19] V.M. Bier, M.N. Azaiez, *Game Theoretic Risk Analysis of Security Threats*, Springer 2008. https://doi.org/10.1007/978-0-387-87767-9.

[20] G. Brown et al., *A Two-Sided Optimization for Theater Ballistic Missile Defense*, "Operations Research" 2005, vol. 53, no. 5, pp. 745–763. https://doi.org/10.1287/opre.1050.0231.

[21] T. Sandler, *Terrorism & Game Theory*, "Simulation & Gaming" 2003, vol. 34, no. 3, pp. 319-337. https://doi.org/10.1177/1046878103255492.

[22] N. Gatti et al., *Game theoretical insights in strategic patrolling: Model and algorithm in normal-form*, in: *Proceedings of the 2008 conference on ECAI 2008: 18th European Conference on Artificial Intelligence* (ECAI 2008), pp. 403-407.

[23] K-w. Lye, J. Wing, *Game Strategies in Network Security*, "International Journal of Information Security" 2005, vol. 4, pp. 71–86. https://doi.org/10.1007/s10207-004-0060-x.

[24] B. An et al., *A Deployed Quantal Response-Based Patrol Planning System for the U.S. Coast Guard*, "Interfaces" 2013, vol. 43, no. 5, pp. 400–420. https://doi.org/10.1287/inte.2013.0700.

is crucial about the system, it does not assume that adversaries possess perfect rationality, allowing for more realistic and robust scenarios.

Image. The PROTECT system was deployed by the United States Coast Guards to protect the Staten Island Ferry route operated by the New York City Department of Transportation. The picture shows the United States Coast Guards boat protecting one of the ferry vessels.

It is noteworthy that numerous Stochastic Stackelberg Games exist, wherein the decision-making abilities of the adversary are limited by bounded rationality. The majority of systems based on Stackelberg games have traditionally relied on the conventional game-theoretical assumption of adversaries being perfectly rational, which aligns with the standard in game theory literature. However, this assumption may not accurately reflect the behavior of real-world adversaries, as human adversaries often exhibit bounded rationality. Therefore, taking inspiration from psychological and behavioral economics models, researchers (e.g. Yang et al. [25]) have delved into studying parametrized models of bounded rationality in these games. The models in question offer versatile approaches for incorporating bounded rationality into game settings, making them applicable to a wide range of game interactions beyond Stackelberg Security Games. An example of such an approach is an instance studied in the work by

[25] R. Yang et al., *Improving Resource Allocation Strategy Against Human Adversaries in Security Games*, in: *Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence* (IJCAI 2011), pp. 458–464.

Nguyen et al.[26], where rather than selecting a single target as the optimal response to the induced coverage C of targets by defense resources, the adversary's response h(C) entails probabilistically choosing a target t based on a probability q_t associated with that target.

Let us conclude by noting that there are various further potential applications of Stackelberg Games in modelling adversarial security scenarios. They do include – among others – the following:

- Patrolling games by Vorobeychik et al.[27], designed to simulate situations where environments need to be patrolled to deter intruders. These games draw inspiration from the widely recognized pursuit-evasion game model but have been expanded in diverse ways, including the incorporation of alarm systems;
- In plan interdiction games by Vorobeychik and Pritchard[28], the defender is tasked with selecting a mitigation strategy to intercept potential attack actions, while the attacker, in response, devises an optimal attack plan that bypasses the implemented mitigations. This model finds relevance in the context of adversaries operating in cybersecurity;
- Audit games (J. Blocki et al.[29]) investigate the economic aspects involved in designing audit mechanisms, with a specific emphasis on efficient resource allocation and suitable punishment schemes. The audit game model expands upon the security game model by introducing an extra parameter related to punishment. These models find practical application in audits aimed at ensuring compliance with privacy policies within diverse institutions, including medical hospitals;

[26] T.H. Nguyen et al., *Analyzing the effectiveness of adversary modeling in security games,* in: *Proceedings of the Twenty-Seventh AAAI Conference on Artificial Intelligence* (AAAI 2013), no. 1, pp. 718–724.

[27] Y. Vorobeychik, B. An, M. Tambe, *Adversarial Patrolling Games,* in*: Papers from the 2012 AAAI Spring Symposium,* vol. 3, pp. 91–98.

[28] Y. Vorobeychik, M. Pritchard, *Plan interdiction games,* in: *Adaptive Autonomous Secure Cyber Systems,* S. Jajodia et al. (ed.), Springer Cham 2020, pp. 159-182. https://doi.org/10.1007/978-3-030-33432-1_8.

[29] J. Blocki et al., *Audit games with multiple defender resources,* in: *Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence* (AAAI 2015), vol. 29, no. 1, pp. 791–797.

- Coalitional security games (Guo et al.[30]) tackle the issue of optimizing the prevention of attacker coalitions, where attackers have the ability to form alliances. This concept is particularly relevant in domains such as disrupting terrorist networks, dismantling cells of these networks, or preventing collusion among multiple attackers.

"AI for Security" Team at the IDEAS NCBR

At the IDEAS NCBR research institute, our team "AI for Security" builds Stackelberg models for various types of critical infrastructure. Currently, we have been focusing on developing software for protecting ports, LNG terminals, railways, and power grids. Figure presents the interface of our basic software.

Figure. The snapshot from the Interface of the security-game software that is under development at IDEAS NCBR by the team "AI for Security". Here, we can see the map of the LNG Terminal in Świnoujście. The red circles represents targets (the size of the circle corresponds to the importance of the target). The blue circles represent the positioning of the patrols and their field of view. The heatmap on the right shows the relative probability of which parts of the site should be patrolled (the optimal strategy of the defender). Note that the positioning of targets and patrols on this snapshot is for demonstration purposes only.

[30] Q. Guo et al., *Coalitional security games*, in*: Proceedings of the 15th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2016), pp. 159–167.

Our goal is to create a system with the following features:

- Risk Assessment: our system should conduct continuous risk assessments through the analysis of diverse data sources, current and historical ones, and intelligence reports. In order to optimize the allocation of security resources, it should take into account elements such as threat levels, target desirability, and vulnerabilities.
- Randomized Patrol Strategy: Our system should employ randomized strategies to determine the optimal patrol routes for security personnel coupled with optimal deployment of security devices. By randomizing routes, the system increases the difficulty for potential adversaries to predict security patterns, thereby strengthening the element of surprise and deterring potential threats.
- Dynamic Adaptation: our system should accommodate evolving threats and adapt to changing security scenarios. It should possess the capability to dynamically modify patrol routes and allocate resources in response to real-time information, such as emerging intelligence that updates the knowledge of the actual risk situation. This goal is to ensure optimal coverage and enhance response abilities.
- Collaboration and Coordination: the system should facilitate collaboration among diverse security teams and agencies operating within the protected area. It should enable the sharing of information, coordination of efforts, and real-time intelligence exchange, all aimed at enhancing situational awareness and achieving improved security outcomes.
- Performance Evaluation and Feedback: finally, it should incorporate mechanisms for evaluating performance, enabling security personnel to analyze the effectiveness of the system and adapt strategies accordingly. The system should offers feedback, identifying areas for improvement and recognizing patterns that may warrant attention.

In the recent work, members of our team "AI for Security" published a paper at one of the key computer science conferences: the Conference on Uncertainty in Artificial Intelligence (UAI 2023, Pittsburgh, USA)[31] that analyzed a situation of an attack that has two phases. Typically, the attack

[31] A. Nagórko, P. Ciosmak, T. Michalak, *Two-phase security games,* in*: Proceedings of the Thirty-Nine Conference on Uncertainty in Artificial Intelligence* (UAI 2023), pp. 1489–1498.

in security games is modeled as a one-off assault during which the attacker has no chance to update their strategy even if new valuable information is gained in the process. This, however, does not cover certain tactics that can be applied by ever more agile covert organizations.

To address this, we propose a model in which, in the first phase, the attacker makes a preliminary move designed to gain extra information on the defender's activities in this particular instance of the game. Next, in the second phase, this insight is used to choose an optimal concluding move.

A recent real-world example of the tactics that are explicitly modeled in our two-phase game are the actions of Lukashenko's regime in Belarus which exploits immigrants to probe the border with Ukraine[32]. This callus behaviour puts the lives of the immigrants in extreme danger both due to very difficult terrain and the ongoing war. In more details, Ukraine's northwestern border of nearly 900 km is a heavily forested area full of forbidding wetlands and the Chernobyl Exclusion Zone. On top of that, the border – that was crossed by the Russian army in February 2022 and then subsequently restored by the Ukrainian counteroffensive – is now heavily fortified with trenches, walls and mine fields.

Regrettably, despite the fact that the border has now become one of the most perilous in the world, the Belarusian border guards are actively organizing and coordinating groups of immigrants in an attempt to breach it. Their objective is to expose and disrupt the Ukrainian defenses, which are obligated to respond to such attempts due to the threat posed by Russian saboteurs.

Given that some sophisticated electronic security measures are in place, most of these border crossings are detected. However, it should be noted that detection does not necessarily guarantee the presence of a patrol close enough to pre-vent unauthorized entry, meaning that the border is not entirely impenetrable. Nevertheless, even in cases where a specific section of the border is unguarded at the moment of entry, the Ukrainian headquarters promptly dispatch a team to the area.

Consequently, subsequent attempts to enter the same section of the border are highly unlikely to succeed, given the swift response and reinforcement measures taken by the Ukrainian authorities.

---

[32] V. Romanenko, *Belarus uses migrants for intelligence on the border with Ukraine*, https://www.pravda.com.ua/eng/news/2022/12/6/7379514/ [accessed: 25 VI 2023].

Let us consider a scaled-down version of the problem, with four sections of the Belarus-Ukraine border (S_1, S_2, S_3, and S_4) and two patrol units. This setting can be modelled as a standard security game in the spirit of the one used at the Los Angeles World Airport[33]. Pure strategies (moves) of the Ukrainian defenders are possible assignments of patrols to the sections of the border:

$$I = \{S_1S_2, S_1S_3, S_1S_4, S_2S_3, S_2S_4, S_3S_4\}$$

We assume there are two possible types of the attacker: low- and high-profile human traffickers (type 1 and 2, respectively). The high-profile type of the attacker inflicts a much larger loss upon the defender as they organize much bigger groups. Both types have the same strategy space, i.e., an attacker of each type can either choose one of the four sections of the border or back off, i.e., $J_1 = J_2 = \{S_1, S_2, S_3, S_4, \varnothing\}$. The payoffs of both parties, depending on the attacker type, increase linearly with S_i: for a high-profile attackers payoffs are 50, 100, 150 and 200 respectively and for a low-profile attacker the payoffs are five times smaller. The defender payoffs are opposite, with small random noise added uniformly from interval [–5,5].

Assuming that probabilities of attacks by these two types are $p_1 = 0{,}8$ for the low-profile attacker and $p_2 = 0{,}2$ for the high-profile one, an optimal strategy for the defender is:

$$(x_{S_1S_2}, x_{S_1S_3}, x_{S_1S_4}, x_{S_2S_4}, x_{S_2S_4}, x_{S_3S_4}) = (0\%, 50\%, 0\%, 0\%, 50\%, 0\%)$$

According to this strategy, border sections S_1 and S_2 are never protected simultaneously. Such a situation is typical for Stackelberg equilibria in one-phase games and can be easily exploited by performing a two-phase attack.

Now, let us discuss the concept of a two-phase attack. Assume that, unbeknownst to the defender, the attacker possesses the necessary resources and capabilities of both a low-profile human trafficker and a high-profile one. Consequently, the attacker can attempt to breach two sections of the border sequentially, in distinct phases.

Based on the optimal strategy derived previously, let's consider the scenario where, in the first phase, a low-profile human trafficker makes an attempt to breach the border at section S_1. This initial

[33] J. Pita et al., *Using game theory for Los Angeles Airport...*

phase provides the attacker with valuable information, regardless of the defender's positioning. This is due to the fact that the attacker now possesses knowledge of a conditional probability distribution pertaining to the defender's resources.

Let $t \in \{0\%, 17\%, 33\%, 50\%, 67\%, 83\%, 100\%\}$ be a chance of encountering a two-phase attacker, $(1 - t)$ x 80% be a probability of encountering a low-profile attacker and $(1 - t)$ x 20% be a likelihood of encountering a high-profile attacker. For $t = 0\%$ this is the standard one-phase model, while $t = 100\%$ describes a pure two-phase attack.

Table 4 shows that presence of two-phase attackers significantly alters the Stackelberg equilibrium of the game. For example, for 33% probability of a two-phase attack (with 53% chance of a single-phase low-profile attack and 13% chance of a single-phase high-profile attack, keeping the 4 : 1 low- to high-profile ratio), the optimal defender strategy becomes

$$(x_{S_1S_2}, x_{S_1S_3}, x_{S_1S_4}, x_{S_2S_4}, x_{S_2S_4}, x_{S_3S_4}) = (12\%, 15\%, 17\%, 17\%, 18\%, 21\%)$$

As we see in Table 4, two-phase Stackelberg equilibria are much more robust against changes of attacker profiles.

Table 4. Each row presents an optimal mixed strategy of the defender against a group of attackers with a given chance of encountering a two-phase attack. As we can see in the last row, without presence of two-phase attackers the Stackelberg equilibrium heavily over-fits to the random noise in payoff matrices.

S_1S_2	S_1S_3	S_1S_4	S_2S_3	S_2S_4	S_3S_4	Chance of a two-phase attack
0.085	0.11	0.12	0.2	0.25	0.23	100%
0.085	0.11	0.12	0.2	0.25	0.23	83%
0.12	0.11	0.12	0.2	0.25	0.23	67%
0.12	0.15	0.17	0.17	0.18	0.21	50%
0.12	0.15	0.17	0.17	0.18	0.21	33%
0.15	0.15	0.17	0.16	0.18	0.18	17%
0	0.5	0	0	0.5	0	0%

Moves of the defender (patrol placements)

Table 5 shows how defender payoffs change against different compositions of attacker groups. For example, the expected payoff of the defender against a single-phase attack drops to –175 when single-phase strategy is pitted against a two-phase attacker.

Table 5. Expected defender payoff when playing a strategy from Table 4 against a given chance of a two-phase attack. As we can see in the last column, the loss incurred by playing a strategy that ignores the possibility of a two-phase attack is an order of magnitude larger than over-cautious protection against such attacks.

100%	83%	67%	50%	33%	17%	0%	Chance of a two-phase attack
-16.2	-16.2	-16.2	-20.3	-20.3	-24.9	-175	100%
-14.8	-14.8	-14.8	-17.3	-17.3	-20.9	-146	83%
-13.4	-13.4	-13.4	-14.3	-14.3	-16.9	-116	67%
-12	-12	-12	-11.3	-11.3	-12.8	-87.1	50%
-10.7	-10.7	-10.7	-8.36	-8.36	-8.84	-57.9	33%
-9.27	-9.27	-9.27	-5.38	-5.38	-4.83	-28.6	17%
-7.89	-7.89	-7.89	-2.41	-2.41	-0.816	0.7	0%

Defender strategy

In order to fix this flaw, we propose a new model which allows for considering one-phase and two-phase attackers simultaneously. With our security model, the expected payoff against coordinated attackers jumps from –175 to –16.2 (the defender is still at a disadvantage). The optimal strategy:

$$(x_{S_1S_2}, x_{S_1S_3}, x_{S_1S_4}, x_{S_2S_4}, x_{S_2S_4}, x_{S_3S_4}) = (8{,}5\%, 11\%, 12\%, 20\%, 25\%, 23\%)$$

forces the low-profile attacker to attack S_1 and the high-profile attacker to back off if S_1 was not patrolled. Note that this comes at a cost: for the uncoordinated (one-phase) attack, when low- and high-profile attackers act independently, this strategy brings payoff –7.89 to the defender (a drop from 0.7).

Summary

In this paper, we have provided an exposition of advanced methodologies to ensure the safety of critical infrastructure that incorporate the combination of game theory, optimization techniques, and AI algorithms. The effectiveness of these methods has been demonstrated through their successful deployment in practice in multiple location in the USA. It is crucial to underline that these improvements were achieved not by adding on security resources but rather by optimally deploying the available ones. The work of our team "AI for Security" at the IDEAS NCBR research institute is focused on extending these results and make them applicable to various types of critical infrastructure and to the security threats that have recently reappeared in Europe. We aspire to have them implemented soon to optimize in practice the protection of the Polish critical infrastructure sites and systems.

A Formal Description

We start with a formal description of security games that follows modern treatment by Xu[34]. Then we describe a broader class of Bayesian Stackelberg games that forms a basis for the two-phase model discussed in the previous part of article and we derive a quadratic optimization problem that can be used to solve these games.

A.1 Security Games

A security game, once again, is a two-player game between a defender and an attacker. The defender possesses multiple security resources and aims to allocate these resources to protect n targets from the set $[n] = \{1,2,\ldots,n\}$. A defender pure strategy is a subset of targets that is protected (covered) in a feasible allocation of these resources. A representation of a pure strategy is a binary vector $e \in \{0,1\}^n$ where the entries of value 1 specify the covered targets. Let $E \subseteq \{0,1\}^n$ denote the set of all defender pure strategies. A defender mixed strategy is a probability distribution x over the elements in E. An attacker pure strategy is a target $i \in [n]$. An attacker mixed strategy is denoted by $y \in \Delta_n$, where Δ_n is an n-dimensional simplex. We will use y_i to denote the probability of attacking target i.

[34] H. Xu, *The Mysteries of Security Games: Equilibrium Computation Be-Comes Combinatorial Algorithm Design*, in: *Proceedings of the 2016 ACM Conference on Economics and Computation* (ACM EC 2016), pp. 497–514.

In a most general phrasing, security games are a form of a bilinear game. A bilinear game is given by a pair of matrices (A,B) and polytopes (P,Q). Given that player 1 plays $x \in P$ and player 2 plays $y \in Q$, the utilities for player 1 and 2 are $x^T Ay$ and $x^T By$ respectively.

We can now give different notions of equilibria for security games. A strategy profile (x, y) is a Nash equilibrium, if:

$$\forall x' \in P \ \forall y' \in Q \ x^T Ay \geq x'^T Ay \ \& \ x^T By \geq x^T By'$$

By The Nash Theorem, there exists at least one NE, possibly multiple NEs, in any bilinear game.

When one player moves before another player, the Stackelberg equilibrium serves as a more appropriate solution concept. A two-player Stackelberg game is played between a leader and a follower. The leader moves first, or equivalently, commits to a mixed strategy. The follower observes the leader's strategy and best responds. The leader's optimal strategy, together with the follower's best response, forms an equilibrium.

Let

$$y_x = \arg\max_{y' \in Q} x^T By'$$

denote the follower's best response to a leader strategy $x \in P$. A strategy profile (x, y) is a strong Stackelberg equilibrium if:

$$x = \arg\max_{x' \in P} x'^T Ay_{x'} \quad \text{and} \quad y = y_x$$

When $B = -A$, the bilinear game is zero-sum. In such games, both NE and SSE, are equivalent to the minimax equilibrium.

A strategy profile (x, y) is a **minimax equilibrium** if

$$\forall x' \in P \forall y' \in Q \ x^T Ay \geq x'^T Ay \ \& \ x^T Ay \leq x^T Ay'$$

If (x, y) is a minimax equilibrium, the strategy x is the player 1's maximin strategy, and y is the player 2's minimax strategy.

The value of the game is:

$$V = x^T Ay = \max_{x' \in P} \min_{y' \in Q} x'^T Ay'$$

We will now describe the payoff structure of the game – given that the attacker attacks target i:

- the defender gets a reward r_i if target is covered or a cost c_i if i is uncovered,
- the attacker gets a cost ξ_i if target i is covered or a reward ρ_i if i is uncovered,
- both players have utility 0 on the other $n - 1$ unattacked targets.

A crucial assumption here is the following: for all $i \in [n]$ we have:

$$r_i > c_i \text{ and } \rho_i > \xi_i.$$

This means that:

- covering a target is strictly beneficial to the defender than uncovering it,
- the attacker prefers to attack a target when it is uncovered.

Definition 1 (Security Game). A security game G with n targets is a tuple (r,c,ρ,ξ,E) that satisfies $r_i > c_i$ and $\rho_i > \xi_i$ for all $i \in [n]$.

The defender's utility can be defined as follows:

$$U^d(e,i) = r_i e_i + c_i(1 - e_i)$$

Given $p \in \Delta_{|\mathcal{E}|}$ and $y \in \Delta_n$, the defender's expected utility is:

$$U^d(p,y) = \sum_{e \in \mathcal{E}} \sum_{i \in [n]} p_e \, y_i U^d(e,i) =$$

$$= \sum_{e \in \mathcal{E}} \sum_{i \in [n]} p_e \, y_i \big(r_i e_i + c_i(1 - e_i)\big) =$$

$$= \sum_{i \in [n]} y_i \sum_{e \in \mathcal{E}} p_e \big(r_i e_i + c_i(1 - e_i)\big) =$$

$$= \sum_{i \in [n]} y_i \left(r_i \sum_{e \in \mathcal{E}} p_e \, e_i + c_i \left(1 - \sum_{e \in \mathcal{E}} p_e \, e_i \right) \right)$$

Given $p \in \Delta_{|\mathcal{E}|}$ i and $y \in \Delta_n$ the defender's expected utility is:

$$U^d(p,y) = \sum_{i \in [n]} y_i \left(r_i \sum_{e \in \mathcal{E}} p_e \, e_i + c_i \left(1 - \sum_{e \in \mathcal{E}} p_e \, e_i \right) \right)$$

If we follow the convention of using:

$$x_i := \sum_{e \in \mathcal{E}} p_e \, e_i$$

where x_i is the marginal coverage probability of target i, then we have:

$$U^d(p, y) = \sum_{i \in [n]} y_i \big(r_i x_i + c_i (1 - x_i)\big)$$

Let $x=(x_1,\ldots,x_n)^T$ denote the marginal probability for all targets induced by the mixed strategy p. Then the equation above shows that the defender's expected utility can be compactly expressed as the bilinear form:

$$U^d(x, y) = \sum_{i \in [n]} y_i \big(r_i x_i + c_i (1 - x_i)\big)$$

Note that $U^d(x, y)$ has the bilinear form

$$x^T A y + a x$$

for some non-negative diagonal matrix A.

A note is in order here: the convex hull of E is a polytope of all the feasible (i.e., implementable by a defender mixed strategy) marginal probabilities:

$$\mathcal{P} = \{x = \sum_{e \in \mathcal{E}} p_e \, e : p \in \Delta_{|\mathcal{E}|}\}$$

so we can simply interpret a point $x \in P$ as a mixed strategy and denote the defender's utility by: $U^d(x, y)$.

Similarly, the attacker's expected utility can be compactly represented in the following form:

$$U^a(x, y) = \sum_{i \in [n]} y_i (\rho_i (1 - x_i) + \xi_i x_i)$$

Note that $U^a(x, y)$ also has the bilinear form

$$x^T B y + \beta y$$

for some non-positive diagonal matrix B.

In zero-sum games, all standard equilibrium concepts are payoff-equivalent to the minimax equilibrium, and our goal is to compute the minimax equilibrium in polynomial time.

When the game is not zero-sum, the main solution concept is the strong Stackelberg equilibrium (SSE): the defender plays the role of the leader and can commit to a mixed strategy before the attacker moves. The attacker observes the defender's mixed strategy and best responds. In this case, the goal is to compute the optimal mixed strategy for the defender to commit to (note that the attacker is not able to observe the defender's real-time deployment, i.e., the sampled pure strategy, since he has to plan the attack before the defender's real-time pure strategy is sampled).

A.2 Bayesian Security Games

The solution deployed at the LAX Airport was based on a broader class of games, called Bayesian security games or Bayesian Stackelberg games. We follow[35] to describe this class and we use the Belarus-Ukraine border protection problem discussed in Section 4 as a running example.

In a Bayesian Stackelberg game, the defender plays against a group of attackers of n distinct types. In each round, the defender plays against a single attacker and encounters the attacker of type $1 \le t \le n$ randomly, with probability p_t. Attackers may have different sets of moves at their disposal that inflict different damage to the defender. In the running example, we have a low-profile attacker ($t = 1$) and a high-profile attacker ($t = 2$), with

$$p_1 = {}^4\!/_5 \text{ and } p_2 = {}^1\!/_5.$$

We let I denote the set of defender's moves. In the running example, the border patrol assigns two patrolling units to four segments of the border, hence $I = \{S_1S_2, S_1S_3, S_1S_4, S_2S_3, S_2S_4, S_3S_4\}$.

In a Bayesian Stackelberg game, the defender picks his mixed strategy x first. Here $x = \{x_i\}_{(i \in I)}$ is a probability measure on I, which we denote by $x \in Prob(I)$ with

$$Prob(I) = \{x: I \rightarrow R: \sum_{i \in I} x_i = 1 \ , x \ge 0\}$$

Strategy x does not depend on t as the defender doesn't know the type of attacker he will encounter.

[35] A. Nagórko, P. Ciosmak, T. Michalak, *Two-phase security games...*

Let J_t denote the set of moves of attacker of type t. In the running example, $J_1 = J_2 = \{S_1,S_2,S_3,S_4,\varnothing\}$, i.e. attackers may either attack one of the border segments or back off. Attackert picks his strategysecond, with the knowledge of the defender's strategy x.

Although it may seem counter-intuitive at first, it is advantageous to the defender to disclose his mixed strategy to the attacker (but not his current defensive positions). It is quite common to disclose information in such scenarios to force the adversary to a favorable response, see e.g. action "ZNICZ" carried out each year by the Polish Police[36].

In each round of the game, both players move independently, according to strategies x and $y^t(x)$ they picked prior. Let $r_{i,t,j}$ denote the defender's payoff if she played move $i \in I$ against the attacker of type $1 \le t \le n$ who played a move $j \in J_t$. Let $c_{i,t,j}$ denote attacker's payoff (which may be different from $-r_{i,t,j}$) as we do not assume that the games are zero-sum in general.

Player payoffs may be compactly presented using payoff matrices. In the running example, the payoff matrices for the high-profile attack are:

	S_1		S_2		S_3		S_4			$\varnothing$
S_1S_2	51,	-50	102,	-100	-152,	150	-211,	200	0,	0
S_1S_3	55,	-50	-123,	100	175,	-150	-221,	200	0,	0
S_1S_4	59,	-50	-108,	100	-169,	150	206,	-200	0,	0
S_2S_3	-69,	50	101,	-100	168,	-150	-221,	200	0,	0
S_2S_4	-55,	50	113,	-100	-170,	150	212,	-200	0,	0
S_3S_4	-75,	50	-123,	100	166,	-150	211,	-200	0,	0

The first number in row i, column j is the defender payoff $r_{i,t,j}$ (here 1 stands for high-profile attacker $t = 1$). The second number is $c_{i,1,j}$. The payoffs for the low-profile attack are:

		S_1		S_2		S_3		S_4		$\varnothing$
S_1S_2	14,	-10	23,	-20	-34,	30	-42,	40	0,	0
S_1S_3	10,	-10	-20,	20	32,	-30	-43,	40	0,	0
S_1S_4	12,	-10	-23,	20	-33,	30	44,	-40	0,	0
S_2S_3	-11,	10	24,	-20	31,	-30	-41,	40	0,	0
S_2S_4	-11,	10	20,	-20	-31,	30	42,	-40	0,	0
S_3S_4	-11,	10	-21,	20	34,	-30	44,	-40	0,	0

[36] *Policyjne działania Znicz*, https://policja.pl/pol/aktualnosci/210088,Policyjne-dzialania-ZNICZ.html [accessed: 25 VI 2023].

Attacker t picks an optimal strategy $\overline{y}^t = \overline{y}^t(x)$ that depends on strategy x known by him and that maximizes his expected payoff

$$\bar{c} = \sum_{i \in I} \sum_{j \in J_t} x_i \bar{y}_j^t c_{i,t,j}$$

This payoff is maximized by a pure strategy, i.e., y^t is optimal if and only if

$$\overline{c} \geq \sum_{i \in I} x_i c_{i,t,j}$$

The defender acts to maximize his expected payoff against the optimal strategies of the attackers, i.e. he picks an optimal strategy x that maximizes his expected payoff:

$$\sum_{i \in I} \sum_{t=1}^{n} \sum_{j \in J_t} p_t x_i \overline{y}_j^t r_{i,t,j}$$

Hence the following quadratic optimization problem solves Bayesian Stackelberg games:

$$\max_{x, y^t} \sum_{i \in I} \sum_{t=1}^{n} \sum_{j \in J_t} p_t x_i y_j^t r_{i,t,j}$$

subject to:

$$\sum_{i \in I} x_i = 1,$$

$$\sum_{j \in J_t} y_j^t = 1 \text{ for each } 1 \leq t \leq n,$$

$$\sum_{i \in I} \sum_{j \in J_t} x_i y_j^t c_{i,t,j} \geq \sum_{i \in I} x_i c_{i,t,j} \text{ for each } 1 \leq t \leq n, j \in J_t,$$

$$x \geq 0, y^t \geq 0 \text{ for each } 1 \leq t \leq n.$$

This formulation coupled with a linearization technique leads to a mixed integer linear programming formulation of Bayesian Stackelberg games published by Paruchuri et al.[37], as the celebrated DOBSS algorithm.

[37] P. Paruchuri et al., *Playing Games for Security: An Efficient Exact Algorithm for Solving Bayesian Stackelberg Games*, in: *Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2008), vol. 2, pp. 895–902.

Bibliography

An B. et al., *A Deployed Quantal Response-Based Patrol Planning System for the U.S. Coast Guard*, "Interfaces" 2013, vol. 43, no. 5, pp. 400–420. https://doi.org/10.1287/inte.2013.0700.

Bier V.M., Azaiez M.N., *Game Theoretic Risk Analysis of Security Threats*, Springer 2008. https://doi.org/10.1007/978-0-387-87767-9.

Blocki J. et al., *Audit games with multiple defender resources*, in: *Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence* (AAAI 2015), vol. 29, no. 1, pp. 791–797.

Brown G. et al., *A Two-Sided Optimization for Theater Ballistic Missile Defense*, "Operations Research" 2005, vol. 53, no. 5, pp. 745–763. https://doi.org/10.1287/opre.1050.0231.

Fang F., Nguyen T.H., *Green security games: Apply game theory to addressing green security challenges*, "ACM SIGecom Exchanges" 2016, vol. 15, no. 1, pp. 78–83. https://doi.org/10.1145/2994501.2994507.

Gatti N. et al., *Game Theoretical Insights in Strategic Patrolling: Model and Algorithm in Normal-Form*, in: *Proceedings of the 2008 conference on ECAI 2008: 18th European Conference on Artificial Intelligence* (ECAI 2008), pp. 403–407. https://doi.org/10.3233/978-1-58603-891-5-403.

Gholami S. et al., *Adversary models account for imperfect crime data: Forecasting and planning against real-world poachers*, in: *Proceedings of the 17th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2018), pp. 823–831.

Guo Q. et al., *Coalitional security games*, in: *Proceedings of the 2016 15th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2016), pp. 159–167.

Haskell W. et al., *Robust protection of fisheries with COmPASS*, in: *Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence* (AAAI 2014), vol. 28, no. 2, pp. 2978–2983.

Hunt K., Zhuang J., *A review of attacker-defender games: Current state and paths forward*, "European Journal of Operational Research" 2023, in press. https://doi.org/10.1016/j.ejor.2023.04.009.

Hutter F. et al., *Boosting Verification by Automatic Tuning of Decision Procedures*, in: *Proceedings of the 19th International Conference on Computer Aided Verification* (CAV 2007), pp. 27–34.

Korzhyk D. et al., *Stackelberg vs. Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness*, "Journal of Artificial Intelligence Research" 2011, vol. 41, no. 2, pp. 297–327.

Lye K-w., Wing J., *Game Strategies in Network Security*, "International Journal of Information Security" 2005, vol. 4, pp. 71–86. https://doi.org/10.1007/s10207-004-0060-x.

Nagórko A., Ciosmak P., Michalak T., *Two-phase security games*, in: *Proceedings of the Thirty-Nine Conference on Uncertainty in Artificial Intelligence* (UAI 2023), pp. 1489–1498.

Nguyen T.H. et al., *Analyzing the effectiveness of adversary modeling in security games*, in: *Proceedings of the Twenty-Seventh AAAI Conference on Artificial Intelligence* (AAAI 2013), no. 1, pp. 718–724.

Nguyen T.H. et al., *Towards a science of security games*, in: *Mathematical Sciences with Multidisciplinary Applications*, B. Toni (ed.), Springer Cham 2016, pp. 347–381.

Paruchuri P. et al., *Playing Games for Security: An Efficient Exact Algorithm for Solving Bayesian Stackelberg Games*, in: *Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2008), vol. 2, pp. 895–902.

Pita J. et al., *Using game theory for Los Angeles Airport security*, "AI Magazine" 2009, vol. 30, no. 1, pp. 43–57. https://doi.org/10.1609/aimag.v30i1.2173.

Sandler T., *Terrorism & Game Theory*, "Simulation & Gaming" 2003, vol. 34, no. 3, pp. 319337. https://doi.org/10.1177/1046878103255492.

Shieh E. et al., *Protect: A deployed game theoretic system to protect the ports of the United States*, in: *Proceedings of the 11th International Conference on Autonomous Agents and Multi-Agent Systems* (AAMAS 2012), vol. 1, pp. 13–20.

Sinha A. et al., *Stackelberg security games: Looking beyond a decade of success*, in: *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence* (IJCAI 2018), pp. 5494–5501.

Stackelberg H. von, *Marktform und Gleichgewicht*, J. Springer 1934.

Tambe M., *Security and game theory: algorithms, deployed systems, lessons learned*, Cambridge 2011.

Tsai J. et al., *Iris - a tool for strategic security allocation in transportation networks*, in: *Proceedings of the 8th International Conference on Autonomous Agents and Multi-Agent Systems* (AAMAS 2009, Industry Track), pp. 37–44

Vorobeychik Y., An B., Tambe M., *Adversarial Patrolling Games,* in: *Papers from the 2012 AAAI Spring Symposium,* vol. 3, pp. 91–98.

Vorobeychik Y., Pritchard M., *Plan interdiction games,* in: *Adaptive Autonomous Secure Cyber Systems,* S. Jajodia et al. (ed.), Springer Cham 2020, pp. 159–182. https://doi.org/10.1007/978-3-030-33432-1_8.

Xu H., *The Mysteries of Security Games: Equilibrium Computation Be-Comes Combinatorial Algorithm Design*, in: *Proceedings of the 2016 ACM Conference on Economics and Computation* (ACM EC 2016), pp. 497–514.

Yang R. et al., *Adaptive resource allocation for wildlife protection against illegal poachers,* in: *Proceedings of the 13th International Conference on Autonomous Agents and Multiagent Systems* (AAMAS 2014), pp. 453–460.

Yang R. et al., *Improving Resource Allocation Strategy Against Human Adversaries in Security Games,* in: *Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence* (IJCAI 2011), pp. 458–464.

Yang R. et al., *Improving resource allocation strategies against human adversaries in security games: An extended study*, "Artificial Intelligence" 2013, vol. 195, pp. 440–469. https://doi.org/10.1016/j.artint.2012.11.004.

Yin Z. et al., *Trusts: Scheduling randomized patrols for fare inspection in transit systems*, in: *Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence* (AAAI 2012), vol. 26, no. 2, pp. 2348–2355.

Zhang Y., Malacaria P., *Bayesian Stackelberg games for cyber-security decision support*, "Decision Support Systems" 2021, vol. 148, art. 113599. https://doi.org/10.1016/j.dss.2021.113599.

Internet sources

Policyjne działania Znicz, https://policja.pl/pol/aktualnosci/210088,Policyjne-dzialania-ZNICZ.html [accessed: 25 VI 2023].

Romanenko V., *Belarus uses migrants for intelligence on the border with Ukraine*, https://www.pravda.com.ua/eng/news/2022/12/6/7379514/ [accessed: 25 VI 2023].

Tomasz P. Michalak, PhD

Leader of an independent research team at IDEAS NCBR and a lecturer at the Faculty of Mathematics, Informatics, and Mechanics at the University of Warsaw. Graduate of the Faculty of Economic Sciences at the University of Warsaw. During his academic career, he conducted research at the Department of Computer Science at the University of Oxford, the School of Electronics and Computer Science at the University of Southampton, the Department of Computer Science at the University of Liverpool, and the Faculty of Applied Economics at the University of Antwerp, where he obtained his Ph.D. in economics.

Michał T. Godziszewski, PhD

Specialist in logic and its applications (in mathematics, philosophy and computer science), artificial intelligence (specialisation - multi-agent systems theory: algorithmic game theory, network analysis, computational social choice theory) and theoretical computer science. His current research focuses on algorithmic analysis of social networks and Stackelberg games, computational complexity in game theory and their applications to security systems modelling.

Andrzej Nagórko, PhD

Adjunct at the Faculty of Mathematics, Informatics and Mechanics at the University of Warsaw. Former employee of the Mathematical Institute of the Polish Academy of Sciences and at universities in United States and Israel. For many years he applied mathematical optimization techniques in diverse fields of mathematics - from artificial intelligence, through game theory to geometric group theory. In IDEAS NCBR he works on applications of these methods to the protection of critical infrastructure.

https://doi.org/10.4467/27204383TER.23.030.18332

https://orcid.org/0000-0002-4015-5774
https://orcid.org/0000-0002-2761-3144
https://orcid.org/0009-0000-7130-0455

PAWEŁ OPITEK
AGNIESZKA BUTOR-KELER
KAROL KANCLERZ

Selected aspects of crime involving virtual currencies

Abstract

The article consists of two parts. The first discusses issues related to the functioning of the crypto-assets market in Poland and internationally and the planned changes in the regulations governing this market. They concern the legal status of digital tokens and their use in money laundering and terrorist financing, as well as the obligations of obliged institutions in the anti-money laundering system. The second part of the study focuses on procedural and non-procedural issues related to virtual currencies. The status of the digital artefact in criminal proceedings, operational work and the conduct of investigations with a view to combating cryptocurrency crime are discussed. The article concludes with demands addressed to law enforcement and law enforcement agencies. The aim of the article is to provide a comprehensive overview of the issues related to the use of virtual currencies in the commission of crimes, covering in particular AML and terrorist financing issues.

Keywords:

cryptocurrencies, virtual currencies, crime, money laundering, terrorist financing, investigation, digital footprints and evidence

Virtual currencies have become integral to the perpetration of various types of crime - they are the object of an executive action when the perpetrator divests an authorised person of authority over bitcoins and the binary data that constitutes them becomes the object of unauthorised manipulation. It is not uncommon for cryptocurrencies to be used for money laundering, obtaining ransomware or social engineering-based attacks. There is also financial embezzlement using cryptocurrencies and crowdfunding, platforms that operate similarly to the traditional forex market or financial pyramid schemes, whose clients are tempted by the promise of a quick and high profit after investing in tokens. There are also cryptocurrencies being issued which are de facto financial derivatives bypassing capital market regulations. The phenomenon of cryptocurrencies is not only analysed in the context of the modus operandi of the perpetrators of criminal acts. It also raises other important issues, such as the legal status of tokens, the criminal analysis of cryptocurrency transfers, the temporary seizure of movable property and property seizure over bitcoin or other altcoins, procedures for obtaining digital footprints and international legal assistance in this regard, or administrative AML/CFT (Anti-Money Laundering/Counter Financing of Terrorism) procedures. This article provides a snapshot of all these issues, but due to its limited volume only some of them could be discussed in more detail.

At the outset, it is worth asking the question: do Polish law enforcement agencies even need capabilities regarding working with crypto-assets? The answer to such a question is certainly yes, which is due to several reasons. In the most general terms, the contemporary crime picture is too often linked to virtual currencies and the technology creating a system of distributed records for institutions intended to protect the economic interests of the state not to orient themselves in the legal, economic and technical aspects of their operation. But there are also specific cases that oblige, for example, the Internal Security Agency (ISA) to take an interest in cryptocurrencies. They are used for large-scale money laundering, and the ISA is obliged to identify, prevent and detect crimes that harm the economic foundations of the state. Security is also about Poland's compliance with international agreements, as this has a direct impact on Poland's position and reputation on the world stage. In this context, it is worth recalling that the sanctions imposed on Russia and Belarus following the aggression of the Russian Federation in Ukraine also cover crypto-activism and Polish services cannot allow these sanctions to be circumvented using domestic network providers. Anonymous transfers on

blockchain can also be a convenient tool to support terrorist organisations and influence agents that exist in various countries, including Poland. The Internal Security Agency is tasked with controlling this segment of the wider financial market in order to prevent such activities.

The article is based on two research objectives: to analyse the current legal status and actual functionality of cryptocurrencies worldwide, and to determine whether they are associated, and on what scale, with the commission of criminal acts, including money laundering and terrorist financing. In the latter case, in addition to taking a critical look at the international dimension of the crime in question, the topic of law enforcement activities in the fight against cryptocurrency crime, which is close to the authors of the study, is also addressed. The analysis of the crime in question on a micro (national) and macro (global) scale led to the identification of actions that require law enforcement agencies to have knowledge of cryptocurrencies and to use it in practice.

The research methodology used consisted of observing and analysing a variety of online sources related to virtual currencies and establishing the ways in which these currencies operate, as well as the thoughts of the article's authors on the issues considered. Among other things, the authors consulted information from the websites of specialist crypto companies and governmental organisations, including the report of a hearing held in the US Congress by representatives of counter-terrorism services on the activities of extremists in the virtual world. In addition, the authors - on the basis of their own competence and professional experience gained from dealing with criminal cases or carrying out supervisory tasks over the capital market - presented conclusions on cryptocurrency crime and the activities of Polish services in this area. They were confronted with source materials in the form of analyses, reports and other studies of organisations and institutions dealing with digital tokens and blockchain technology. Reference was also made to legal acts in force or in the process of being drafted, which regulate the crypto market. Finally, based on the totality of the information obtained, an inductive method was used to record the observations made in relation to the previously stated dataset.

In the article, the terms: cryptocurrencies, virtual currencies and crypto-assets (digital assets) are used interchangeably as it concerns crime and this terminological arbitrariness is of little relevance to the description of the research topic. However, it should be emphasised that cryptocurrencies are the term with the broadest conceptual scope, although they lack a legal

definition in Polish law. Pursuant to the *Executive Order of the President of the United States of 9 March 2022 on ensuring the responsible development of digital assets*[1], the term digital asset refers to digital money issued by a central bank digital currency (CBDC) regardless of the technology used to issue it, and other representations of value, including securities, financial derivatives and other financial products that are used to make payments, invest, transfer or exchange funds or their equivalent, issued or represented in digital form using distributed ledger technology (DLT) regardless of the product name. The term cryptocurrencies, on the other hand, refers to digital assets that can be a medium of exchange, generated or supported by DLT technology. In the middle of the conceptual scopes of these two terms lie virtual currencies.

Legal status of digital tokens

In terms of regulation, virtual currencies are treated differently around the world. Although they have been recognised as legal tender in some countries, these are exceptional situations, as they are most often denied a position similar to that of fiat money. This is due to the fact that the governments of individual countries rigorously guard their monopoly on the issuance of money, as through it they can shape the monetary policy of the country and influence economic processes. Research by the International Monetary Fund shows that virtual currencies have gained the strongest foothold in sub-Saharan Africa, where 25 per cent of countries have regulated their legal status in detail and more than half of them have decided to lift many restrictions on the operation of cryptocurrencies in the traditional financial market[2]. However, this applies to the regulation of payment tokens, such as bitcoin, which is the simplest in its operation. For example, in October 2021, the Central Bank of Nigeria introduced a virtual

[1] *Ensuring Responsible Development of Digital Assets*, Executive Order 14067 of March 9, 2022, Federal Register. The Daily Journal of the United States Government, https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets [accessed: 5 IV 2023]. Translations in the article are from the authors (editor's note).

[2] *Living on the Edge*, International Monetary Fund, October 2022, https://www.imf.org/en/Publications/REO/SSA/Issues/2022/10/14/regional-economic-outlook-for-sub-saharan-africa-october-2022 [accessed: 5 IV 2023].

token called eNaira as a back-up to traditional fiat money. The system was developed by Fintech Bitt, and two apps for using eNaira - eNaira Speed Wallet and eNaira Merchant Wallet - are available in the Google and Apple app shops. 500 million eNaira ($1.21 million) have already been issued in 2022, but the Nigerian government has simultaneously banned transactions in its own banking sector with other cryptocurrencies[3].

In contrast, initiatives are being taken in highly developed countries to systematise approaches to advanced digital tokens issued on the basis of blockchain technology and similar in operation to financial derivatives. Work on the tokenisation of such instruments is well advanced in Japan. In October 2021, MUFG, Japan's largest bank, announced the results of a Security Token Research Consortium group (renamed the Digital Asset Co-creation Consortium in 2022) dedicated to building an infrastructure for tokenised securities. It was planned to record their trading on the Corda corporate blockchain. The right to sub-connect to it has been granted to other companies interested in digital financial instruments - securities listed on the Osaka Digital Exchange, which has integrated with the Progmat platform and allows P2P (peer-to-peer) transactions[4] between investors[5]. The platform is expanding its functionality all the time (it has grown from 80 companies to 163 by the end of 2022) and is currently emphasising the development and trading of stablecoin, enabling settlements to be made outside the official banking system[6].

On the other side are countries that have completely banned the possession of virtual currencies, i.e. China, Nepal, Bangladesh, Afghanistan, Morocco, Algeria and Bolivia[7]. In the case of the Middle

---

[3] P. Opitek, *Funkcjonowanie instrumentów finansowych w oparciu o technologię blockchain* (Eng. Functioning of financial instruments based on blockchain technology), Łódź 2022, p. 214.

[4] P2P transactions - transactions between individuals excluding intermediaries, such as shops, and factories and corporations (editor's note).

[5] *MUFG, SBI share roadmap for Japanese security tokens*, Ledger Insights, 7 X 2021, https://www.ledgerinsights.com/mufg-sbi-share-roadmap-for-japanese-security-token-platform/ [accessed: 27 III 2023].

[6] *MUFG's Progmat security token platform to become digital asset joint venture*, Ledger Insights, 22 XII 2022, https://www.ledgerinsights.com/mufg-progmat-security-token-digital-asset-joint-venture/ [accessed: 5 IV 2023].

[7] F. O'Sullivan, *Where Is Crypto Illegal in 2023? The Countries That Ban Cryptocurrency*, Cloudwards, 22 II 2023, https://www.cloudwards.net/where-is-crypto-illegal/ [accessed: 5 IV 2023].

Kingdom, there are several reasons why this has happened. China has a several-year lead over the rest of the developed economies of the globe in the development of the Central Bank's national digital currency, so the government there may have seen decentralised assets as competition threatening the centralised yuan project. Furthermore, China's economic system favours top-down management of the financial market and arguably the existence of a stand-alone bitcoin is not beneficial to it. As a result, the Chinese authorities began to pursue anti-crypto-currency policies and media marketing campaigns discouraging the use of bitcoin and altcoin. Eventually, a ban on cryptocurrency-related search terms on the internet was introduced, as well as the closure of digital platforms[8].

In the United States and European Union countries, ownership of virtual currencies is permitted, and the only obligations involved relate to some form of registration (notification) of business activities conducted using cryptocurrencies. The issue of financial instruments on blockchain protocols is problematic. In Europe, such activities are generally prohibited, while in the United States, the principle of technological neutrality applies and financial instruments can be tokenised, although in practice this is subject to a number of requirements and is generally unprofitable. Recently, the White House published for the first time ever guidelines to comprehensively define a framework for the responsible development of digital assets in the United States. Following an executive order from President Joe Biden, the country's administration made recommendations to protect consumers, investors, businesses, financial stability, national security and the environment in the context of crypto market operations. The 9 March 2022 Executive Order on Ensuring Responsible Development of Digital Assets[9] outlined an innovative approach to addressing the risks and harnessing the potential benefits of digital assets and their underlying technology. Government agencies have developed frameworks and recommendations to support consumer and investor protection, promotion of financial stability and economic competitiveness, and innovation, among others. The US is also recognised as a global leader in the application of anti-money laundering and counter-terrorist financing procedures in the digital asset environment and sets global standards in this sphere. The White House noted that the popularity

[8] P. Opitek, *Funkcjonowanie instrumentów finansowych…*, p. 212.

[9] *Ensuring Responsible Development…*

of cryptoassets has also led to an increase in the number of cybercriminals carrying out, among other things, money laundering and financing illegal activities. In order to counter such practices, there is a need for increased regulation and oversight of the cryptocurrency market, more intensive law enforcement involvement in the fight against the crime in question, and changes to laws, including the key US Bank Secrecy Act (BSA), toughening the penalties provided for the anonymous transfer of crypto assets and making them also apply to providers of online exchanges and non-fungible NFTs (unique tokens that identify a digitised work of art, such as a sculpture or painting). As part of the steps taken, the White House has committed the US Department of Justice to prosecute serious digital asset crimes committed in any jurisdiction and the Treasury to finalise a risk assessment of illicit decentralised finance in 2023[10].

In turn, the European Union lacks, according to the European Commission, uniform rules applicable to crypto-related services, which exposes consumers and institutional investors to a significant risk of loss. Furthermore, the fact that some Member States have introduced relevant regulations at national level and others have not, leads to a fragmentation of common law that distorts competition in the European single market, hinders service providers from expanding their operations across borders and leads to regulatory arbitrage. This is why the European Parliament will soon vote to adopt the Markets in Crypto-assets (MiCA) Regulation. The regulation would establish harmonised rules for such assets at EU level, thus providing legal certainty for crypto-assets not covered by existing EU legislation. This is expected to enhance consumer and investor protection and financial stability, promote innovation and opportunities for DLT-based tokens. The regulation establishes three types of crypto-assets: asset-linked tokens (akin to stablecoins), e-money tokens and crypto-assets not covered by EU legislation. Already in the initial negotiation agreement, very important issues were established, such as, for example, securing the liquidity and redemption of cryptoassets in such a way that they are backed by the value of reference currencies (1:1 rule). The issuer of cryptocurrencies will be obliged to ensure their redemption in the event

[10] *White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets*, The White House, 16 IX 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/ [accessed: 9 IV 2023].

of market turmoil. This is to ensure a high level of consumer and investor protection and the integrity of the crypto ecosystem, and to minimise the risks to financial stability and monetary policy that may arise from the widespread use of cryptoassets and DLT technology in practice[11].

The European Parliament is also working on a new regulation to tighten policy on virtual currencies by closing a regulatory loophole. The tightening is to oblige decentralised organisations such as DAOs[12], NFTs and DeFi platforms[13] to comply with AML rules on the same basis as traditional financial market players. In April 2023, the US Department of the Treasury published the world's first comprehensive risk assessment of illicit DeFi financing. It shows that criminals are keen to use the services of the 'decentralised finance' market primarily to benefit from ransomware attacks, theft, fraud, drug trafficking and proliferation financing, as well as activities in support of terrorism. The key factors facilitating such activities for them stem from DeFi's lack of AML/CFT and KYC procedures[14], the low degree of cyber-security of its protocols and the fact that its administrators often operate in jurisdictions that do not respect international legal

[11] *Proposal for a Regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Directive (EU) 2019/1937*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593 [accessed: 9 IV 2023]; *Markets in crypto-assets (MiCA)*, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)739221 [accessed: 9 IV 2023].

[12] DAO (decentralised autonomous organisation) - a decentralised organisation that makes autonomous management decisions in accordance with the will of governance token holders, i.e. those with voting rights.

[13] DeFi (decentralised finance) - a decentralised financial system designed for an unlimited number of investors, dedicated blockchain platforms, financial products and services and their creators. DeFi uses fiat money, bank accounts or cashless payment systems in various ways, but the most important are cryptocurrencies, innovative distributed ledger protocols and smart contracts reminiscent of bank accounts and deposits, various forms of credit and financial derivatives. Individual and institutional clients provide the capital for the operation of DeFi and look forward to the return on the investments made, especially as the rate of earnings offered is often much higher than in the traditional capital market. On the other hand, investing in DeFi involves a relatively high risk of losing the funds involved or missing out on the benefits promised by the trader. The decentralisation of DeFi means that there is no single, leading organisation or institution that is responsible for the entire system or its individual components. See: P. Opitek, *Funkcjonowanie instrumentów finansowych…*, p. 156.

[14] KYC (Know Your Customer) - the due diligence procedure that financial institutions and other legally defined entities must carry out to identify their customers (editor's note).

assistance mechanisms or cannot be linked to any territory at all[15]. The plan is therefore to oblige credit and financial institutions to apply stringent due diligence rules when executing crypto transactions exceeding €1k, and business relationships with commercial unlicensed entities would be completely prohibited. The same limit of €1k would apply to transfers originating from self-hosted wallets, when identifying the identity of the holder of such a wallet is much more difficult. EU authorities have also proposed the establishment of a new AML authority to oversee and enforce AML rules across all 27 EU countries[16].

In Polish law, the only legal definition relating to blockchain-anchored digital tokens is found in the *Act of 1 March 2018 on countering money laundering and terrorist financing* (hereinafter: AML/CFT Act). It is made up of two elements: it says what virtual currency is not (e.g. legal tender), and it lists its positive characteristics, such as: digital representation of value, exchangeability in business for legal tender, acceptability as a means of exchange, the possibility of electronic storage or transfer, or the possibility of being subject to electronic commerce. Although a detailed legal analysis of this definition[17] is beyond the scope of this article, it should be noted that in practice its interpretation and application poses many difficulties. There is no doubt that it applies to bitcoin and other altcoins, but one gets the impression that the financial market regulators are unable to clearly address the question of whether Article 2(2)(26) of the AML/CFT Act also applies to stablecoins or NFT tokens. One can risk the thesis that the Polish legislator does not intend to take independent steps towards tighter regulation of the crypto market, but instead waits for changes being processed in the European Parliament. This is partly justified by the fact that the common European policy on cryptocurrencies is shaped at the EU level and there is no point in introducing specific national solutions on the eve of the entry into force of regulations such as the MiCA.

[15] *Illicit Finance Risk Assessment of Decentralized Finance*, U.S. Department of the Treasury, April 2023, https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf [accessed: 14 IV 2023].

[16] I. Preiss, *Crypto AML rules passed by MEPs*, The Block, 28 III 2023, https://www.theblock.co/post/223215/crypto-aml-rules-passed-meps [accessed: 6 IV 2023].

[17] Such an analysis was carried out in the article: G. Ocieczek, P. Opitek, *Analiza definicji walut wirtualnych z ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (Eng. Analysis of the definition of virtual currencies from the Act of 1 March 2018 on the prevention of money laundering and terrorist financing), "Consilium Iuridicum" 2022, no. 3–4, pp. 122–139.

Money laundering using virtual currencies

The offence of money laundering is stipulated in Article 299 of the Criminal Code[18] and presupposes, as an object of protection, the security of economic turnover and the legitimate origin of property values. Of the objects of the executive action described in this provision, such as means of payment, financial instruments, securities, it is virtual currency that will fall within the scope of the property right. This is because the concept of a property right refers to all rights that realise the economic interest of the right holder and comprise their assets[19]. According to Chainanalysis' *Crypto Crime Report*[20], between 2017 and 2022, virtual currencies were used in 'laundering' to the tune of more than $33 billion, with a significant proportion of this value being transferred using online exchanges. In 2021 alone, this volume amounted to almost $9 billion, of which more than 750 million was transferred to DeFi platforms. Observed trends indicate that decentralised finance platforms are becoming an increasingly popular environment for investing illicitly obtained funds, and 2022 was a record year in this respect[21]. This has resulted in the aforementioned work by the European Parliament and the US administration to bring DeFi more tightly under AML regulation.

The professional experience of the article's authors also confirms that virtual currencies are used to commit various types of crimes, including drug trafficking, arms smuggling, fraud, tax evasion, cyber attacks, paying for sabotage and diversion activities, human trafficking and acts of child sexual exploitation. Cryptocurrencies have been seen as a potential source of funding for corruption for some time, but studies of this phenomenon have been general in nature and based more on conjecture than on a convincing methodology[22]. However, the case of Sam Bankman-Fried has shown that such criminality does exist. Bankman-Fried was accused by a US prosecutor of embezzling billions of dollars paid by defrauded

---

[18] *Act of 6 June 1997 – Criminal Code*.

[19] *Prawo cywilne – część ogólna* (Eng. Civil law - general part), M. Safjan (ed.), series: System Prawa Prywatnego, vol. 1, Warszawa 2007, p. 717.

[20] Chainalysis, *The 2022 Crypto Crime Report*, February 2022.

[21] Ibid.

[22] See: M. Alnasaa et al., *Crypto, Corruption, and Capital Controls: Cross-Country Correlations*, International Monetary Fund, 25 III 2022, https://www.imf.org/en/Publications/WP/Issues/2022/03/25/Crypto-Corruption-and-Capital-Controls-Cross-Country-Correlations-515676 [accessed: 4 V 2023].

customers to his cryptocurrency operating company called FTX.com. The investigation found that in a bid to secure favour with politicians, Bankman-Fried made millions of dollars in donations to the election campaigns of both Democratic Party and Republican Party[23]. In addition, in November 2021, he was alleged to have given a bribe of $40 million to at least one Chinese official in exchange for inducing the Middle Kingdom to unblock $1 billion worth of cryptocurrencies seized by Chinese law enforcement authorities[24].

In addition, it appears that transnational criminal organisations are increasingly using digital tokens to transfer and conceal profits from drug trafficking. This is particularly true in Latin American countries, where illicit groups use exchanges operating without KYC and AML procedures to 'launder' billions of dollars a year and, by this means, transfer part of their financial resources to the virtual world in order to avoid prosecutorial detection and confiscation of the 'fruits of the crime'. This includes Mexico's Cártel Jalisco Nueva Generación and Sinaloa Cartel, as well as Central America's Mara Salvatrucha and Brazil's Primeiro Comando da Capital. In the same geographical areas, a growing number of corrupt governments are specifically deregulating the crypto market so that funds invested therein obtained through bribery remain anonymous. Such actions coincide with the interests of Russia, whose allies in South America, such as the Maduro regime in Venezuela, have developed their own cryptocurrency systems to avoid sanctions imposed on the Russian Federation by Euro-Atlantic states and bypass Western currency markets. Venezuela's petro cryptocurrency is used to transfer value between Venezuela and Russia via Russian banks[25]. Such activity was the subject of an indictment filed by the prosecutor in October 2022 in Federal Court in New York. Five Russian nationals were charged therein in connection with illegal purchases of military technology for the Russian Federation (including

[23] *United States of America v. Samuel Bankman-Fried*, https://storage.courtlistener.com/recap/gov.uscourts.nysd.590940/gov.uscourts.nysd.590940.80.0.pdf [accessed: 9 IV 2023].

[24] M. Sigalos, R. Goswami, *Sam Bankman-Fried paid over $40 million to bribe at least one official in China, DOJ alleges in new indictment*, CNBC, 28 III 2023, https://www.cnbc.com/2023/03/28/sam-bankman-fried-paid-over-40-million-to-bribe-at-least-one-chinese-official-doj-alleges-in-new-indictment.html [accessed: 9 IV 2023].

[25] D. Farah, M. Richardson, *The Growing Use of Cryptocurrencies by Transnational Organized Crime Groups in Latin America*, Georgetown University, 20 III 2023, https://gjia.georgetown.edu/2023/03/20/the-growing-use-of-cryptocurrencies-by-transnational-organized-crime-groups-in-latin-america/ [accessed: 6 IV 2023].

advanced semiconductors and microprocessors used in fighter aircraft, missile and space military systems), its smuggling and money laundering using cryptocurrencies. Representatives of Petróleos de Venezuela S.A., Venezuela's state-owned oil company, were also involved in the crime-bearing procedure. The complex criminal scheme involved, among other things, the transfer of millions of dollars' worth of cryptocurrencies, which were used to purchase technology outside the official financial market, as well as to 'launder' the proceeds of illegal activities[26]. In this context, it may be added that on 2 March 2022, the US Attorney General established Task Force KleptoCapture as a law enforcement task force to enforce the extensive sanctions and export restrictions imposed on Russia.

In the European Union and the United States, standards for the regulation of the virtual currency market from an anti-money laundering perspective are shaped by the Financial Action Task Force (FATF)[27]. In 2021, it updated its guidance on a risk-based approach to virtual currency trading and Virtual Assets Service Poviders (VASPs)[28]. The FATF report *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*[29] (September 2020) identifies the technological advantages of crypto-assets and blockchain, but also the risks generated by the new technology. Abuses are fostered by the high anonymity of transfers, the operation of direct P2P value exchange services, 'tumblers' and 'mixers', as well as the different regulation of virtual currencies in different jurisdictions. Indeed, the very concept of a digital token is ambiguous in nature and individual tokens may differ in many respects. This translates into the action of the prosecutor,

[26] *Five Russian Nationals and Two Oil Traders Charged in Global Sanctions Evasion and Money Laundering Scheme*, United States Attorney's Office, Eastern District of New York, 19 X 2022, https://www.justice.gov/usao-edny/pr/five-russian-nationals-and-two-oil-traders-charged-global-sanctions-evasion-and-money [accessed: 7 IV 2023].

[27] The Financial Action Task Force was established in 1989 by the International Monetary Fund and currently has 37 member countries. The purpose of the FATF is to define standards and promote legal measures to combat money laundering, terrorist financing and other serious threats to the integrity of the global financial system. Although the FATF does not explicitly decide on the AML/CFT solutions adopted by individual countries, it is de facto instrumental in shaping them.

[28] A Virtual Asset Service Provider is a provider of a virtual platform and other services to manage virtual currencies.

[29] *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, FATF, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html [accessed: 7 IV 2023].

who is sometimes faced with the difficult task of determining what the cryptocurrencies revealed in the course of an investigation are.

The role of individual states in combating this crime is highlighted, as well as how they should monitor threats and assess the risks involved. The fight against money laundering on the crypto market remains a constant concern for the EU, and the countries of the Old Continent have either incorporated anti-laundering institutions into their legislation or are in the process of introducing new solutions. These include the *travel rule*, which relates to the transmission and sharing of transaction information by service providers operating in the virtual asset market. Such a solution increases the transparency of transfers and therefore the possibility of identifying those involved in operations and blocking suspicious funds. The implementation of the *travel rule* also reduces the risks associated with money laundering and terrorist financing, especially with regard to transfers of an international nature[30]. A further instrument for tidying up the crypto market relates to the obligation in each EU state to establish a register for virtual currency operators. On Polish soil, this has found expression in Article 129m of the AML/CTF Act. Entities obliged to register have the status of an obliged institution, which will be discussed later in this article. At this point, a question may be asked about the actual benefits of the functioning of the register[31], in which, as of 6 April 2023, there were 705 entities entered declaring the type of services they provide, i.e. exchange between virtual currencies and cash, between virtual currencies themselves, intermediation in such exchange and account maintenance for virtual currencies. In the authors' opinion, such an entry, declaratory in nature, currently serves more for companies to authenticate their activities, as affirmed by the state, than for the actual control of these companies by the authorities authorised under the AML/CFT Act.

Different countries implement AML/CFT policy obligations in different ways, and it is a priority of the FATF that the framework of the global

[30] *Anti-money laundering: Provisional agreement reached on transparency of crypto asset tra*nsfers, Council of the EU, 29 VI 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/ [accessed: 7 IV 2023].

[31] According to the law, the register is kept by the Minister of Finance and is actually managed by the Chamber of Fiscal Administration in Katowice (the register is located at the following address: https://www.slaskie.kas.gov.pl/izba-administracji-skarbowej-w-katowicach).

AML regime be uniform. The FATF documents recommend a functional approach. According to this, individual countries model the detailed legal solutions according to their internal, specific circumstances, but everywhere the implementation of the essential guidelines should be at a consistently high level. In the European Union, this task is carried out by the Committee of Experts on the Evaluation of Anti-Money Laundering and Terrorist Financing (Moneyval), which is a permanent monitoring body of the Council of Europe. The Committee is entrusted with assessing the compliance of national norms with international AML/CFT standards, the effective implementation of these norms, as well as making recommendations to state authorities on how to improve regulations in this field. The recommendations of the FATF and Moneyval therefore require countries to build efficient AML procedures, including the imposition of specific obligations on crypto-asset market participants, although each government can concretise the solutions adopted on a case-by-case basis[32]. Determinants in the implementation of EU directives include factors such as a country's political system, its economic development, the openness of a given society to innovation and its wealth.

Terrorist financing through cryptocurrencies

Cryptocurrencies have been linked to the activities of extremist organisations - since at least 2015, terrorists have been recorded trying to use bitcoins to create crowdfunding collections to fund their operations[33].

---

[32] P. Opitek, *Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML* (Eng. Anti-money laundering using virtual currencies in light of national and international AML regulations), "Prokuratura i Prawo" 2020, no. 12, pp. 41–70, Lex, https://sip.lex.pl/komentarze-i-publikacje/artykuly/przeciwdzialanie-praniu-pieniedzy-z-wykorzystaniem-walut-151383722 [accessed: 7 IV 2023].

[33] *Statement of Stephanie Dobitsch, Deputy Under Secretary, Office of Intelligence and Analysis, Department of Homeland Security*, in: *Terrorism and Digital Financing: How Technology is Changing the Threat. Hearing before the Subcommittee on Intelligence and Counterterrorism of the Committee On Homeland Security House of Representatives*, 2021, https://www.congress.gov/117/chrg/CHRG-117hhrg45867/CHRG-117hhrg45867.pdf, p. 8 [accessed: 10 V 2023]. Polish law enforcement services have already discussed the topic of terrorism in 2018, including following a lecture by Paweł Opitek entitled *The use of cryptocurrencies in organised crime and terrorism* presented during a training course for prosecutors of the Department for Organised Crime and Corruption of the National Public Prosecutor's Office and officers

For the most part, these have been organised by groups operating in the Middle East with strong ideological motivations, but illegal activities involving cryptocurrencies and terrorism have also occurred in the United States, Western Europe and, more recently, Ukraine and Poland. US services reports have confirmed that new technologies, such as cryptocurrencies, enable terrorists to further expand and support their efforts to raise funds for illegal activities[34].

Financial support is needed to organise terrorist activities and its beneficiaries can be assisted by crypto-assets. The financing of terrorism through virtual currencies is linked, among other things, to Islamic fundamentalism and the circumvention of economic sanctions by states that do not fully comply with the financial market rules imposed by Western, liberal democracies. There was a debate in Islamic fundamentalist circles as to whether cryptocurrencies were permitted by the Shariah and whether Muslims should use them. Eventually, Al-Qaeda published a manifesto online in the summer of 2014 entitled *Bitcoin wa Sadaqat al-Jihad*[35]. It promoted the use of bitcoin as a convenient means of supporting the fight against infidels bypassing the Western banking system, which restricted donations to the jihad. The manifesto recommended pursuing cryptocurrency transfers for ideological and religious reasons, and described the technical virtues of virtual currencies: resistance to counterfeiting, anonymity of senders and recipients, global reach, and difficulty for law enforcement to detect payments. The superiority of the Bitcoin system over methods such as PayPal or eBay, which are top-down managed and centralised, was highlighted. The manifesto's creators aimed to develop a completely anonymous system for sending donations in bitcoin from the US, the UK, South Africa, Ghana, Malaysia, Sri Lanka or elsewhere in the world to a Mujahideen-managed DarkWallet address. The publication of such a tool has been announced (coming in 2019). In their conclusion, the manifesto's authors said that although the use

of the Central Bureau of Investigation of the Police and the Internal Security Agency, as well as representatives of other bodies, on combating terrorist threats, held in Waplewo on 5-7 November 2018.

[34] *Statement of Chairwoman Elissa Slotkin*, w: *Terrorism and Digital Financing: How Technology is Changing the Threat. Hearing before the Subcommittee on Intelligence and Counterterrorism...*, p. 3.

[35] *Bitcoin wa Sadaqat al-Jihad*, https://krypt3ia.files.wordpress.com/2014/07/btcedit-21.pdf [accessed: 20 I 2019].

of bitcoin faces various obstacles, with most kafirs using it to purchase drugs, the cryptocurrency can be used for a number of useful purposes: from purchasing weapons to donating to the mujahideen. This stance was one of the reasons for the emergence of many social media pages organising cryptocurrency collections for Islamic terrorists from various countries and organisations. The collections are not only conducted by entities directly linked to the criminals, but also by their sympathisers living in the United States or Europe.

Al-Qaeda has used forums and chat rooms on the open Internet since its inception, but after a large-scale service crackdown in 2000 and the arrests of several jihadist supporters, many platforms moved to the Darknet. Today, advanced jihadist forums protect themselves from surveillance by the services with cryptographic encryption, use tools such as Sigaint or TorBox, and access to the platform is verified by the administrator. Forums affiliated with radical movements, such as Shumukh al-Islam oscillating between ISIS and Al-Qaeda supporters, are emerging online[36]. In 2019, the Hamas' military wing (the Izz ad-Din al-Qassam Brigades) posted on social media and on their websites (alqassam.net, alqassam.ps, qassam.ps) a call for contributions in bitcoin for a 'terror campaign'. At the same time, the criminals were learning the rules of cyber security. Izz ad-Din al-Qassam Brigades initially requested that cryptocurrency be sent to a single address hosted on a US exchange, but later developed the technology to generate an individual address for each contribution to make it difficult to trace the origin and transfer of funds. The introduction of new solutions by terrorist groups indicates that they may be adapting to strategies that minimise risk and exploit various technological vulnerabilities[37]. Cyber-terrorist activity is not limited to crowdfunding. In early 2021, Al-Qaeda media offered a reward of 1 bitcoin, worth $60,000 at the time, to the person who murders a police officer in a Western country. Two years earlier, Brenton Tarrant, the perpetrator of attacks on mosques in Christchurch, New Zealand, claimed to have made money from cryptocurrency trading. At the same time, a racially motivated extremist who attempted to carry

[36] B. Berton, *The dark side of the web: ISIL's one-stop shop?*, European Union Institute for Security Studies, June 2015, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf [accessed: 23 VIII 2019].

[37] *Risk Assessment. 2022 National Terrorist Financing*, Department of the Treasury, February 2022, https://home.treasury.gov/system/files/136/2022-National-Terrorist-Financing-Risk-Assessment.pdf, p. 22 [accessed: 10 V 2023].

out an attack at a synagogue in Germany testified that he received financial support in bitcoins[38]. There are many indications that the perpetrators of the terrorist attacks carried out on 13 November 2015 in Paris were supported by cryptocurrency transfers during their organisation[39].

The activity of online terrorists has been noticed and dissected by US law enforcement agencies, which have developed the most effective and advanced tools and methods to combat extremism on the Internet. In the United States, one of the main public bodies dealing with counter-terrorism is the Department of Homeland Security (DHS). Its representative stated at a 2021 Congressional hearing that the DHS, along with the Internal Revenue Service (IRS) and the Federal Bureau of Investigation (FBI), conducted a global cyber operation and dismantled the virtual infrastructure of the Izz ad-Din al-Qassam Brigades. Beginning in October 2019, undercover agents of Homeland Security Investigations (HSI), a counter-terrorism service, made bitcoin donations to terrorists in order to unravel the links of entities running online collections for Hamas. These actions enabled investigators to identify supporters of the organisation living in the United States and to carry out further tracking of transferred funds. Sixty-four unique channels of communication (including email addresses) were identified, allowing the donors' bitcoin wallets to be secured. The operation revealed the terrorists' modus operandi on the internet, including how they recruit supporters online, their funding methods, as well as the domains they use and their IT infrastructure, operating in the US, Canada, Russia, Germany and Saudi Arabia, among others. In July 2020, HSI and IRS special agents executed 24 federal search warrants, seizing cryptocurrency and securing data at numerous online exchanges and network service providers - email, VPNs, online payments. Servers were requisitioned and numerous domains and email boxes linked to terrorist activity were shut down. Friendly services around the world joined the cyber operation, allowing the seizure of terabytes of terrorist-controlled data, hundreds of bitcoin wallets, cryptocurrency worth several million dollars and the dismantling of sites designed for bitcoin donations. Another 2020 investigation by the HSI, IRS and FBI had to do with 24 cryptocurrency accounts identified as foreign assets or

[38] *Statement of Stephanie Dobitsch...*, p. 8.

[39] See i.a.: Y.B. Perez, *Bitcoin, Paris and Terrorism: What the Media Got Wrong*, CoinDesk, 6 III 2023, https://www.coindesk.com/bitcoin-paris-and-terrorism-what-the-media-got-wrong [accessed: 10 V 2023].

sources of influence for Al-Qaeda. The cyber operation concerned the use of cryptocurrency to support and finance terrorism, and 60 virtual wallets were seized as a result[40].

Activities targeting terrorist financing using virtual currencies are regarded by the US government as an important front in the fight against international terrorism. This is confirmed by the 2020 *National Strategy for Combating Terrorist and Other Illicit Financing*[41] prepared by the United States Department of the Treasury. It argues that after the attacks of 11 September 2001, the authorities there focused on vulnerabilities in the financial system. At issue are abuses by charities and unlicensed remittances that allowed Al-Qaeda to transfer money internationally to fund terrorist attacks. After the attack on the World Trade Center, some extremist groups abandoned global operations (complex and widespread attacks) and concentrated on the activities of individual terrorists. Radicalised individuals can carry out relatively inexpensive and uncomplicated, but casualty-producing attacks using knives, firearms and cars. Such activities are facilitated by online communication and cryptocurrency transfers made covertly directly to individuals' wallets, reducing the financial footprint[42].

However, the issue of 'cryptocurrencies and extremism' does not only apply to terrorists, but also to other subversive organisations that threaten the stability and security of democratic states. Virtual crowdfunding is also used by neo-Nazi organisations. Extreme right-wing extremists active on the internet use cryptocurrencies, among other reasons, because they are

---

[40] *Statement of John Eisert, Assistant Director, Investigative Programs, Homeland Security Investigations, Immigration and Customs Enforcement, Department of Homeland Security* in: *Terrorism and Digital Financing…*, pp. 14–16. In 2021, the US Department of Justice announced the dismantling of the infrastructure of three campaigns conducted in cyberspace to finance terrorism, involving the Izz ad-Din al-Qassam Brigades. Sophisticated cyber tools were used in these campaigns, including soliciting donations in the form of cryptocurrencies from around the world. The campaign demonstrated, a US government communiqué proclaimed, how various terrorist groups have similarly adapted their terrorist financing activities to the cyber era. US authorities seized millions of dollars linked to the illegal activity, more than 300 cryptocurrency accounts, four websites and four Facebook pages. See: *Global Disruption of Three Terror Finance Cyber-Enabled Campaigns*, The United States Department of Justice, 13 VIII 2020, https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns [accessed: 9 V 2023].

[41] *National Strategy for Combating Terrorist and Other Illicit Financing 2020*, https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf [accessed: 7 VII 2023].

[42] Ibid, pp. 11–12.

associated with an ideology of deep-seated distrust of financial institutions as those controlled and managed by the 'Jewish finance'. The libertarian origins of the philosophy associated with the rise of bitcoin combining with a distrust of the global establishment also appeals to them. No less important are the purely practical issues surrounding the operation of cryptocurrencies. American neo-Nazis are being roughed out of popular crowdfunding platforms like Patreon, so they are creating alternative sites designed to make donations in the form of decentralised tokens. This is how Hatreon was created. Hosting companies refused to maintain it, so they changed domains to increasingly mask the platform's administrator[43].

Cryptocurrency collection, for example, is carried out by an online US neo-Nazi website called The Daily Stormer. It contains detailed instructions on how to make bitmoney transfers to the address provided there, and the recommended form of deposit is through cryptobanking machines. Andrew Anglin, the site's chief editor, who also publishes a magazine of the same title, is a well-known activist who implements successful crowdfunding campaigns for his organisation. Anglin has repeatedly extolled, including in the pages of The Washington Post, virtual currencies as an excellent tool for raising funds for activities fought by state authorities, and has confirmed that he has received significant donations from people supporting his projects and ideology.

Jihadist recruitment activities on the internet are often closely linked to crowdfunding-based appeals for financial assistance to terrorists. The ease of donating funds and the possibility to donate relatively small amounts can help an extremist organisation materially, while the donor's activity goes unnoticed by the AML system. An example of a completed cryptocurrency crowdfunding carried out for the benefit of militants of the so-called Islamic State was the case of Ali Shukri Amin. The man was born in Africa and emigrated to the United States with his mother when he was a few years old. He settled in Virginia and attended university there. He was interested in science subjects, cyber security topics, encryption and cryptocurrencies. At the same time, Amin radicalised himself and promoted his ideas on social media. Among other things, he set up a Twitter account called @AmreekiWitness, where he posted 7,000 tweets praising

[43] P. Opitek, *Wykorzystanie walut i serwisów wirtualnych do prania pieniędzy i finasowania terroryzmu* (Eng. Use of virtual currencies and services for money laundering and terrorist financing), Warszawa 2019, pp. 43–44 (diploma thesis written during post-graduate studies at the Warsaw School of Economics, unpublished, in the author's possession).

radical Islam and promoting financial support for ISIS through anonymous bitcoin transfers. In addition, he created the blog Al-Khilafah Aridat, where he encouraged the fight against the infidels, as well as producing a series of articles aimed at supporters of the so-called Islamic State. He described in detail how to communicate anonymously online and use encryption during illegal activity on behalf of terrorists. Amin also helped a male acquaintance to reach Syria via Turkey and join the Islamic State militants. In 2015, the prosecutor filed an indictment against him with the court[44], charging him with engaging with other identified and undetermined persons in terrorist activity involving material support and expert advice to foreign ISIS terrorists. The man was sentenced by the court to 11 years' imprisonment.

Obliged institution's responsibilities in the anti-money laundering regime

A pillar of the fight against the crime of money laundering is the AML policy, which must be carried out by obliged institutions. These are entities involved in the broadly defined trading of virtual currencies and, as such, specific obligations have been imposed on them by national governments to counter money laundering. Many of the AML activities relating to crypto-assets are similar to those that have long been associated with cash or e-money payments. However, given the specificity of risk management of transactions involving digital tokens, it is advocated that high requirements for the crypto market must be observed in relation to the activities there, e.g. obtaining a company licence, meeting prudential requirements to hold share capital guaranteeing liquidity, maintaining transparent accounting and periodic audits, holding reserve assets equivalent to the tokens issued. This guarantee fund, which protects investors, provides a financial safety net should, for example, the blockchain protocol be hacked and the underlying value 'stolen'. In view of such cyber threats, obliged institutions must comply with high requirements protecting the assets they hold, including cryptographic keys, and apply, embedded in corporate governance, professional control, risk management and reporting

[44] *United States of America v. Ali Shukri Amin*, CRIMINAL NO. 1:15-CR-164, https://www.investigativeproject.org/documents/case_docs/2826.pdf [accessed: 10 V 2023].

systems. These are accompanied by requirements for the company's internal record-keeping processes, anti-money laundering and countering the financing of terrorism, secure outsourcing, operational resilience of key services (ensuring continuity of the company's operations and high quality of service in the event of a failure of electronic systems or physical events such as fire or interruption of electricity supply). Challenges such as adopting appropriate insolvency and bankruptcy regulations for a company that has placed its assets in cryptocurrencies or provided services and sold products in the crypto market also need to be addressed[45].

The fight against money laundering and counter-terrorism, including virtual currencies, is based on common solutions implemented by the EU into the legal orders of the Union countries. The Fifth Anti-Money Laundering Directive (EU) 2018/843[46], which entered into force in June 2018, played a special role. In Poland, the regulations implementing the solutions contained in this act are effective from May 2021[47]. AML directives issued jointly by the European Parliament and the Council of the EU shape the rights and obligations of professional market participants, public administrations (including FIUs), and indirectly affect state criminal policy. The latter include the possibilities of enforcing obligations against obliged institutions, punishing those responsible for non-compliance, using sources of evidence or securing criminal assets.

In order for law enforcement authorities to take advantage of the opportunities offered by the provisions of the AML/CFT Act in Poland, it is necessary to know the mechanisms governing the AML regime in relation to obliged institutions, including entities engaged in the business of providing virtual currency services (Article 2(1)(12) of the AML/CFT Act). Such entities are obliged to draw up and apply (as well as update and verify) an internal anti-money laundering and counter-terrorist financing

[45] *UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf, p. 20–21 [accessed: 9 IV 2023].

[46] *DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU,* https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018L0843&from=en.

[47] *Act of 30 March 2021 amending the Act on counteracting money laundering and terrorist financing and certain other acts.*

procedure referred to in Article 50 of the AML/CFT Act. The aforementioned provision enumerates exhaustively what such procedure contains, taking into account the nature, type and size of the entrepreneur's activities, and the entire approach to financial security is based on risk estimation. This risk is the possibility of the actualisation of a threat (including the possibility of committing an offence) in relation to a specific customer of the obliged institution within the framework of the services provided by it. Such risks may be determined as minimal and then no special precautions are required. However, once the risk is assessed as high, enhanced financial security measures are implemented (in-depth investigation of the source of funds, identification of the beneficial owner), including the possibility for the obliged institution to terminate the business relationship with the client. It is already incumbent on the cryptocurrency company to assess the extent and frequency of the measures in question, and further tightening is planned. On 7 December 2022, the Council of the EU agreed on a position whereby a maximum cash payment limit of €10,000 will apply across the Union and, in addition, the anonymity of transfers will be reduced for crypto-asset trading, as all providers of such services will be required to carry out due diligence, i.e. a detailed assessment of the counterparty's current situation and the identification of existing and potential risks associated with the planned financial operation for transactions of €1,000 or more[48]. Already now, an obliged institution should take a closer interest in its client when typical symptoms indicating the possibility of money laundering using cryptocurrencies appear in its activity on the platform. These include the use of multiple accounts registered in the names of different persons, multiple conversions of funds held in accounts or conversions between money and virtual currencies without a specific business purpose, the client's use of ATMs, cash deposit machines cryptobanking machines or other devices that allow anonymous deposits or withdrawals of cash and virtual currencies without a reasonable justification in the person's transaction profile, or the use of non-standard payment methods such as Mistertango, N26, Revolut, Western Union, Wirex, PayPal, MoneyGram for transactions (funds entry or exit)[49]. The identification and assessment of AML/CFT risks

[48] *Fight against money laundering and terrorist financing*, https://www.consilium.europa.eu/en/policies/fight-against-terrorism/fight-against-terrorist-financing/ [accessed: 9 IV 2023].

[49] E. Przewłoka, *Metodyka podstawowych czynności realizowanych przez funkcjonariusza Policji i związanych z przestępstwem „kradzieży" waluty wirtualnej* (Eng. Methodology of basic actions carried out by a police officer and related to the crime of "theft" of virtual currency),

should take into account a number of factors, including those relating to the status of the clients (country of origin, size of the company and profile of its activities), the countries or geographical areas of their origin, the type of products and services offered by the counterparties and the channels of distribution of goods, the type of transactions performed. The catalogue of circumstances examined is not closed and is subject to adaptation to changing internal and external conditions in the environment of the entity involved in cryptocurrency activities.

The first request that ISA or any other special service conducting operations should make to an obliged institution whose activities are of interest to the service is to request the submission of an internal AML and terrorist financing procedure in order to check how the procedure was shaped, whether the document meets the requirements of the law and corresponds to the actual activities of the institution, and then to verify how the procedure was implemented in practice. If the document is sound, it will tell you who was responsible for what in the entity's AML policy, how the risks were estimated, where the metadata collected during remote contacts with counterparties is located and what it contains. In addition, enquiries can be made as to whether a particular client:

1. Concealed real personal data in business relationships?
2. Used an account (e.g. payment, bank, virtual currencies) established in the name of another person or pretended to be someone else in his/her dealings with institution staff?
3. Submitted documents raising concerns as to their authenticity or reliability?
4. Logged on to third-party accounts?
5. Declined to submit certain documents or to state the source of funds at his disposal?
6. In yet another way, he impeded the action of the obliged institution in carrying out its AML obligations?
7. Used ATM deposits or withdrawals with commitment of funds to the stock market[50]?

Other documents which, in accordance with Article 50(2) of the AML/CFT Act, constitute obligatory components of the obliged institution's internal AML procedure, i.e. rules on the application of financial security

Bydgoszcz 2023 (Police internal methodology, in the author's posession).

[50] Ibid.

measures, the retention of documents and information, the performance of duties involving the provision of information on transactions and notifications to the General Inspector of Financial Information (GIFI), the dissemination of knowledge of AML regulations among the obliged institution's employees and the reporting by employees of actual or potential violations of these regulations, internal audit, are also subject to examination.

The obligations enshrined in the AML policy of the obliged institution also apply to the analysis of the transactions made with virtual currencies themselves. The prosecutor may require the exchange to provide, in analytical form, information on the customer's order history (entry and exit of funds), the financial or cryptocurrency services and products (especially unusual ones) used by the customer, to submit an individual (currently in force and in the past if it has changed) assessment of the risk attributed to the person or institution, to verify whether it transferred or attempted to transfer funds to tax havens or sanctioned countries. As of 21 March 2023, cryptocurrencies are subject to sanctions imposed on Russia, i.e. provisions relating to the seizure of assets of certain persons, the prohibition of their sharing by such persons and any economic use. Cryptocurrencies should also not be used to circumvent any sanctions established under EU Council Regulation 833/2014[51]. Union entities are further prohibited from providing services related to the operation or provision of cryptocurrency wallets, accounts or custodial services related to crypto values to both Russian citizens and natural persons residing in the Russian Federation, in addition to legal persons and other entities established there. This means that European service providers should close the crypto accounts of their Russian clients and return the digital assets to them (possibly converting them into money or another category of assets that are not subject to sanctions) and, in the case of sanctioned individuals, freeze their assets. The sanctions provisions should be read in conjunction with the deposit limit set out in Article 5b of the said regulation and, in this respect, the conversion of crypto-assets into fiat deposits would only be possible up to the amount allowed for deposits[52].

---

[51] *COUNCIL REGULATION (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*.

[52] *Crypto-assets. Relevant provision: Article 5b(2) of Council regulation (EU) NO 833/2014*, https://finance.ec.europa.eu/system/files/2023-03/faqs-sanctions-russia-crypto_en.pdf [accessed: 10 IV 2023].

The question of how effective the sanctions imposed on Russia are in practice remains open. According to a report by renowned analyst firm Inca Digital, based on an analysis of data collected from 163 cryptocurrency trading platforms around the world, including centralised and decentralised exchanges and P2P sites, as well as OTC (Over the Counter) Brokers[53], as many as 79 of them allow Russian citizens to purchase cryptocurrency (notably the P2P stablecoin Tether), and 11 out of 62 international platforms have no requirements for Russians to meet the KYC procedure before trading[54]. The Seychelles-based Huobi and KuCoin exchanges are the most user-friendly and widely used. They have not taken any steps to prevent sanctioned Russian banks from using their platforms and continuously allow transactions with debit cards issued by these banks, including Sberbank. According to Inca Digital, Binance too offers Russians various methods of converting the currency they hold into crypto, including using the OTC system and the P2P market bypassing the KYC procedure up to the equivalent of a $10,000 deposit, but this limit is easy to circumvent. Transactions can be concealed by, among other things, qualifying payments to non-Russian utilities. ByBit, which operates from Singapore, allows users to exchange Russian roubles for cryptocurrencies using a P2P marketplace and a fiat deposit. The situation described is a direct violation of US and European sanctions and confirms that the market under review is a loophole that limits Russia's economic opportunities. Although, due to the sanctions imposed, many exchanges have officially restricted their activities in the country and declare that they are blocking Russian users from accessing the services offered, in reality they continue, in a more or less veiled form, to cooperate with Russian

[53] The name refers to services provided by OTC brokers, which are primarily large cryptocurrency exchanges such as Kraken, Binance, Coinbase, Satstreet, facilitating direct cryptocurrency trading between two parties to a crypto-crypto (e.g. exchange of bitcoin for ethereum) or crypto-fiat money transaction. This is because traders with large amounts of wealth are looking for secure and anonymous channels for the unlimited exchange of wealth, under predetermined conditions, which are not formally listed on centralised exchanges. Negotiating transactions through OTC brokers between sellers and buyers can take place over the telephone or the web, or even provide for an in-person meeting between the parties.

[54] *How Russians Use Tether to Evade Global Sanctions*, Inca Digital, https://inca.digital/intelligence/how-russians-use-tether/ [accessed: 10 IV 2023].

citizens, including by allowing them to benefit from maximum limits on deposits, trading and withdrawals[55].

An immanent feature associated with the trading of virtual currencies is the difficulty of accessing information about the entities involved in the operations, as they usually operate via the Internet. Therefore, there is an emphasis in the legislation to control the digital footprint of such activities. It follows from the wording of Article 76 of the AML/CFT Act that the obliged institution is under a statutory obligation to have information or documents concerning, inter alia, the IP addresses from which the client's connection to the obliged institution's ICT system took place and the time stamps of the connections to the system. The collection of log histories by the prosecutor may allow a number of relevant data to be established about the person of interest, e.g. the geolocation of the electronic devices used and the frequency and time or period of his/her contacts with the obliged institution. Additional analysis of IP addresses in light of the evidence gathered may prove that:

- transactions were carried out from IPs previously used for illegal activities (e.g. fraud, phishing attacks, distribution of ransomware);
- transactions were carried out from sanctioned countries, tax havens or other "exotic" territory or countries supporting international terrorism;
- the person of interest to law enforcement authorities used tools that anonymise network traffic (Tor, VPNs, proxies);
- there are discrepancies between the IP addresses associated with the customer profile and those from which the transactions were initiated (it can be concluded from this that the person under investigation was a so-called 'strawman' and his personal data were used by the actual beneficiary of the transaction)[56].

---

[55] S. Sutton, L. Seligman, *Two major crypto exchanges failed to block sanctioned Russians*, Politico, 24 II 2023, https://www.politico.com/news/2023/02/24/two-major-crypto-exchanges-failed-to-block-sanctioned-russians-00084391 [accessed: 10 IV 2023]; *Crypto exchanges Huobi, KuCoin enabled Russian sanction evasion. Binance also mentioned*, Ledger Insights, 28 II 2023, https://www.ledgerinsights.com/russia-sanctions-crypto-exchanges-huobi-kucoin-binance/ [accessed: 10 IV 2023].

[56] J. Skała, *Uzyskiwanie przez prokuratora informacji i danych od instytucji obowiązanych na podstawie ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (Eng. Obtaining information and data by the public prosecutor from obliged institutions under the Act of 1 March 2018 on the prevention of money laundering and terrorist financing), "Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2022, n. 3, pp. 92–93. https://doi.org/10.53024/4.3.47.2022.

Crypto transactions should be categorised as higher risk and analysed in detail. In order to increase their transparency, on 29 June 2022 the Council and the EU Parliament reached a preliminary agreement to update the EU Regulation on information accompanying transfers of funds. The new rules will make it mandatory for providers of crypto-asset services to collect and make available certain information about the senders and beneficiaries of transfers. This is to ensure transparency of cryptocurrency transfers in order to better identify suspicious operations and block the funds involved[57]. This increased risk due to the anonymity of crypto transactions extends to other financial market participants (including banks) in addition to typical VASPs, who, although not involved in the trading of virtual currencies, are indirectly exposed to crypto money laundering because, for example, they maintain bank accounts in which funds from the exchange of digital tokens for fiat money are deposited.

An important category of obligations imposed on institutions is the notification to the competent state authorities of events that may constitute an offence or an attempt to commit an offence and notification of a reporting nature. In the latter case, it is a matter of providing the GIFI with information on accepted payments and withdrawals of funds, foreign exchange transactions and transfers exceeding a threshold of a certain monetary value, i.e. on suprathreshold transactions (art. 72 of the AML/CFT Act). Obliged institutions also notify the GIFI of circumstances that may indicate a suspicion that a money laundering or terrorist financing offence has been committed (art. 74 of the AML/CFT Act) and cases where a reasonable suspicion has been obtained that a transfer order or specific property values may be related to money laundering or terrorist financing (art. 86 of the AML/CFT Act). In such a situation, the platform administrator blocks the funds covered by the notification and further decisions on the fate of the assets are taken by the public prosecutor notified by the GIFI. In addition, Article 89 of the AML/CFT Act regulates the obligation to notify the competent public prosecutor on obtaining a reasonable suspicion that the assets transacted or accumulated in the account originate from or are connected to a crime other than the crime of money laundering or terrorist financing or a fiscal crime. The indicated 'blocking' procedures are described in detail in the mentioned articles, but it is worth noting the wording of some of the legal institutions described in the law.

[57] *Fight against money laundering and terrorist financing…*

Determining the status of a digital artefact in criminal proceedings

In the event that any cryptocurrency comes into the interest of a law enforcement agency, its technical and legal status must be established. This is because important issues depend on this, such as the possibility of fulfilling the elements of a crime through the mere possession or issuance of tokens (e.g. prohibited tokenisation of securities), the way in which actual power over digital property is taken (whether the crypto-assets are placed on a public or private blockchain, or perhaps have nothing to do with blockchain techniques at all), the possibility of searching for traces of the crime committed (location of the server). Determining the aforementioned status is not always easy, and although the largest number of cases involve bitcoin or similar altcoins (ethereum or litecoin), there are situations where it is quite challenging to establish all the characteristics of the token. This has happened in the case of parlours running illegal gambling games, where players purchased gaming points for money in the form of a digital representation of their value in a QR code. The research shows that Polish crypto-asset users have sophisticated tokens in their portfolios, the issuance of which on the domestic capital market is subject to numerous legal requirements, subject to supervision by regulatory authorities and often even prohibited. These include such digital assets specific to the DeFi market as PAXGOLD, USDT, COMP[58]. The majority of users further declared that they had used or invested in equity tokens similar to stocks or bonds, derivatives in the form of crypto-assets, and almost half held tokens resembling options, futures or swaps[59].

The centralised and decentralised crypto-asset market is growing and public authorities, not only in Poland but also globally, have great difficulty in navigating it and enforcing the legal obligations imposed on participants in this market. It is to be presumed that criminal acts in the form of financial embezzlement or money laundering carried out in an environment such as DeFi too often remain beyond any control of states and governments. The authors of this article are not aware of a case in which Polish law enforcement or capital market supervisory authorities have carried out sophisticated fraud-related activities in the decentralised finance market. In contrast, the US financial market regulator, The Securities and Exchange Commission (SEC), has been effective in this area. In August

[58] P. Opitek, *Funkcjonowanie instrumentów finansowych…*, p. 235.

[59] Ibid.

2021, it charged the defendants with conducting an unregistered sale of securities to the SEC for more than $30 million using smart contracts and decentralised finance technology, as well as misleading investors about the actual profitability of the products offered. The defendants operated as a company called Blockchain Credit Partners and issued and offered for sale on the DeFi Money Market platform two types of tokens called mTokens with significant returns and DMG tokens giving voting rights in a virtual company (DAO)[60]. The Commodity Futures Trading Commission (CFTC) regulatory agency in March 2023 accused the holding company Binance, the world's largest virtual currency trading platform, and its director Changpeng Zhao of offering digital token derivatives for sale to US citizens without the legally required registration with the CFTC in a civil action in federal court[61].

Another example of the variety of 'digital values' found in the virtual world is computer games, especially those played online. Artefacts in games can represent human characters, weapons (swords, guns), ammunition, parts of armour, objects hiding other things (chests, safes) or more abstract elements whose function represents some kind of value to the users of a given platform. Situations have been known where in-game artefacts have been used for money laundering[62] or have been the subject of assassination[63] or activities in support of terrorism. Where it is suspected that they fall within the modus operandi of the perpetrator of a crime, the legal status of such 'values' must be carefully established. An example of the importance

[60] *SEC Charges Decentralized Finance Lender and Top Executives for Raising $30 Million Through Fraudulent Offerings*, U.S. Securities and Exchange Commission, https://www.sec.gov/news/press-release/2021-145 [accessed: 24 III 2023].

[61] *CFTC Charges Binance and Its Founder, Changpeng Zhao, with Willful Evasion of Federal Law and Operating an Illegal Digital Asset Derivatives Exchange*, CFTC, 27 III 2023, https://www.cftc.gov/PressRoom/PressReleases/8680-23 [accessed: 5 IV 2023].

[62] P. Opitek, *Kryptowaluty w aspekcie czynności dochodzeniowo-śledczych Policji* (Eng. Cryptocurrencies in the aspect of police investigative activities), "Przegląd Policyjny" 2017, no. 2, p. 150. https://doi.org/10.5604/01.3001.0013.6082.

[63] In the verdict of the District Court for Kraków-Krowodrza, II Criminal Division, of 3 August 2012, ref. no. II Ka 776/11/K, the defendant was convicted for the fact that on 6 February 2011 in the city of K., in order to gain financial benefit, without authorisation, he influenced the transfer of information by breaking electronic security in such a way that he changed the access password to the e-mail box named "...@poczta.onet.pl" belonging to T. K., and took over his character in the game "Metin 2", named "Joker 78", thus leading T. K. to a disadvantageous dispossession of property in the amount of at least PLN 500, i.e. an act under Article 287 § 1 of the Criminal Code.

of properly assessing the nature of an artefact, and how a mistake can discredit a prosecutor, is the case concerning so-called 'skins' that is pending before the court. The defendant was found guilty by the District Court in Przasnysz[64] of an offence under Article 107 of the Fiscal Penal Code[65] in conjunction with Article 29a(1) and in connection with Article 2(1) of the *Act of 19 November 2009 on gambling games* (in the wording prior to 1 April 2017), consisting in the fact that between 2016 and 2017 he organised gambling games of a random nature on online platforms, in which the object of the winnings were the aforementioned skins. They are a type of feature used in the game C*ounter-Strike: Global Offensive* in the form of various types of weapons that the player can rent and in this way change the appearance of the artefacts used in the game[66]. Individuals who participated in the draw arranged by the accused submitted their skins to a virtual drum. These were then mixed and, depending on the rules of the platform in question, a randomly selected participant received the highest number of skins and the accused received a commission for organising the game.

In the wording prior to 1 April 2017, Article 2(1) of the Act on gambling games provided that (...) *games of chance are games, including those arranged via the Internet, for winnings in cash or in kind, the outcome of which depends in particular on chance*. Thus, the condition for the perpetrator to fulfil the elements of the offence was the court's recognition that the skin constitutes money or an object[67]. In the appeal filed against the conviction, the defendant's defence counsel argued that skin cannot be treated as money, as it is not issued by the National Bank of Poland, nor is it a tangible object, but only a piece of programming code, and therefore does not meet the definition of a thing under Article 45 of the Civil Code[68]. The Regional Court in Ostrołęka, 2nd Criminal Division[69], shared the argumentation

[64] Case file of the District Court in Przasnysz, 2nd Criminal Division, ref. no. II K 608/18.

[65] *Act of 10 September 1999 Fiscal Penal Code*.

[66] https://counterstrike.fandom.com/wiki/Skins [accessed: 17 II 2022].

[67] The charge in the indictment and judgment of the court of first instance states that "so-called skins - virtual keys that have a real monetary value in the real world and allow access to virtual weapons of varying strengths and attachments used in the battles of the 3D arcade game Counter-Strike Global Offensive (CS: GO for short) offered on the STEAM community platform owned by Valve Corporation based in Bellevue, Washington, USA" are at risk.

[68] *Act of 23 April 1964 – Civil Code*.

[69] Ref. no.: II Ka 40/20.

contained in the appeal and acquitted the accused of the alleged act in a judgement of 27 August 2020. In the justification for the verdict, the court indicated that the provisions of Article 2(1)(1) of the Act cannot be interpreted broadly and by analogy, and it is clear that skins do not have the status of things or objects, as they are virtual values[70].

In determining the legal status of a token, it is of fundamental importance to answer the question whether it constitutes a virtual currency, the legal definition of which is provided in Article 2(2)(26) of the AML/CFT Act. Carrying out such an assessment and providing an unambiguous answer as to whether a given asset is subject to the regime of the AML Act may prove very difficult, inter alia, because the aforementioned definition is very capacious and the phrases used therein are vague[71]. The classification of tokens as virtual currencies means that law enforcement authorities can enforce a number of obligations on an obliged institution dealing in such currency to provide information on suspicious persons and transactions. At the request of a law enforcement agency, the obliged institution should provide full data obtained during the first and subsequent client verification (KYC) and histories of the transactions performed by the client, news about possible reporting alerts to the GIFI on suspicious operations or a database of IP numbers that were used to commit a crime. Entities engaged in the business of providing services for exchanges between virtual currencies and means of payment or conversions between tokens themselves are furthermore required to submit, upon request by law enforcement authorities, the documentation set out in the AML Act, including, inter alia, the risk estimation procedure adopted and the attribution of the level of risk to a specific client[72]. A discussion of all

[70] Under the current state of the law, such behaviour would constitute an offence under Article 2(5) as amended by the *Act of 15 December 2016 amending the Act on gambling games and certain other acts* (Journal of Laws 2017, item 88), which reads: "Games on slot machines are also games on mechanical, electromechanical or electronic devices, including computer games, as well as games corresponding to the rules of slot machine games arranged via the Internet organised for commercial purposes, in which the player does not have the possibility of obtaining a prize in cash or in kind, but the game is of a random nature".

[71] For a detailed discussion of the various components of the definition of the term "virtual currencies", see: G. Ocieczek, P. Opitek, *Analiza definicji walut wirtualnych z ustawy*..., pp. 122–139.

[72] For a detailed discussion of the sources of evidence that law enforcement agencies may use in litigation and operational activities related to virtual currencies, see: J. Skała, *Uzyskiwanie przez prokuratora informacji i danych*...

the means and sources of evidence that can be used in a cryptocurrency investigation is beyond the scope of this paper, but what is certain is that the AML gives law enforcement agencies ample scope for action, which is poorly known among officers and too rarely used by them.

Operational work in the fight against cryptocurrency crime

Experience gained as a prosecutor shows that covert non-prosecution activities are an essential element in the successful fight against cryptocurrency crime. This is the case for several reasons. The perpetrators who commit such criminal acts are very cautious and usually operate in an environment of people at least as hermetic as organised drug trafficking groups or football hooligans. This is because the logistical facilities for trading cryptocurrencies are accessed remotely, so those using them operate in a virtual world, access to which may be irretrievably lost with the closing of their laptop matrix. This is one of the reasons why, in recent years, the methodology for conducting searches of places occupied by suspects and securing electronic equipment belonging to them has been re-evaluated. Previously, the indisputable rule was that an officer participating in a search which revealed a working computer unit should not search the memory of the device himself, as he would alter the data record on the laptop, which would negatively affect the evidentiary value of the traces obtained from it. Today, a search of a flat or an arrest of a person is not infrequently preceded by operational activities aimed at revealing and seizing the perpetrator's open computer at the time of their execution. This provides the opportunity to gain access to a lot of valuable information and data stored on the device's memory or the cloud resources to which it connects. In this way, it is possible to seize digital assets as collateral, obtain passwords to access applications used to commit crimes or to access an account on a cryptocurrency exchange, check which websites and web services were used by the perpetrator, find out the content of their instant messaging conversations. If the computer is shut down, it is likely that a computer forensics expert will not be able to break the password securing access to the device, and even if they do, data stored in elusive RAM or access to artefacts stored by the offender on other servers will be lost.

Actions taken to seize an open computer may range from deception (e.g. entering a flat "as a postman"), through a forensic trap (provoking a criminal to open a laptop in a public place in order to seize it), to the use of advanced operational and reconnaissance activities. This can be preceded by covert surveillance of people and places, property intelligence or cooperation with a network service provider to which the suspect is a subscriber. Operational control, controlled purchase and controlled delivery are also involved. There have been cases where law enforcement agencies have purchased bitcoins, set up their own darkmarket accounts and purchased drugs offered on the platform in order to establish the channels of transmission of prohibited substances, the method of their delivery and to obtain a quasi-forensic opinion on physicochemical testing, as well as to establish what drugs they are dealing with under the Act on counteracting drug addiction[73].

The effectiveness of covert operations in cyberspace aimed at combating cryptocurrency-related crime is confirmed by the experience of the US services. This includes the use of an undercover officer operating on the internet or determining the location and shutting down servers storing illegal content. The physical seizure of a server is a major success, as it contains traces that provide law enforcement agencies with valuable information on hundreds of individuals conducting illegal activities using IT infrastructure. However, such a takeover is no small challenge and is usually only possible through international cooperation. On 28 February 2023, German and Ukrainian police, with the support of Europol, Dutch police and the FBI, arrested members of a criminal group responsible for ransomware cyber attacks based on DoppelPaymer and Dridex software and targeting the critical infrastructure of private companies. The ransomware was distributed through various channels, including phishing and documents containing malicious JavaScript or VBScript code attached to spam emails. One of the most serious attacks was launched against the University Hospital in Düsseldorf, and in the US, victims paid at least €40 million in cryptocurrency to decrypt their data[74].

[73] *Act of 29 July 2005 on counteracting drug addiction.*

[74] *Germany and Ukraine hit two high-value ransomware targets*, Europol, https://www.europol.europa.eu/media-press/newsroom/news/germany-and-ukraine-hit-two-high-value-ransomware-targets [accessed: 6 IV 2023]. Elissa Slotkin, President of Intelligence and Counterintelligence for the US Congress, during testimony before Congress in 2021, spoke of the ransomware terrorist attacks in the US at the time, "which struck at

The characteristics of ransomware are likened to terrorist attacks in that they pose a serious threat to national security. Like terrorism, ransomware focuses on soft targets such as civilian critical infrastructure, but unlike terrorism it is primarily motivated by financial considerations[75]. However, it is sometimes difficult to draw a clear line between the two cyber threats. The North Korean government, for example, has been responsible for many major ransomware attacks on critical infrastructure around the world. In 2021, the US Department of Justice announced the indictment of three North Korean government officials suspected of carrying out some of the most dangerous cyber attacks, including WannaCry 2.0 (the ransom for decrypting data was paid in cryptocurrency), the hacking of the Sony Pictures database and the Bank of Bangladesh. The indictment alleges that the hackers are members of the Korean military intelligence service, linked to the hacker group called Lazarus, which has been involved in cyber operations for years[76]. The Korean lead was also attributed to a sophisticated and camouflaged cyber-attack on the Polish Financial Supervisory Authority's ICT system carried out in 2021. Although all the attackers' objectives are still not public today, one of them was to penetrate the trusted internal network of the banking systems, take control of the computers located there and establish communication between the victim's systems and the infrastructure controlled by the criminals[77].

---

the heart of everyday life in America, from gas pipelines and meat and plant processing to the operation of schools and hospitals", and at her meeting with constituents, "the first questions from farmers were about cyber attacks, cryptocurrency and what the government has done to protect them". See: *Statement of Chairwoman Elissa Slotkin*, p. 2.

[75] *Ransomware Attacks on Critical Infrastructure Sectors*, U.S. Department of Homeland Security, https://www.dhs.gov/sites/default/files/2022-09/Ransomware%20Attacks%20.pdf, p. i [accessed: 11 V 2023].

[76] M. Dugas, *The Latest North Korea Cyber Indictment Should Serve as a Model*, Just Security, 24 II 2021, https://www.justsecurity.org/74930/the-latest-north-korea-cyber-indictment-should-serve-as-a-model/ [accessed: 11 V 2023]. The indictment found that North Korea earned a total of more than $1.3 billion (the country's GDP is estimated at just $28 billion) through cyber-terrorism, i.e. bank hacking, cryptocurrency theft. The United Nations, meanwhile, estimated that in 2019 North Korea raised more than $2 billion in illicit financing from its cyber operations to fund its weapons programme.

[77] For more on the attack see: A. Maciąg, I. Tarnowski, *Atak teleinformatyczny na polski sektor finansowy* (Eng. ICT attack on the Polish financial sector), Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/ [accessed: 11 V 2023].

Effective action against organised crime groups operating on the Internet requires the formation of operational teams made up of representatives of various law enforcement services, and often international cooperation. In the United States, a special unit called J-CODE (Joint Criminal Opioid and Darknet Enforcement) has been created to combat cybercriminals, which is made up of seven institutions, including the FBI, HSI, the Department of Justice and The Postal Inspection Service. It follows that border guards, customs inspectors and the postal service have an invaluable role to play in combating the virtual trade in prohibited substances, as the delivery of goods ordered via the Internet is the point at which the virtual world of criminals meets the material world, and the resulting situation makes it possible not only to seize the illegal goods, but also to take other measures to identify and apprehend the criminals[78]. The state of affairs observed in one of the national services, in which the division dealing with asset recovery was separated from the units carrying out operational and exploratory and investigative activities, is therefore inadvisable. Effective combating of cryptocurrency crime, including the realisation of property seizure on digital tokens, requires constant cooperation and rapid flow of information between persons dealing with various aspects of combating crime, i.e. operational work, investigative work, asset recovery. *A contrario*, a person involved in the recovery of criminal assets will have serious difficulties in carrying out this task in relation to crypto-assets if he or she is not at all involved in the procedural activities of searching or interviewing a witness or does not have access to ongoing information from non-procedural arrangements.

The problem of the application of operational control in the form of obtaining and recording data contained in IT data carriers, telecommunication terminal devices, IT and ICT systems[79], i.e. control of the terminal device, is interesting. It can be stated with certainty that today's fight against cybercrime requires the use of such a method of operational work, as criminals mainly contact each other via devices that form the Internet. The law explicitly allows the obtaining of data recorded on the device's disk as one of the forms of operational control.

[78] P. Opitek, *Biegły z zakresu kryptowalut w sprawach karnych* ((Eng. Cryptocurrency expert in criminal cases), in: *Wokół kryminalistyki. Nauka i praktyka. Księga pamiątkowa dedykowana Profesorowi Tadeuszowi Widle*, D. Zienkiewicz (ed.), Toruń 2021, p. 434.

[79] This method of control is provided for in the laws governing the work of the police and the nine services.

At present, the efforts of the Police, as well as the Internal Security Agency and the Central Anticorruption Bureau, should focus on increasing the technical capabilities for operational control of the memory of a laptop, phone, modem or router in a passive manner, i.e. without modifying the digital traces present in the controlled object. Ideally, operational control of a hardware cryptocurrency wallet would be included, although technically this is a difficult task to achieve. This would make it possible, among other things, to know the entire transaction history, the current balance of bitcoins contained in the device or even the realisation of a property seizure on the disclosed cryptocurrencies[80]. Similar information would be provided by subjecting to control in the form of obtaining and recording the content of correspondence, including correspondence conducted via electronic means of communication, the so-called 'figurehead' account established on the exchange, to which additional data is sent, such as codes for withdrawing money at an ATM after the conversion of crypto into fiat money. It is true that on the basis of a letter or an order of the public prosecutor, the exchange administrator can be requested to submit the aforementioned data, but taking control of the account would help in obtaining up-to-date information and planning in advance the execution of tasks. Looking more broadly, it makes sense to introduce a new method of operational control in the form of uninterrupted ("on-the-fly") tracking of transfers of non-cash money, other means of payment or crypto-assets by establishing a new statutory form of operational work[81].

Traditional methods and forms of operational work are applied in the fight against cryptocurrency crime. For example, a police or secret service officer operating on an online platform under the guise of its real user is given the status of an undercover officer, with all the consequences this entails. Thus, an operational combination takes place in the form of, for example, the controlled purchase of drugs by an agent, followed

[80] The statement that the wallet contains units of virtual currency is a mental shortcut. This is because, in reality, the wallet contains the digital data to manage the altcoin units in the form of a so-called public and private key, but the tokens themselves are mapped to a ledger called a blockchain in the form of a digital data record.

[81] See in more detail: P. Opitek, *Kontrola transferów pieniądza bezgotówkowego w czasie rzeczywistym jako nowa forma czynności operacyjno-rozpoznawczych na przykładzie ustawy o Agencji Bezpieczeństwa Wewnętrznego (postulaty de lege ferenda)* ((Eng. Real-time control of non-cash money transfers as a new form of operational and reconnaissance activities on the example of the law on the Internal Security Agency (de lege ferenda postulates)), "Prokuratura i Prawo" 2021, no. 2, pp. 154–175.

by a controlled delivery. The aim is to unravel the environment of those involved in the online trafficking of illicit substances, to establish how the drugs are shipped and delivered to the customer, the chemical composition of the substances and how the buyer and seller communicate. The cryptocurrencies used to pay for the establishment of an account or to pay the price of goods will come from the service's operational fund, and the operations carried out with them are documented in detail until the costs of the actions taken are fully accounted for. These operations must be properly documented in the form of notes of the activities carried out at each stage of the special operation, accompanied by screen shots, and preferably a video recording, documenting what the undercover officer is doing in cyberspace. Snapshots of instant messaging conversations conducted by an agent with lawbreakers are important, as this is most often the form in which cybercriminals pass information to each other. Documents from the activities carried out, which constitute evidence of a suspected crime, should be made available in due course by the Chief of Police or the Head of a special service for criminal proceedings.

Investigation into cryptocurrency crime

2022 was a record year in terms of the number of trainings and conferences on virtual currencies organised by Polish law enforcement agencies. Most attention was devoted to the topic of property seizure on cryptocurrencies. It turns out, however, that the strictly procedural implementation of the security itself (i.e. the issuance of relevant decisions by the prosecutor) is easier than the disclosure of criminally derived bitcoins and the actual taking of their self-possession. Investigating cryptocurrency crime in cases of high gravity or where there is a real possibility of prosecuting specific individuals is an arduous detection process associated with the collection of extensive evidence. The success of this investigation depends on the knowledge and determination of those conducting it, and sometimes it is also determined by luck.

The criminal proceedings in question require skills in collecting digital traces and evidence not only from Polish and foreign providers of network services, such as cryptocurrency exchanges and bureaux de change, but also from Internet providers, telecommunications operators or financial institutions, led by banks. Administrators of industrial monitoring

systems (recordings of ATM withdrawals), national road administrators (registration of vehicle movements), carriers in air transport, entities operating the BLIK fast payments or administrators of online shopping platforms may also have valuable information for the investigation. Nevertheless, cryptocurrency exchanges remain the source of the largest amount of data. They can be requested to release information on:

- personal data of the exchange user, which is collected during the KYC procedure and can be changed during the customer's use of the platform (name, surname, date of birth, personal identification number, telephone number, home address, etc.);
- a scan of documents confirming his or her identity (identity card, driving licence, passport, etc.) and other documents submitted by the client in the course of using the services offered by the exchange (e.g. declaration of the source of funds invested);
- information on transactions carried out in virtual currencies and fiat money (list of transactions, their date, value of operations, beneficiary of funds received);
- the date of access to the exchange system by a potential perpetrator (submission of a summary of logins to the platform by persons of interest to law enforcement authorities, including any attributes in the form of IP addresses of ports with an indication of the exact time of log-in, BTS location, IMEI/MAC numbers of the device initiating Internet connections). In addition, check whether a new trusted device has been added for logins to the exchange account and the details of the devices from which logins occurred (operating system, system version, screen resolution, browser version);
- the history of the exchange user's account (codes sent to carry out ATM transactions, information and warnings received from the exchange administrator);
- information on whether transaction anomalies occurred during the course of the business relationship with the customer (e.g. a transaction was not completed because funds came from an address deemed to be suspicious, bank accounts or virtual currency addresses were blocked, transactions were stopped - if so, when and why);
- records of telephone or video conference calls made between exchange staff and the suspected person;

– reporting by the obliged institution to the GIFI, the prosecutor's office or another public authority on an exchange user (when and for what reason the report was issued);
– withdrawals of 'stolen' funds, notably the destination wallet address to which the funds were withdrawn and the transaction identifier (transaction *hash*).

The procedures and extent of data (e.g. logs) and information (transaction history) that can be obtained from exchanges depend on several factors, including the location of the exchange, the type and amount of data left on the platform by its user or the stage of the criminal proceedings. Law enforcement authorities and online service providers have developed a number of rules of cooperation. Sometimes obtaining the content requested by the prosecutor is done on the basis of a pleading. The request should indicate the officer and the unit conducting the case, the reference number of the proceedings, contain a brief description of the case indicating what offence the requested person is charged with. It should be sent electronically to the official contact point of the exchange, information about which is usually held by law enforcement authorities. The letter should be written in English or in the language of the country where the exchange operates. The main document should be a scan of the official letter and the attachment with the details should be sent in editable form so that it is possible to copy the data (e.g. cryptocurrency addresses) and further work on them. If the matter is of an urgent nature, this should be made clear in the letter. Importantly, as some exchanges inform their customers of an investigation against them, it is possible to stipulate in the request that the network service provider should refrain from doing so, and to justify this request.

There are, however, jurisdictions where obtaining information other than metadata (non-content data) will be conditional on a warrant being issued by the locally competent court. In such cases, requests for international legal assistance are made on the basis of agreements between sovereign states, which in practice significantly prolongs the process of collecting artefacts. This includes the United States, the territory with the largest number of network service provider companies. In Europe, the European Investigation Order commonly used by police officers and prosecutors is proving helpful. A person dealing with cryptocurrency crime must therefore be familiar with both the legal and practical aspects

of obtaining evidence, as the procedure involved depends on several factors:

- the company's headquarters and the location of the data server;
- the type of data in question: content data or non-content data (the latter are often made available in a deformalised manner);
- the procedure followed: "freezing" the data pending authorisation of its transfer, the procedure for obtaining the relevant data or the urgent obtaining of data in emergency cases);
- the internal policy of the entity obliged to provide information and data management.

Ultimately, if an exchange or other digital platform refuses to comply with the legally prescribed procedure for the release of data and information, or makes it significantly more difficult, one may consider seizing its server in order to extract the necessary artefacts or check that they have not been removed from it. Sometimes the vision of the inevitability of the seizure of the infrastructure leads to an opening for cooperation on the part of the service provider. Such actions are not possible with respect to darkmarket actors, where the location of their infrastructure is unknown, and in countries that do not cooperate with international legal assistance.

Another important piece of information for an investigation with a cryptocurrency thread is recorded on the electronic equipment used by end users of the Bitcoin protocol, most notably their phones and computers. There are artefacts on the secured evidentiary media to determine whether its user has used virtual currencies, connected to sites designed to handle them, and there may be traces or information (passwords, logins, etc.) in the computer's memory, including operational RAM, to authorise access to databases, i.e. applications, cloud resources or cryptocurrency wallets. If any system reveals data stating digital tokens and belonging to a suspect, it must be secured immediately for an ongoing investigation. To this end, the authors postulate that an operational and investigative group should be created in one of the leading special services in the area of the economic security of the Republic of Poland (e.g. the ISA) or the Police, consisting of officers who will have competences related to securing bitcoins and have the technological background to take possession of them. This refers to such skills as the visual inspection or search of the computer evidence system of the computer at the place of its disclosure, the handling of the electronic purse belonging to the perpetrators of the criminal act, but also to the possession by the formations fighting crime of their own hardware

wallet for accepting cryptocurrency, recognising the types of digital assets, generating addresses for them. Particularly important is the institution of property seizure on cryptocurrencies, as referred to in Article 291 § 1 of the Code of Criminal Procedure et seq. In Poland, such collateral has already been implemented for several years (the first one was executed in 2017), and the number is increasing every year. In order to seize bitcoin, police officers most often cooperated with online exchanges, which first froze the funds in the suspect's account and then created a special account for the prosecution and stored the object of the security there. There is also at least one known case of police officers generating a paper wallet, but it is most secure and practical for the services to have a hardware wallet such as Ledger or Trezor. The most difficult task in the course of operational or investigative activities seems to be to determine where the virtual currencies from the investigation are located and then to gain actual access to them with the possibility of transferring them to an address managed by the investigator. There are known cases in which, on the basis of criminal analysis of cryptocurrency transfers, addresses for storing significant amounts of tokens originating from crime, e.g. hacks on exchanges, were established, but they were not linked to any public Internet platforms, there were no findings regarding the persons managing these addresses and, consequently, the possibility of taking control over virtual funds. In such a situation, the only thing left to do is to flag such an address and thus monitor it in anticipation of the funds accumulated therein being transferred by someone to another, less anonymous address.

For bitcoin, which has already been seized by law enforcement, there are legal and factual difficulties with its storage. These are due to the fact that the price of virtual currencies is very liquid and subject to large exchange rate variations in short intervals, and that each wallet is vulnerable to hacking, mechanical or IT failure, and human error related to their handling may occur. In addition, Polish courts are not ready to seize cryptocurrencies that would be handed over with an indictment. A practical solution to these problems is the sale of secured assets during the investigation under Article 232 § 1 of the Code of Criminal Procedure. in conjunction with Article 236a of the Code of Criminal Procedure. They stipulate that items the storage of which would be connected with excessive difficulties or would cause a significant reduction in the value of the property may be sold according to the procedure specified for the competent authorities of the enforcement proceedings, and this

provision applies accordingly to digital tokens constituting IT data. The sale of the thing takes place in accordance with the provisions on enforcement proceedings in administration or those contained in the Code of Civil Procedure, depending on what was the basis for the seizure of the funds (Article 291 § 1, points 1-5 of the Code of Criminal Procedure). Another legal problem concerns the content of Article 295 § 1 of the Code of Criminal Procedure, which refers to movable property and bitcoin is not a thing within the meaning of Article 45 of the Civil Code. However, in practice, the institution of temporary seizure of movable property has already been effectively applied to virtual currencies and, moreover, Article 236b of the Code of Criminal Procedure, i.e. recognition of cryptocurrency as funds accumulated in an account and issuance of a decision on material evidence, may prove to be a solution in such a case.

Digital evidence relating to virtual currencies and, more generally, to the cybercrime committed should be properly collected, secured and then used in the investigation. The presentation of digital evidence in the course of criminal proceedings is based on the rule that it represents not only what can be seen, but also has metadata. This problem arose in the already mentioned case of the District Court in Przasnysz, in which the prosecutor, as evidence of the appearance and functioning of websites dedicated to skins, attached printouts of such websites to the indictment. In the pleading, the accused's defence counsel pointed out the unsuitability of evidence in the form of paper printouts of websites, which contained information which, according to the public prosecutor, constituted evidence of the commission of the offence charged against the accused. The accused's defence counsel argued that:

> (...) in the factual situation under examination, it is clearly the case that the taking of evidence indicated in the request for evidence cannot lead to the establishment of the circumstance indicated therein. The website is interactive in nature and a mere 'screenshot', printed on a piece of paper, does not reflect its essence and functioning. In the view of the defence counsel, the evidence of the circumstances referred to in the contested printouts of the websites should be carried out in such a way that the prosecutor, during the course of the evidence, reconstructs the functioning of the established websites. This is certainly technically possible (if only by saving the pages to

> a permanent medium), but undoubtedly requires a little more effort on the part of the prosecutor[82].

The court shared the position of the defence and this, as well as many other mistakes made in the investigation, resulted in the acquittal of the accused. It follows that police officers should have had the knowledge, skills and due software for interactive visual inspection or web searches[83]. Particularly the latter activity, i.e. a cyber search, could be performed more often in the course of procedural activities, as it allows to obtain information and secure the most important evidence for the investigation, and yet the referents of criminal cases are either afraid to carry out such, in their opinion, difficult activities, or they do it without due diligence in the form of taking an official note, despite the fact that Article 143 § 1 (1) and (6) of the Code of Criminal Procedure requires a record to be made in this case.

Conclusions

The analysis of selected aspects of crime involving virtual currencies carried out leads to some basic conclusions. The role of cryptocurrencies in the activities of professional capital market players is steadily growing and more and more people are using this type of property. Cryptocurrencies are also used by criminals and the number of criminal cases related to cryptocurrency crime is increasing every year. Reports from public institutions and the authors' experience show that illegal activities involving crypto infrastructure can involve serious criminal acts harming the economic foundations of the state, serve to sponsor terrorism and espionage activities, corruption, circumvent sanctions, and therefore affect Poland's security and reputation internationally. This leads to the simple conclusion that law enforcement agencies, including the relevant special services, must have multifaceted capabilities (appropriately prepared people and logistical facilities) to work with cryptocurrencies, in both general (working with digital evidence, learning the essence of blockchain technology) and specific (the ability to use virtual wallets, redefining

[82] Case file of the District Court in Przasnysz, 2nd Criminal Division, ref. no. II K 608/18.

[83] See: P. Opitek, *Przeszukanie na odległość jako czynność procesowa (art. 236a k.p.k.)* (Eng. Remote search as a procedural act (Article 236a of the Code of Criminal Procedure)), "Prokuratura i Prawo" 2022, no. 9, pp. 100–128.

the work of an undercover officer in cyberspace, and perhaps creating an operational fund in the form of cryptoassets). It is obvious that not every officer of such an institution will be a specialist in cryptocurrencies, nevertheless they should immediately receive professional support when topics related to digital tokens arise in their proceedings. Furthermore, given that it is not always possible for a state security leader to cooperate with other law enforcement agencies specialised in fighting cybercrime, it is all the more reason for such an elite formation to have its own group (structure) of individuals specialised in the implementation of procedural and non-procedural activities related to cryptocurrencies (e.g. property seizure on bitcoin).

Looking more broadly, the Polish virtual currency market should be monitored for possible money laundering using binary values or circumventing sanctions imposed on Belarus and Russia. Instruments useful for the aforementioned tasks are offered by the AML/CFT Act. All the objectives regarding the minimisation of threats based on crypto-assets cannot be achieved without institutional cooperation between the ISA, the Public Prosecutor's Office, the GIFI and the FSA, as each of these institutions has specific legal tools and factual capabilities assigned only to it. Only their synergy offers the possibility to build an effective and comprehensive AML/CFT policy.

An analysis of the topic of cryptocurrencies has shown that they have also been used to support terrorist activities of a different nature - sponsorship of terrorist organisations using online crowdfunding, direct donations to a specific individual helping to organise or motivated to organise attacks, or cyber attacks targeting the ICT infrastructure of areas critical to the functioning of the state. According to information provided by an HSI representative, the number of criminal investigations involving cryptocurrencies in the US has increased from one in 2011 to more than 604 investigations in 2021. During this time, HSI has confiscated bitcoins and altcoins worth the equivalent of $79,825,606.65. This illustrates the increasing reliance of the perpetrators of the highest gravity of illegal acts on crypto-assets, and therefore implies the need for law enforcement agencies to gain competence to combat this type of terrorist financing[84]. And although the main sources of this financing still rely on traditional

[84] *Statement of John Eisert...*, pp. 14–16.

financial institutions[85] (it is estimated that cryptocurrency terrorist financing currently generates only 1 per cent of such transactions[86]), the problem is bound to grow. Perpetrators' modus operandi and approach to the virtual world are changing and evolving towards the most favourable solutions for them. Thanks to the successful actions of the US services against online platforms described in the article, the Izz ad-Din al-Qassam Brigades declared in April 2023 that it was suspending the collection of donations using bitcoin, citing an increase in 'hostile' activity towards donors. *This is out of concern for the safety of donors and to spare them any harm,* the Hamas announcement read[87]. At the same time they called for (...) *continued donations to Kassam and the resistance by all available means*[88].

Poland has been the subject of terrorist activities using the Internet infrastructure and cryptocurrencies. These include ransomware attacks targeting Poland or advertisements posted on the Darknet, which operates with bitcoin, encouraging the assassination of key named Polish politicians. Cryptocurrency issues are also linked to the activities of hostile intelligence organisations targeting Poland's security. It is therefore necessary for the most important state security services to increase their competence in the field of activity in the virtual world, the implementation of cyber operations and countering hostile IT attacks. This includes the ability to investigate cryptocurrency transfers, to secure such assets, but also to actively use them for their own purposes.

Bibliography

Chainalysis, *The 2022 Crypto Crime Report,* February 2022.

[85] *Risk Assessment. 2022 National Terrorist Financing*...

[86] *Statement of Ranking Member August Pfluger*, in: *Hearing before the Subcommittee on Intelligence and Counterterrorism*..., p. 3.

[87] N. Al-Mughrabi, *Hamas armed wing announces suspension of bitcoin fundraising,* Reuters, 28 IV 2023, https://www.reuters.com/world/middle-east/hamas-armed-wing-announces-suspension-bitcoin-fundraising-2023-04-28/ [accessed: 9 V 2023]; *Hamas armed wing to stop crypto fundraising over 'hostility' against donors,* i24NEWS, 30 IV 2023, https://www.i24news.tv/en/news/middle-east/palestinian-territories/1682688395-hamas-armed-wing-to-stop-crypto-fundraising-citing-hostility-against-donors [accessed: 9 V 2023].

[88] Ibid.

Ocieczek G., Opitek P., *Analiza definicji walut wirtualnych z ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (Eng. Analysis of the definition of virtual currencies from the Act of 1 March 2018 on the prevention of money laundering and terrorist financing), "Consilium Iuridicum" 2022, no. 3–4, pp. 122–139.

Opitek P., *Biegły z zakresu kryptowalut w sprawach karnych* (Eng. Cryptocurrency expert in criminal cases), in: *Wokół kryminalistyki. Nauka i praktyka. Księga pamiątkowa dedykowana Profesorowi Tadeuszowi Widle*, D. Zienkiewicz (ed.), Toruń 2021, pp. 413–447.

Opitek P., *Funkcjonowanie instrumentów finansowych w oparciu o technologię blockchain* (Eng. Functioning of financial instruments based on blockchain technology), Łódź 2022.

Opitek P., *Kontrola transferów pieniądza bezgotówkowego w czasie rzeczywistym jako nowa forma czynności operacyjno-rozpoznawczych na przykładzie ustawy o Agencji Bezpieczeństwa Wewnętrznego (postulaty de lege ferenda)* (Eng. Real-time control of non-cash money transfers as a new form of operational and reconnaissance activities on the example of the law on the Internal Security Agency (de lege ferenda postulates)), "Prokuratura i Prawo" 2021, no. 2, pp. 154–175.

Opitek P., *Kryptowaluty w aspekcie czynności dochodzeniowo-śledczych Policji* (Eng. Cryptocurrencies in the aspect of police investigative activities), "Przegląd Policyjny" 2017, no. 2, pp. 138–158. https://doi.org/10.5604/01.3001.0013.6082.

Opitek P., *Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML* (Eng. Anti-money laundering using virtual currencies in light of national and international AML regulations), "Prokuratura i Prawo" 2020, no. 12, pp. 41–70, Lex, https://sip.lex.pl/komentarze-i-publikacje/artykuly/przeciwdzialanie-praniu-pieniedzy-z-wykorzystaniem-walut-151383722.

Opitek P., *Przeszukanie na odległość jako czynność procesowa (art. 236a k.p.k.)* (Eng. Remote search as a procedural act (Article 236a of the Code of Criminal Procedure)), "Prokuratura i Prawo" 2022, no. 9, pp. 100–128.

Opitek P., *Wykorzystanie walut i serwisów wirtualnych do prania pieniędzy i finasowania terroryzmu* (Eng. Use of virtual currencies and services for money laundering and terrorist financing), Warszawa 2019 (diploma thesis written during post-graduate studies at the Warsaw School of Economics, unpublished, in the author's possession).

Prawo cywilne – część ogólna (Eng. Civil law - general part), M. Safjan (ed.), series: System Prawa Prywatnego, vol. 1, Warszawa 2007.

Przewłoka E., *Metodyka podstawowych czynności realizowanych przez funkcjonariusza Policji i związanych z przestępstwem „kradzieży" waluty wirtualnej* (Eng. Methodology of basic actions carried out by a police officer and related to the crime of "theft" of virtual currency), Bydgoszcz 2023 (Police internal methodology, in the author's posession).

Skała J., *Uzyskiwanie przez prokuratora informacji i danych od instytucji obowiązanych na podstawie ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (Eng. Obtaining information and data by the public prosecutor from obliged institutions under the Act of 1 March 2018 on the prevention of money laundering and terrorist financing), "Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2022, n. 3, pp. 83–100. https://doi.org/10.53024/4.3.47.2022.

Internet sources

Al-Mughrabi N., *Hamas armed wing announces suspension of bitcoin fundraising*, Reuters, 28 IV 2023, https://www.reuters.com/world/middle-east/hamas-armed-wing-announces-suspension-bitcoin-fundraising-2023-04-28/ [accessed: 9 V 2023].

Alnasaa M. et al., *Crypto, Corruption, and Capital Controls: Cross-Country Correlations*, International Monetary Fund, 25 III 2022, https://www.imf.org/en/Publications/WP/Issues/2022/03/25/Crypto-Corruption-and-Capital-Controls-Cross-Country-Correlations-515676 [accessed: 4 V 2023].

Anti-money laundering: Provisional agreement reached on transparency of crypto asset transfers, Council of the EU, 29 VI 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/ [accessed: 7 IV 2023].

Berton B., *The dark side of the web: ISIL's one-stop shop?*, European Union Institute for Security Studies, June 2015, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf [accessed: 23 VIII 2019].

Bitcoin wa Sadaqat al-Jihad, https://krypt3ia.files.wordpress.com/2014/07/btced-it-21.pdf [accessed: 20 I 2019].

CFTC Charges Binance and Its Founder, Changpeng Zhao, with Willful Evasion of Federal Law and Operating an Illegal Digital Asset Derivatives Exchange, CFTC, 27 III 2023, https://www.cftc.gov/PressRoom/PressReleases/8680-23 [accessed: 9 IV 2023].

Crypto-assets. Relevant provision: Article 5b(2) of Council regulation (EU) NO 833/2014, https://finance.ec.europa.eu/system/files/2023-03/faqs-sanctions-russia-crypto_en.pdf [accessed: 10 IV 2023].

Crypto exchanges Huobi, KuCoin enabled Russian sanction evasion. Binance also mentioned, Ledger Insights, 28 II 2023, https://www.ledgerinsights.com/russia-sanctions-crypto-exchanges-huobi-kucoin-binance/ [accessed: 10 IV 2023].

Dugas M., *The Latest North Korea Cyber Indictment Should Serve as a Model*, Just Security, 24 II 2021, https://www.justsecurity.org/74930/the-latest-north-korea-cyber-indictment-should-serve-as-a-model/ [accessed: 11 V 2023].

Farah D., Richardson M., *The Growing Use of Cryptocurrencies by Transnational Organized Crime Groups in Latin America*, Georgetown University, 20 III 2023, https://gjia.georgetown.edu/2023/03/20/the-growing-use-of-cryptocurrencies-by-transnational-organized-crime-groups-in-latin-america/ [accessed: 6 IV 2023].

Fight against money laundering and terrorist financing, European Council, https://www.consilium.europa.eu/en/policies/fight-against-terrorism/fight-against-terrorist-financing/ [accessed: 9 IV 2023].

Five Russian Nationals and Two Oil Traders Charged in Global Sanctions Evasion and Money Laundering Scheme, United States Attorney's Office, Eastern District of New York, 19 X 2022, https://www.justice.gov/usao-edny/pr/five-russian-nationals-and-two-oil-traders-charged-global-sanctions-evasion-and-money [accessed: 7 IV 2023].

Germany and Ukraine hit two high-value ransomware targets, Europol, https://www.europol.europa.eu/media-press/newsroom/news/germany-and-ukraine-hit-two-high-value-ransomware-targets [accessed: 6 IV 2023].

Global Disruption of Three Terror Finance Cyber-Enabled Campaigns, The United States Department of Justice, 13 VIII 2020, https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns [accessed: 9 V 2023].

Hamas armed wing to stop crypto fundraising over 'hostility' against donors, i24NEWS, 30 IV 2023, https://www.i24news.tv/en/news/middle-east/palestinian-territories/1682688395-hamas-armed-wing-to-stop-crypto-fundraising-citing-hostility-against-donors [accessed: 9 V 2023].

How Russians Use Tether to Evade Global Sanctions, Inca Digital, https://inca.digital/intelligence/how-russians-use-tether/ [accessed: 10 IV 2023].

https://counterstrike.fandom.com/wiki/Skins [accessed: 17 II 2022].

Illicit Finance Risk Assessment of Decentralized Finance, U.S. Department of the Treasury, April 2023, https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf [accessed: 14 IV 2023].

Living on the Edge, International Monetary Fund, October 2022, https://www.imf.org/en/Publications/REO/SSA/Issues/2022/10/14/regional-economic-outlook-for-sub-saharan-africa-october-2022 [accessed: 5 IV 2023].

Maciąg A., Tarnowski I., *Atak teleinformatyczny na polski sektor finansowy* (Eng. ICT attack on the Polish financial sector), Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/ [accessed: 11 V 2023].

MUFG's Progmat security token platform to become digital asset joint venture, Ledger Insights, 7 X 2021, https://www.ledgerinsights.com/mufg-progmat-security-token-digital-asset-joint-venture/ [accessed: 5 IV 2023].

MUFG, SBI share roadmap for Japanese security tokens, Ledger Insights, 7 X 2021, https://www.ledgerinsights.com/mufg-sbi-share-roadmap-for-japanese-security-token-platform/ [accessed: 27 III 2023].

National Strategy for Combating Terrorist and Other Illicit Financing 2020, https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf [accessed: 7 VII 2023].

O'Sullivan F., *Where Is Crypto Illegal in 2023? The Countries That Ban Cryptocurrency*, Cloudwards, 22 II 2023, https://www.cloudwards.net/where-is-crypto-illegal/ [accessed: 5 IV 2023].

Perez Y.B., *Bitcoin, Paris and Terrorism: What the Media Got Wrong*, CoinDesk, 6 III 2023, https://www.coindesk.com/bitcoin-paris-and-terrorism-what-the-media-got-wrong [accessed: 10 V 2023].

Preiss I., *Crypto AML rules passed by MEPs*, The Block, 28 III 2023, https://www.theblock.co/post/223215/crypto-aml-rules-passed-meps [accessed: 6 IV 2023].

Ransomware Attacks on Critical Infrastructure Sectors, U.S. Department of Homeland Security, https://www.dhs.gov/sites/default/files/2022-09/Ransomware%20Attacks%20.pdf [accessed: 11 V 2023].

Risk Assessment. 2022 National Terrorist Financing, Department of the Treasury, February 2022, https://home.treasury.gov/system/files/136/2022-National-Terrorist-Financing-Risk-Assessment.pdf [accessed: 10 V 2023].

SEC Charges Decentralized Finance Lender and Top Executives for Raising $30 Million Through Fraudulent Offerings, U.S. Securities and Exchange Commission, https://www.sec.gov/news/press-release/2021-145 [accessed: 24 III 2023].

Sigalos M., Goswami R., *Sam Bankman-Fried paid over $40 million to bribe at least one official in China, DOJ alleges in new indictment*, CNBC, 28 III 2023, https://www.cnbc.com/2023/03/28/sam-bankman-fried-paid-over-40-million-to-bribe-at-least-one-chinese-official-doj-alleges-in-new-indictment.html [accessed: 9 IV 2023].

Sutton S., Seligman L., *Two major crypto exchanges failed to block sanctioned Russians*, Politico, 24 II 2023, https://www.politico.com/news/2023/02/24/two-major-crypto-exchanges-failed-to-block-sanctioned-russians-00084391 [accessed: 10 IV 2023].

Terrorism and Digital Financing: How Technology is Changing the Threat. Hearing before the Subcommittee on Intelligence and Counterterrorism of the Committee On Homeland Security House of Representatives, https://www.congress.gov/117/chrg/CHRG-117hhrg45867/CHRG-117hhrg45867.pdf [accessed: 10 V 2023].

UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf [accessed: 9 IV 2023].

United States of America v. Samuel Bankman-Fried, https://storage.courtlistener.com/recap/gov.uscourts.nysd.590940/gov.uscourts.nysd.590940.80.0.pdf [accessed: 7 IV 2023].

United States of America v. Ali Shukri Amin, CRIMINAL NO. 1:15-CR-164, https://www.investigativeproject.org/documents/case_docs/2826.pdf [accessed: 10 V 2023].

Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, FATF, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html [accessed: 7 IV 2023].

White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets, The White House, 16 IX 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/ [accessed: 9 IV 2023].

Legal acts

DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (OJ EU L 156/43 of 19 June 2018).

COUNCIL REGULATION (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine (OJ EU L 229/1 of 31 July 2014).

Act of 30 March 2021 amending the Act on counteracting money laundering and terrorist financing and certain other acts (Journal of Laws 2021, item 815, as amended).

Act of 1 March 2018 on counteracting money laundering and terrorist financing (Journal of Laws 2023, item 1124, as amended).

Act of 19 November 2009 on gambling games (Journal of Laws 2023, item 227).

Act of 29 July 2005 on counteracting drug addiction (Journal of Laws 2023, item 172, of 2022, item 2600).

Act of 10 September 1999 Fiscal Penal Code (Journal of Laws 2023, item 654, as amended).

Act of 6 June 1997 Criminal Code (Journal of Laws 2022, item 1138, as amended).

Act of 23 April 1964 Civil Code (Journal of Laws 2022, item 1360, as amended).

Ensuring Responsible Development of Digital Assets, Executive Order 14067 of March 9, 2022, Federal Register. The Daily Journal of the United States Government, https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets [accessed: 5 IV 2023].

Case law

Case file of the District Court in Przasnysz, 2nd Criminal Division, ref. no. II K 608/18.

Judgment of the District Court in Ostrołęka of 27 August 2020, ref. no. II Ka 40/20.

Judgment of the District Court for Kraków-Krowodrza, 2nd Criminal Division, of 3 August 2012, ref. no. II Ka 776/11/K.

Other documents

Markets in crypto-assets (MiCA), https://www.europarl.europa.eu [accessed: 9 IV 2023]. *Proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Directive (EU) 2019/1937*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593 [accessed: 9 IV 2023].

The views expressed in the article are the personal views of the authors and do not express the official position of the institution in which they are employed.

Paweł Opitek, PhD

Doctor of Law, Prosecutor of the District Prosecutor's Office in Kraków delegated to the National Prosecutor's Office.

Agnieszka Butor-Keler, PhD

Doctor in social sciences in the discipline of economics and finance, assistant professor in the Department of Management Accounting at the Warsaw School of Economics.

Karol Kanclerz

Legal trainee, chief specialist in the Legal Department of the Office of the Financial Supervision Authority.

https://doi.org/10.4467/27204383TER.23.031.18333

https://orcid.org/0000-0003-0385-3650

AGNIESZKA DOBRZYŃSKA-JAROSZ

Zonal security applied to modern diplomatic facilities, as exemplified by the construction of embassy buildings in Europe at the turn of the 20th and 21st centuries

Abstract

Diplomatic facilities are buildings with a unique structure and of great international importance. One of the important factors in their design is security and therefore the use of possible security measures (active and passive) to prevent potential threats. The aim of this article is to present the security measures used for the architecture of diplomatic facilities using the example of embassy buildings in Europe. Twenty-two embassies located in Warsaw, Berlin and Rome were analysed from this perspective. The article characterises the elements used in their design, implementation and modernisation at the turn of the 20th and 21st centuries.

Keywords:

embassy architecture, security, diplomatic facilities, security features

The construction of diplomatic facilities compared to other public facilities is relatively rare and the building or upgrading is undertaken for specific reasons by the sending states. Due to their location - mostly in national capitals - there are other diplomatic buildings or mixed-use facilities in their immediate surroundings, i.e. government buildings, public buildings, service buildings and residential developments. Diplomatic missions form zones of their own in the urban environment and, like other buildings, are part of the urban environment for many years. It is therefore extremely important to design them accordingly. Designers of diplomatic facilities must take into account, among other things, legal, economic, utilitarian, technical, spatial and security considerations.

The research objective of this article is to collect, describe, organise and systematise information on the architecture of embassy buildings constructed or modernised in Europe at the turn of the 20th and 21st centuries in relation to contemporary security measures and architectural solutions used in this area.

When considering the issue of embassy architecture, in addition to the analysis of architectural and construction projects, literature on international law and the field of diplomacy in the broadest sense is also important, including publications on diplomatic law, consular law, foreign policy, and the origins of international relations, which often omit architectural aspects. The literature on the subject includes mainly foreign publications on security in urban public spaces published by governmental organisations (mainly British and American) and executive bodies of the European Union. Of the Polish publications, the most important include the works of, among others, architect Artur Jasiński, on security and anti-terrorist protection of building space and facilities, in which the author introduces the contemporary principles of forming urban and architectural requirements for properties. He describes legal regulations on construction, security of buildings and open spaces. In his analyses, he takes into account British and American standards, and also refers to the anti-terrorist security features of the architecture of contemporary American embassies.

Recent European studies on the design of safe public spaces include publications by the European Commission (EC), including the Communication of 9 December 2020 *A counter-terrorism agenda for*

the EU: anticipate, prevent, protect, respond[1] and the late 2022 study entitled *Security by Design: Protection of public spaces from terrorist attacks: Protection of public spaces from terrorist attacks*[2].

It is worth noting that in architecture, embassies were treated primarily as representative buildings. Only in the last 30 years has there been a noticeable increase in interest in their architectural solutions[3]. This is confirmed, among other things, by the increasing number of publications on the subject, although in Poland these are still mainly a small number of articles on specific projects published, for example, in monthly trade magazines[4].

---

1 *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond*, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0795&from=PL [accessed: 5 VII 2023].

2 European Commission, *Security by Design: Protection of public spaces from terrorist attacks*, https://www.urbanagenda.urban-initiative.eu/news/security-design-protection-public-spaces-terrorist-attacks [accessed: 20 IV 2023]. (Translations in the text are from the author - editor's note).

3 The increase in interest is linked to the collapse of the communist era in the central and eastern European states and the fall of the Berlin Wall in 1989, when multifaceted international cooperation took place. Shortly afterwards, the European Union came into being and the sending countries decided to present their premises (mainly in Germany) anew.

4 These include, among others.: A. Jasiński, *Wpływ zabezpieczeń antyterrorystycznych na architekturę współczesnych ambasad amerykańskich* (Eng. The impact of anti-terrorism protection on the contemporary architecture of American embassies), "Internal Security Review" 2015, no. 12, pp. 97–114; T. Fretton, G. Stiasny, *Ambasada Wielkiej Brytanii w Warszawie* (Eng. British Embassy in Warsaw), "Architektura. Murator" 2009, no. 12, pp. 56–63; B. Gadomska, *Ambasada Izraela w Berlinie* (Eng. Embassy of Israel in Berlin), "Architektura. Murator" 2002, no. 2, pp. 16–19; W. Gorczyński, *Ambasada Kanady w Warszawie* (Eng. Canadian Embassy in Warsaw), "Architektura. Murator" 2002, no. 2, pp. 9–15; H. Jootsen, A. Stępniowska, *Ambasada Niemiec w Warszawie* (Eng. German Embassy in Warsaw), "Architektura. Murator" 2009, no. 12, pp. 48–55; M. Leśniakowska, *Architektura polskich ambasad* (Eng. Architecture of Polish embassies), "Architektura. Murator" 2004, no. 2, pp. 60–62; K. Majewski, M. Sroka-Strzeszyńska, *Ambasada Korei Południowej* (Eng. Embassy of South Korea), "Architektura. Murator" 2004, no. 2, pp. 38–41; J.P. Pagarde, G. Stiasny, *Ambasada Francji w Warszawie* (Eng. French Embassy in Warsaw), "Architektura. Murator" 2005, no. 2, p. 30; A. Sitko, S. Szafarczyk, *Technologie architektury – Ambasada Królestwa Niderlandów w Warszawie* (Eng. Architectural technologies - Embassy of the Kingdom of the Netherlands in Warsaw), "Architektura. Murator" 2004, no. 2, pp. 90–97; E. van Egeraat, G. Stiasny, *Ambasada Królestwa Niderlandów* (Eng. Embassy of the Kingdom of the Netherlands), "Architektura. Murator" 2004, no. 2, pp. 25–37; G. Stiasny, *Konkursy na nowe budynki ambasad w Warszawie* (Eng. Competitions for new embassy buildings in Warsaw), "Architektura. Murator" 2004, no. 2, pp. 44–59.

Potential threats to embassies

Terrorist activities observed in the last 20-plus years are contributing to changes in the urban and architectural structures of cities. The most at risk are national capitals and metropolises[5]. As a result of terrorist activity, restrictions on the minimization and prevention of attacks are tightening. In the 21st century, terrorism has taken on a new dimension. Thanks to the development of technology, communication, social media, information can be transmitted at an increasingly rapid pace. This makes it possible to rapidly recruit potential attackers, who also target civilians and public places[6] in order to achieve an attack with as many injuries and deaths as possible[7]. As already mentioned, embassies are mostly located in the centres of capital cities, near government buildings and other important public facilities, in areas crowded during the day. Thus, they can become direct or indirect targets of terrorist attacks. It is therefore important to adequately address potential threatening activities - as early as the design and construction stage - in order to fully secure the facilities or minimise the consequences of a potential terrorist attack.

It is worth emphasising that the design of foreign missions is by no means unified. The selection of conceptual, construction or implementation designs for embassy buildings depends on the internal legal regulations of both the sending and the receiving states, taking into account the legal norms of the embassy's home country in the first instance. The number of upgrades, purchases of facilities or designs for new buildings is determined by the budget allocated for these purposes. Many premises and facilities are rented. In 2004, the head of the Investment and Renovation Unit of the Polish Ministry of Foreign Affairs stated that the purchase of a new facility is profitable when the ratio of rental costs to purchase costs pays off within ten years[8].

---

[5] A. Jasiński, *Architektura w czasach terroryzmu. Miasto–przestrzeń publiczna–budynek* (Eng. Architecture in times of terrorism. City-public space-building), Warszawa 2013, p. 9.

[6] Examples of the terrorist attacks described are the attacks carried out on, among others, the World Trade Center twin towers in New York using hijacked passenger planes (11 IX 2001) and the London underground and bus bombing (July 2005).

[7] Contemporary terrorism is understood to be the activity of extremist groups which, through attacks, assassinations, kidnappings, etc., seek to draw the attention of the public to the ideas they promote or try to force governments of individual countries to make certain concessions or benefits. From: *Encyklopedia,* vol. 9, Warszawa 2001, p. 141.

[8] K. Rzechowski, *Polskie placówki dyplomatyczne* (Eng. Polish diplomatic missions), "Architektura. Murator" 2004, no. 2, pp. 63–70.

Terrorist attacks, which are the greatest threat to the security of diplomatic missions, can consist of individual actions (using firearms, explosives) or mass attacks (using explosives, chemical, biological, and radiological (CBR) weapons)[9]. The greatest risk, however, comes from an attack carried out using a vehicle-borne improvised explosive device. The impact of an explosion is often catastrophic, and it is therefore advisable to locate parking areas for potential threat vehicles as far away from buildings as possible, in order to reduce the risk of damage[10]. Consideration shall be given to the possible speed and weight of vehicles[11].

The 1980s saw a number of terrorist attacks on US diplomatic missions in the Middle East. In April 1983, a raid on the US embassy in Beirut and the explosion of a car filled with explosives driven by an Islamic suicide bomber killed 63 people and injured 120 others. A year later, there was another explosion at the embassy, which killed 24 people and injured 21. On 23 October 1983, 241 soldiers were killed in an attack on the US Marines barracks at the airport. On 12 December 1983, attacks were carried out on the embassies of the United States and the French Republic in Kuwait[12]. In August 1998 American embassies in Kenya and Tanzania were attacked (Image 1). These events demonstrated the enormity of the inadequacies in their protection and defence system. Since then, the US government has been working to improve the guidelines and standards for protecting and shaping its foreign diplomatic missions[13].

[9] Attacks using explosives (bombs) are also the most common threat. Among these we can distinguish: explosion of a parked car loaded with explosives near or on the premises of an establishment, ramming of the entrance or entrance or facade of an embassy with a car loaded with explosives, placing an explosive charge in a consignment or goods to be delivered, planting or placing a charge on the premises of a building, attack by a suicide bomber. See: *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, series: Buildings and Infrastructure Protection Series, http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, p. 1/15 [accessed: 16 V 2016].

[10] *Embassy Perimeter Improvement Concepts & Design Guidelines*, Department of State Bureau of Overseas Buildings Operations, June 2011, https://www.scribd.com/document/261408078/Embassy-Perimeter-Improvement-Concepts-Design-Guidelines, p. 56; *Site and Urban Design for Security. Guidance Against Potential Terrorist Attacks*, series: Risk Management Series, https://www.fema.gov/sites/default/files/2020-08/fema430.pdf [accessed: 13 V 2023].

[11] *Embassy Perimeter Improvement Concepts...*, pp. 56–72.

[12] *Site and Urban Design for Security...*, pp. 1/29–1/31.

[13] See in more detail: A. Jasiński, *Wpływ zabezpieczeń...*, pp. 97–114.


A


B

Image 1. The state of the US embassy buildings after the terrorist attacks in August 1998 - in Nairobi in Kenya (A), in Dar es Salaam in Tanzania (B).

Source: *Site and Urban Design for Security. Guidance Against Potential Terrorist Attacks*, series: Risk Management Series, US Federal Emergency Management Agency (FEMA 430), December 2007, https://www.fema.gov/sites/default/files/2020-08/fema430.pdf, p. 1/29, 1/31 [accessed: 13 V 2023].

Embassy buildings can also be damaged as a result of a terrorist attack carried out in the vicinity of the facility. This happened, for example, in Athens in November 2015, when the embassy of the Republic of Cyprus was severely damaged by a bomb explosion (Image 2). The most likely target of the terrorists was the Federation of Greek Industries building located opposite the embassy. However, the force of the explosion and blast was so great that the entrance area of the building, the front façade and the glazing of the outer wall from the ground floor to the sixth floor were damaged. The structure of the embassy buildings suffered significantly, although this was not the intention of the bombers.


A


B

Image 2. Embassy of the Republic of Cyprus in Athens: entrance area, state before the explosion (A), state after the bomb explosion (B).

Source: image 2A - property of the author; 2B – A. Kades, *Cypriot embassy severely damaged in Athens bomb blast*, CyprusMail, 24 XI 2015, http://cyprus-mail.com/2015/11/24/cypriot-embassns-bomb-attack/ [accessed: 24 XI 2015].

It is noteworthy that anti-terrorist policies, with strict conditions concerning, among other things, their own foreign establishments, have been most thoroughly developed in the United States and the United Kingdom. Individual legal regulations covering the issue of terrorism contain important guidelines for the design of the architecture of embassies and the spaces belonging to them. In the light of large-scale research into the security of buildings, diplomatic facilities and public spaces against terrorist threats, both approaches - the appropriate use of security features and the formation of facilities - are relevant already in the design process.

Ways of securing diplomatic facilities

When analysing issues concerning the security of embassy buildings, the most important and binding piece of legislation is the Vienna Convention on Diplomatic Relations, under which embassies, their grounds and staff are protected. It specifies that the premises of missions are guaranteed inviolability[14]. Similarly, the residence of the ambassador, whether inside or outside the embassy building, is protected by the host state[15]. The host state, on the other hand, is obliged, inter alia, to take all appropriate steps to protect the embassy from unwanted intrusion or harm, to protect it from disturbance to the mission and from impairing its dignity. Crucially, the host state is responsible for the safety, security and respect of the foreign post even in the event of armed conflict, the severance of diplomatic relations or the cancellation of the mission. The inviolability of embassies also applies in the event of public gatherings, demonstrations, etc.[16] Host states are also obliged to prevent attempts to carry out attacks on embassies. Despite all the regulations and obligations imposed on the host state, it is possible to observe the occurrence of situations that breach the security of embassies and their staff.

[14] *Vienna Convention on Diplomatic Relations, drawn up in Vienna on April 18, 1961,* Articles 22, 29 and 30.

[15] Ibid, Article 30. The private residence of a diplomatic representative enjoys the same inviolability and protection as the premises of the mission.

[16] In the case of the organisation of assemblies in the vicinity of diplomatic representations, the municipality must immediately notify the Minister of Foreign Affairs of the place, date and potential number of participants. See: *Act of 24 July 2015 - Law on assemblies.*

As mentioned, the most important Polish study on shaping architecture and urban space in terms of terrorism was published by architect Artur Jasiński. He identifies two possibilities for ensuring an adequate level of security in the event of a terrorist attack carried out with explosives. The first solution is zonal security, i.e. a sufficiently large safety zone, equipped with intermediate obstacles, whereby the building can be kept at an appropriate distance from the site of a possible explosion so that it is not damaged. The second way is to reinforce its structure and elements. Jasiński stresses that the first option is more effective, economical and quicker to implement, as not all existing buildings can be technically altered[17].

In his publications, Jasiński describes and characterises documents, legal acts and academic publications - mainly produced in the United States and the United Kingdom - dedicated to the issue of terrorism and the adequate protection of public spaces and mixed-use buildings[18]. At the same time, he points out that there is a lack of studies on the subject in the Polish literature and mentions only his own research and publications.

The preferred zonal defences consist of deploying protective barriers around the protected object and using measures between the boundaries of the plot and the building that can significantly reduce the effectiveness of the attack[19]. Elements such as fences, gated entrances, technical entrances, entrances, car parks, access and security controls (video surveillance, turnstiles, sensory gates, metal detection gates, X-ray scanners for baggage and parcel control) are important. Zonal security elements include, but are not limited to, the form of the terrain, its irregularities, the watercourses present and man-made elements, e.g. barriers in the form of walls, fences, retaining walls, as well as landscaping elements[20]. The literature on the subject distinguishes between two groups of zoning protection for facilities: passive and active[21].

---

17 A. Jasiński, *Architektura w czasach terroryzmu…*, p. 177.

18 See in more detail: ibid., pp. 13–30.

19 *Reference Manual to Mitigate…*, p. 2/2.

20 A. Jasiński, *Architektura w czasach terroryzmu…*, p. 177.

21 Protective measures for public spaces and areas around the building have been recommended and described, among other things, in: *Reference Manual to Mitigate…*, pp. 2/18–2/77; *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks*, series: Risk Management Series, https://www.fema.gov/sites/default/files/2020-08/fema427.pdf, pp. 6/1–6/7 [accessed: 30 V 2023]; A. Jasiński, *Architektura w czasach terroryzmu…*, pp. 177–198.

Passive ways to zonal security of diplomatic facilities

Passive elements to protect embassies include[22]:

- **reinforced steel or reinforced concrete urban furniture**, e.g. benches, seats, posts, flowerbeds, flower pots, bicycle racks, lamp posts, information boards, bus shelters, shelters - adapted to the site so that the distance between them is no more than 1.2 m;
- **retaining walls or freestanding walls** (point or perimeter) intended to protect against ramming and unwanted entry onto a plot of land, e.g. by complementing and reinforcing naturally occurring landforms, structures or fences. When located in a publicly accessible area (i.e. square, pavement, etc.), these can be walls fitted with seating or planting, or clad with special finish cladding. In addition, integrated perimeter systems with vegetation elements, rest areas and information points can be introduced, incorporating breaks for pedestrian walkways (recommended width is 1 m). Solutions in the form of reinforced, prefabricated, concrete road barriers (jersey barriers), which can be moved efficiently and can effectively separate specific zones, are also used.
- **static, free-standing columns** that prevent unauthorised entry and parking of cars and delimit traffic exclusion zones (Image 2). They can occur singly or in groups and take different forms, such as simple - with a purely protective function, architectural-decorative (e.g. integrated with lighting), visible or concealed (integrated with other elements such as flowerbeds, benches or flower pots) – (Image 3);

A

B

Image 3. Static posts as part of zonal protection in front of the Embassy of the Kingdom of the Netherlands in Berlin (A), freestanding protection posts and pots as part of passive zonal protection in front of the Israeli Embassy in Athens (B).

Source: property of the author.

[22] Developed based on U.S. standards for embassy design and recommendations from the U.S. Federal Emergency Management Agency. See also: D. Cormie, G. Mays, P. Smith, *Blast effects on buildings*, London 2009, pp. 250–273; *Embassy Perimeter Improvement Concepts...*, pp. 56–72; *Site and Urban Design for Security...*

– **sculptures** (*NoGo barriers*) originally designed for the Wall Street area in New York[23], which are an evolved form of static free-standing posts (Image 4). *NoGo barriers* are designed and constructed to be aesthetically pleasing, visually appealing and can - in addition to their primary protective function - be used as seats or tables. Protection elements can also be sculptures or art installations;

A

B

Image 4. *NoGo barriers* - security elements within the Wall Street zone. bronze sculptural forms integrated with lighting (A), seats integrated with pneumatically lowered crossing posts (B).

Source: http://www.rogersmarvel.com/projects/NYSE/ [accessed: 15 VI 2016].

– **natural forms of protection**, i.e. elements of nature that can act as a protective barrier while integrally complementing the composition of the surroundings (Image 5). Natural forms of protection may include, among others, boulders, massively and sufficiently deeply founded, which can be an effective zonal protection; natural or secondarily created watercourses (streams, ponds, ponds, moats, waterfalls, fountains, rivers, etc.); garden *aha* forms[24] (Fr. ha-ha), i.e. hidden elements preventing the encroachment of the garden area, e.g. a hidden ditch, a fault or a watercourse; a hidden planting, a rockery, a small pond, a small pond, a moat, a moat, a waterfall, a fountain, a river, etc. hidden ditch, fault or watercourse; massive plantings whose root system cannot damage other zoning

[23] Artistic forms intended to provide an adequate level of security in the Wall Street area were designed by the American design firm Roger Marvel Architects. See: http://www.rogersmarvel.com/projects/NYSE/ [accessed: 28 V 2023].

[24] From: *Encyklopedia humanistyczna* (Eng. Encyclopedia of the humanities), http://encenc.pl/aha/ [accessed: 14 V 2023].

security elements (e.g. fences), placed at a sufficient distance from the perimeter guards to ensure full view and control by a camera system and physical security system, preventing climbing and passage by unwanted persons;


A


B

Image 5. Trees, flower pots and flower beds that are part of the passive security zone in front of the Embassy of the French Republic in Warsaw (A), Embassy of Canada in Warsaw (B).

Source: property of the author.

– **fences** of different materials in terms of texture and transparency (e.g. stone, brick, solid, glass, perforated metal, mesh), made in such a way as to prevent climbing (Image 6). Vertical baffles are recommended to allow users of the urban space to see into the embassy area, giving the establishment a friendly and open character.


A


B

Image 6. Façade and front fence of the Embassy of the Kingdom of the Netherlands in Warsaw (A), view of the fence and façade from the north-west side of the Embassy of the United Kingdom in Warsaw (B).

Source: property of the author.

Active means of zonal security of diplomatic facilities

Active zonal security measures are mainly found at entrances, crossings, access points, technical entrances, emergency entrances and exits. Among

these, we can distinguish between two types of solutions: mechanically or manually controlled:

– **free-standing posts** placed within the crossing area, hydraulically, pneumatically, electrically or manually lowered, made of aluminium, steel, fibreglass, often supplemented with additional elements (lighting, information boards)[25] – (Image 7);

A

B

Image 7. Free-standing drop-down posts - in front of the entrance gate to the car park of the US Embassy in Berlin (A), within the entrance to the inner courtyard of the Embassy of the Kingdom of the Netherlands in Berlin (B).

Source: property of the author.

– **rotating crossing platforms**[26], which as a hybrid solution consist of two elements: a rotating panel and posts (Figure 1).

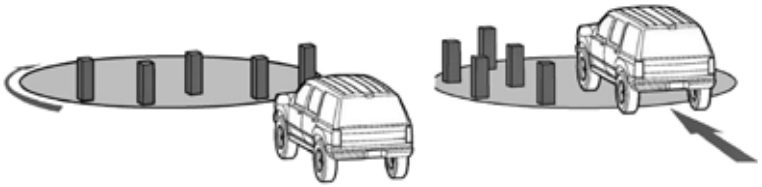


Figure 1. Rotating crossing platforms. Left - closed crossing, right - open crossing.

Source: *Site and Urban Design for Security. Guidance Against Potential Terrorist Attacks*, series: Risk Management Series, https://www.fema.gov/sites/default/files/2020-08/fema430.pdf, p. 4/48 [accessed: 13 V 2016].

[25] See in more detail: *High Security Bollards*, Delta Scientific Corporation, http://deltascientific.com/high-security/bollards/ [accessed: 28 V 2023].

[26] Ch.G. Oakes, *The Bollard: Crash- and Attack-Resistant Models*, Whole Building Design Guide, 9 II 2016, https://www.wbdg.org/resources/bollard-non-crash-and-non-attack-resistant-models [accessed: 9 I 2023].

– **discs or crossing-road barriers**[27] to block the entry of unauthorised vehicles. They can be extended upon receipt of a signal from the control panel and, once the danger has passed, retracted. Depending on the form of the movable element, there are two types of road barriers, which can vary in size, height, width and strength. The first is the rising wedge barriers – (Image 8 and Figure 2).

Image 8. US Embassy in Baku - rising wedge type road barrier in front of the entrance gate to the facility.

Source: *U.S. Embassy security upgrades in Baku*, Pernix Group, https://www.pernixgroup.com/project/baku-design-build-isat-security-upgrades/ [accessed: 10 I 2023].

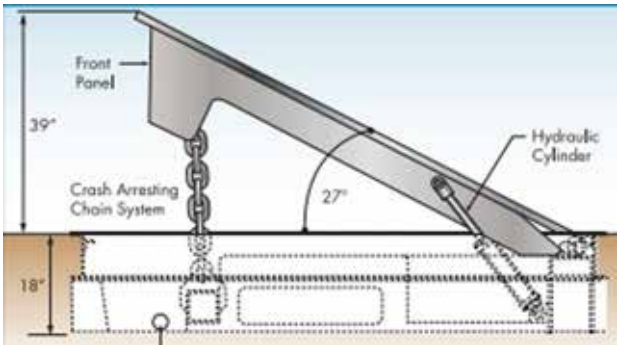


Figure 2. Cross-section of a rising wedge type road barrier.

Source: *Site and Urban Design for Security. Guidance Against Potential Terrorist Attacks*, series: Risk Management Series, https://www.fema.gov/sites/default/files/2020-08/fema430.pdf, p. 4/40 [accessed: 13 V 2023].

[27] *Reference Manual to Mitigate...*, pp. 2/57–2/61.

The second type is equipped with a rotating wedge system – (Image 9 and Figure 3).

Image 9. Road barrier with rotating panel in the entrance area in front of the entrance to the Embassy and Residence of Japan in Warsaw.

Source: http://www.google.pl/maps/ [accessed: 10 III 2015].

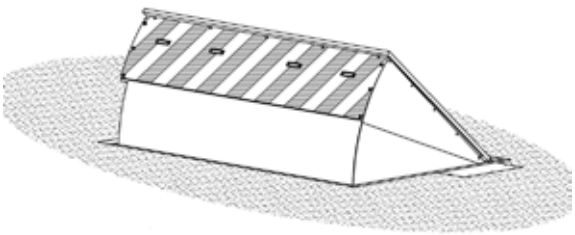


Figure 3. Road barier.

Source: https://deltascientific.com/wp-content/uploads/2021/01/90140-Rev-B-DSC207S-General-Arrangement.pdf [accessed: 9 I 2023].

Portable road barriers that are lowered and raised hydraulically, either automatically or manually, are also available (Image 10)[28].

[28] The portable element protects against entry and ramming by unwanted vehicles in an area where a permanent barrier cannot be made. The advantage of such a solution is that there is no special foundation or anchoring. The blockade consists of two lateral steel components weighing no more than 318 kg, which must be filled with concrete in advance or on site. The firewall is equipped with a radio panel and a card reader. See in more detail: *DSC1100 K8 Portable Barriers,* Delta Scientific Corporation, https://deltascientific.com/product/portable-barrier-dsc1100/ [accessed: 28 V 2023].

Image 10. British Embassy in Budapest - portable road barrier (DSC 1100 type).

Source: *DSC1100 K8 Portable Barriers*, Delta Scientific Corporation, https://deltascientific.com/product/portable-barrier-dsc1100/ [accessed: 28 V 2023].

– **entrance gates** (sliding, swinging or hinged opening with or without ground clearance) for pedestrians and vehicles (Image 11)[29]. To increase the level of security, entrance gates can be integrated with other elements to protect embassy facilities and spaces. In practice, they are combined with shields or road barriers or hydraulically or pneumatically lowered free-standing posts.

Image 11. Embassy of the Republic of Turkey in Berlin - openwork entrance gate in front of the garage exit, with movable security posts behind it (in the background).

Source: property of the author.

[29] There are manually or mechanically operated systems. Gate sizes and forms depend on the manufacturers. They offer different types of gates with spans from 3.6 m to 9.15 m. The following finishes are proposed to enhance the aesthetics of the massive frames: glass, screen-printed glass, stone, steel, concrete, wood and painting with a specific range of colours. See in more detail: *Sliding High Security Crash Rated Gates*, Delta Scientific Corporation, https://deltascientific.com/high-security/sliding-gates/ [accessed: 28 V 2023].

– **barriers**, whether permanently or temporarily installed, e.g. as mobile installations[30].

Security measures applied in embassies built or upgraded in Europe at the turn of the 20th and 21st centuries

For the purpose of researching the security aspect of embassy buildings, an analysis of source materials and field and photographic research was carried out on 22 selected buildings located in Warsaw, Berlin and Rome.

In the vicinity of the development, in addition to reinforced site security and massive static road barriers, patrols and permanent observation booths can be seen, in line with the legal regulations of the Vienna Convention for ensuring an adequate level of protection and security for diplomatic and consular posts. The US Embassy in Athens is a case in point (Image 12).

Image 12. US Embassy in Athens - zonal security in the form of static road barriers, high fencing, a permanent guard booth for law enforcement and road patrol.

Source: property of the author.

The aftermath of the 11 September 2001 attack on the WTC twin towers in New York resulted in the abandonment of attempts to fully integrate embassies into the urban spaces of host capitals[31]. An example of abandoning the initial assumptions of openness is the Embassy of the French Republic in

[30] The control of the unit comes in two versions: manual and hydraulic. The device requires neither anchoring nor foundations, making it possible to move it quickly and efficiently. See in more detail: *P500 High Security Portable Barriers*, Delta Scientific Corporation, http://www.deltascientific.com/high-security/portable-barriers/ip500 [accessed: 28 V 2023].

[31] Excluding American implementations, whose relocation and shape modification was defined in the 1980s and 1990s. This is evidenced by the Inman and Cowe reports.

Berlin, located at Pariser Platz 5 (Image 13). It is a compact building situated in the frontage of the square and street, with internal courtyards and no fence. On the west side of the main façade, directly against the wall of the building adjacent to the establishment, is the Rue publice - a two-storey internal pedestrian passage, 5 m wide, glazed and paved. It is L-shaped and connects the public spaces on the Wilhelmstraße and Pariser Platz sides. Designed to be open and accessible to the public, the walkway was intended as a way of inviting passers-by inside the embassy, but as a result of increased terrorist attacks in the early years of the 21st century, the walkway was already closed to the public during the construction phase for security reasons[32].


A


B

Image 13. Embassy of the French Republic in Berlin – front facade facing Pariser Platz (A), interior of Rue publice and courtyard with visible sculpture (B).

Source: image 13A - property of the author; 13B – S. Redecke, *Der Weg zum Licht – Französische Botschaft am Pariser Platz in Berlin*, "Bauwelt" 2003, no. 10, p. 14.

Inman Report, a 1985 report outlining the scope and dimension of security problems in US foreign diplomatic missions and identifying elements to ensure an adequate level of security and protection for those working in or visiting missions. The report is available on the website of the Federation of American Scientists, which provides scientific analysis and solutions to, inter alia, protect against threats to national and international security. See: *Report of the Secretary of State's. Advisory Panel on Overseas Security*, http://www.fas.org/irp/threat/inman/ [accessed: 5 VII 2023]; J.C. Barker, *The Protection of Diplomatic Personnel*, University of Sussex 2006, pp. 9–10.
The Crowe Report on embassy security – a Government Department report produced under the leadership of Admiral Wiliam J. Crowe. The report assumed the introduction of a 10-year government programme to build diplomatic facilities, secure missions and staff at US embassies around the world. The projected annual cost of the venture was US $1.4 trillion. See: J.C. Loeffler, *Embassy design: security vs. openness*, "Foreign Service Journal", September 2005, pp. 44–51.

[32] K. Englert, J. Tietz, *Botschaften in Berlin* (Eng. Embassies in Berlin), Berlin 2004, pp. 130–131; S. Redecke, *Der Weg zum Licht – Französische Botschaft am Pariser Platz in Berlin* (Eng. The Path to Light - French Embassy on Pariser Platz in Berlin), "Bauwelt" 2003, no. 10, pp. 12–19; P. Ulrich, *Die franzoesische Vertretung am Pariser Platz will trotz hoher Sicherheitsanforderungen ein offenes Haus sein: Bald bietet die Botschaft Fuehrungen durch das neue Gebaeude* (Eng. The French representation on Pariser Platz wants to be an open house despite high security requirements: Soon the embassy will offer guided tours of the new building), "Berliner Zeitung", 24 I 2003.

Some embassy developments do not include a developed security structure in their programme. An example is the free-standing Embassy of the Italian Republic in Berlin (Image 14). The building was constructed between 1938 and 1942, and the historic building was rebuilt between 1999 and 2003. The embassy is located on a trapezoidal-shaped plot of land. The three-winged building, resolved in a U-shape, is closed on the west side with a two-storey portico. The front part of the building is not separated from the public space in any way, nor are the western and eastern elevations. The only visible security feature is the CCTV.

Image 14. Front facade of the Embassy of the Italian Republic in Berlin.

Source: property of the author.

The design of buildings in terms of security should be in balance with other important aspects such as aesthetics, prestige, accessibility, functionality, technical consumption, the environmental impact of the facility or the use of renewable energy sources. The countermeasures used in design and implementation should be integrated with other elements of the establishment so that they create a friendly working environment that is positively perceived by the users of the diplomatic facilities and the residents of the capital. Appropriate landscaping of both the plots on which embassies are located and the adjacent surroundings can prevent hazards from approaching the building walls. Not all building plots and facilities can be secured within their occupied area. Available publications on building security recommend maintaining safety zones between the building and the fence or plot boundary. If an area outside or on the outskirts of a city is being considered, the requirement to maintain a distance does not usually pose difficulties. The situation is different in the case of inner city developments, where - due to the intensive built-up

area - alternatives are used, e.g. the exclusion of parts of streets or pavements used as public spaces, as exemplified by the British Embassy in Berlin (Image 15), where a section of Wilhelmstraße has been partially excluded from traffic using road barriers, thus ensuring that only authorised vehicles can access the building.

Image 15. British Embassy in Berlin - exclusion by means of zone barriers of a section of Wilhelmstraße. View from Behrenstraße.

Source: property of the author.

The Table shows the results of the zonal security analysis of the 22 embassies located in Warsaw, Berlin and Rome. Passive property zoning security in the form of building access control, internal and external monitoring is present in all of the surveyed facilities. In the case of 68% of the establishments, there are additional guards with a security post within the fence or directly at the entrance area of the building. Half of the surveyed permanent diplomatic missions use elements of permanent road barriers in the form of bollards or posts in their landscaping or areas adjacent to their plots. More than three-quarters of the embassies surveyed (77%) are completely or partially isolated from neighbouring spaces and plots by means of fencing.

Active safety elements of zonal road barriers to block the entry of unauthorised vehicles (discs) were used in only 9% of the cases. Movable barriers in the form of posts or bollards were used in 27% of facilities, massive reinforced entrance gates were used in 54%, and double road barriers occurred in three developments (14%). In 27% of the establishments, both the entrance areas within the fence and the embassy gates were doubled. This created locks to ensure control of entrances and entrances, as if

unwanted persons or vehicles cross the first zone with security elements, the services have the ability to block this section and prevent further access.

Table. Characteristics of security in embassies - zonal security: passive and active.

No.	Embassy	City	Security of the embassy building/complex										
			Passive zone protection components						Active zone protection components				
			Access control	Guard box(es) with a security post	External CCTV	Internal CCTV	Road barriers (fixed posts)	Fence	Hydraulic road barriers (discs)	Hydraulic road barriers (posts)	Double road barriers	Solid, reinforced entrance gates	Double entry and exit zones (locks)
1.	French Republic	Warszawa	•	•	•	•	•	•	–	–	–	•	–
2.		Berlin	•	–	•	•	–	–	–	–	–	–	–
3.	Kingdom of the Netherlands	Warszawa	•	•	•	•	–	•	–	–	–	–	–
4.		Berlin	•	•	•	•	•	–	–	•	–	–	–
5.		Rzym	•	•	•	•	–	•	–	–	–	•	–
6.	United Kingdom	Warszawa Polska	•	•	•	•	•	•	–	•	–	•	•
7.		Berlin	•	•	•	•	•	–	–	•	•	•	•
8.	Scandinavian countries	Berlin	•	–	•	•	•	•	–	–	–	–	–
9.	Japan	Warszawa	•	•	•	•	–	•	•	–	–	•	•
10.		Berlin	•	•	•	•	–	•	•	–	–	•	•
11.	South Korea	Warszawa	•	•	•	•	–	•	–	–	–	•	–
12.	United States	Berlin	•	–	•	•	•	•*	–	•	•	–	•
13.	Swiss Confederation	Berlin	•	•	•	•	–	•	–	–	–	–	–
14.	Canada	Warszawa Polska	•	•	•	•	•	•	–	–	–	•	–
15.		Berlin	•	–	•	•	•	–	–	•	–	–	–
16.	Federal Republic of Germany	Warszawa	•	•	•	•	•	•	–	–	–	•	•

17.	Kingdom of Spain	Warszawa	•	•	•	•	•	•	–	–	–	•	–
18.	United Mexican States	Berlin	•	–	•	•	–	•*	–	–	–	–	–
19.	Republic of India	Berlin	•	•	•	•	–	•	–	–	–	•	–
20.	Republic of Turkiye	Berlin	•	•	•	•	•	•	–	•	•	•	–
21.	South Africa	Berlin	•	–	•	•	–	•	–	–	–	–	–
22.	Kingdom of Belgium	Berlin	•	–	•	•	–	–	–	–	–	–	–
Percentage ratio:			100%	68%	100%	100%	50%	77%	9%	27%	14%	54%	27%
Legend : • element is present, •* element is fragmented, – no element													

Source: own elaboration.

Given the increased likelihood of an attack on embassies, the need for security at the facility cannot be overlooked either. Individuals may bring a dangerous element directly into the facility. In order to be able to respond quickly to potential danger, backpacks, bags or electronic devices, i.e. computers, cameras or mobile phones, are prohibited in a large group of establishments. These must be deposited at the control point and are returned to the guest after the visit.

The security of permanent diplomatic missions is extremely important and often complex. The process of putting in place security must run in parallel with the design stages that follow. The use of available methods allows for a coherent implementation of the investment and the development of the adjacent surroundings. Manufacturers of containment barriers are able to tailor catalogue solutions to specific individual requests. The use of belaying elements in the form of reinforced landscaping and appropriately shaped landscaping not only improves the aesthetics, but also provides a hindrance to potential attackers.

Summary

Contemporary studies on security by design and the protection of public spaces emphasise the need to apply security concepts from the initial stages of designing or modernising urban spaces, taking into account, for example, the reorganisation of urban planning and communication

solutions in the vicinity of areas or facilities exposed to potential terrorist attacks. The focus should also be on integrated design, in line with sustainability and the New European Bauhaus, i.e. design with an emphasis on safety, inclusiveness, quality and ease of life, accessibility for users and the introduction of attractive and functional solutions[33]. It is also important to remember to use elements that can make a positive contribution to minimising climate change. These conditions should be met in each of the six categories of public spaces classified by the EC. Diplomatic missions belong to governmental spaces[34].

The four key aspects of the concept of designing safe public spaces include: multifunctionality, proportionality, aesthetics and cooperation with parties who may influence or be affected by the proposed solutions. The European Commission emphasises the need for the necessary protection measures, with the concept of "invisible security" stating that forms of protection should be small-scale architectural and urban engineering elements that are integrated into the surroundings and do not give the impression of fortification[35]. Consideration of the above aspects and the involvement of an interdisciplinary design team comprising qualified professionals and stakeholders involved in the design process, will allow the implementation of timely, effective and aesthetically pleasing implementation solutions.

A wide range of measures are used to ensure that embassies have adequate security. Within the building, state-of-the-art technology, integrated monitoring and intruder alarm systems, access control devices, motion sensors, protective film for glass, reinforcement of the building's structure, ventilation security (securing all building inlets and outlets, i.e. exhausts and intakes, to avoid the placement of threatening elements), as well as physical active and passive zonal protection elements and satellite views are used. All of these measures are designed to protect against and

[33] See in more detail: https://new-european-bauhaus.europa.eu/index_en [accessed: 5 VII 2023].

[34] According to the classification used by the EC, the following categories of public space are distinguished: recreational, commercial, public, religious, communication, governmental. See: *Security by Design: Protection…*, pp. 19–29, 38–39.

[35] A. Jasiński, *Koncepcja „niewidzialnego bezpieczeństwa" stosowana w zabezpieczeniu antyterrorystycznym amerykańskich miast metropolitalnych* (Eng. The concept of "invisible safety" used in the counter-terrorist security measures in the US metropolitan cities), "Internal Security Review" 2011, no. 5, pp. 99–115.

prevent potential terrorist attacks[36]. However, the ever-increasing ingenuity of criminal groups and the current intensification of assaults using various types of objects, machines or devices are causing the field of security to constantly evolve.

Security at the lot and embassy is provided primarily by a fence, separating the facility space from neighbouring areas, and checkpoints, where petitioners and visitors are carded and their belongings and vehicles are checked (x-rayed). Depending on the needs of investors, checkpoints may be located within the perimeter fence line, within the building or both. Checkpoints within the fence can be common to several locations (e.g. separate checkpoints for the consular area, the residence and the chancellery) or individual for each of them. The first solution is related to the need to save money and thus reduce the number of guard buildings and security personnel. In contemporary embassy developments or modernisations, there are cases where neither fencing nor an external access control point is part of the solution. Security controls are supplemented by both plot monitoring and landscaping elements such as plantings and other landscape elements (watercourses, boulders, hills). In the vicinity of European developments, in addition to reinforced site protection and massive, static road barriers, patrols and permanent observation booths can be observed, in accordance with the legal regulations of the Vienna Convention for ensuring an adequate level of protection and security for diplomatic and consular posts. In major developments, the location of car parks or garages within buildings is increasingly being abandoned, as they are easy places to detonate an explosive charge. It is advisable to locate parking areas outside the perimeter of the building and, if this is not possible, they should be reserved for a specific group of vehicles (employees and privileged persons).

When discussing security measures, the need to ensure security within the premises of the facility, where individuals may bring a dangerous item directly into the facility (weapons, cargo), cannot be overlooked. Access control points are most often located in front of the entrance areas. Within them, persons, vehicles and consignments are monitored, controlled, checked and legitimised before entering or entering the facility. Surveillance and access rules are primarily governed by intra-state procedures and modern security requirements. Typically, mechanical

[36] *Reference Manual to Mitigate...*, pp. viii–ix.

and electronic access control systems are used, i.e. video surveillance - cameras (CCTV system), entry turnstiles, low turnstiles (tripods) or sensor gates, metal detecting gates, passageways with locks requiring numeric (PIN) codes or access cards (proximity, chip, magnetic) and x-ray scanners for baggage and parcel inspection.

The diversity of uses of properties adjacent to diplomatic buildings in Europe has allowed the integration of areas with different functions and, in some cases, increased interest in them from both the local community and tourists. Therefore, the applied reinforcement of the spatial forms of buildings and areas adjacent to embassies should not significantly affect the aesthetics of the facilities. The use of landscaping elements and appropriately shaped relief not only improves the appearance, but also provides additional difficulty for potential attackers. It should be recalled, of course, that the security measures applied both on the grounds and in embassy buildings can vary considerably depending on the sending country, the mutual relations with the host country and their internal regulations, the financial resources of the investor and the location of the facility. Nowadays, there are embassy developments located within a section, floors or storey of a building with a different purpose, which makes it much more difficult to put in place the safeguards outlined and ensure an adequate level of security.

Bibliography

Barker J.C., *The Protection of Diplomatic Personnel*, University of Sussex 2006.

Cormie D., Mays G., Smith P., *Blast effects on buildings*, London 2009.

van Egeraat E., Stiasny G., *Ambasada Królestwa Niderlandów* (Eng. Embassy of the Kingdom of the Netherlands), "Architektura. Murator" 2004, no. 2, pp. 25–37.

Encyklopedia, vol. 9, Warszawa 2001.

Englert K., Tietz J., *Botschaften in Berlin*, Berlin 2004.

Fretton T., Stiasny G., *Ambasada Wielkiej Brytanii w Warszawie* (Eng. British Embassy in Warsaw), "Architektura. Murator" 2009, no. 12, pp. 56–63.

Gadomska B., *Ambasada Izraela w Berlinie* (Eng. Embassy of Israel in Berlin), "Architektura. Murator" 2002, no. 2, pp. 16–19.

Gorczyński W., *Ambasada Kanady w Warszawie* (Eng. Canadian Embassy in Warsaw), "Architektura. Murator" 2002, no. 2, pp. 9–15.

Jasiński A., *Architektura w czasach terroryzmu. Miasto–przestrzeń publiczna–budynek* (Eng. Architecture in times of terrorism. City-public space-building), Warszawa 2013.

Jasiński A., *Koncepcja „niewidzialnego bezpieczeństwa" stosowana w zabezpieczeniu antyterrorystycznym amerykańskich miast metropolitalnych* (Eng. The concept of "invisible safety" used in the counter-terrorist security measures in the US metropolitan cities), "Internal Security Review" 2011, no. 5, pp. 99–115.

Jasiński A., *Wpływ zabezpieczeń antyterrorystycznych na architekturę współczesnych ambasad amerykańskich* (Eng. The impact of anti-terrorism protection on the contemporary architecture of American embassies), "Internal Security Review" 2015, no. 12, pp. 97–114.

Jootsen H., Stępniowska A., *Ambasada Niemiec w Warszawie* (Eng. German Embassy in Warsaw), "Architektura. Murator" 2009, no. 12, pp. 48–55.

Leśniakowska M., *Architektura polskich ambasad* (Eng. Architecture of Polish embassies), "Architektura. Murator" 2004, no. 2, pp. 60–62.

Loeffler J.C., *Embassy design: security vs. openness*, "Foreign Service Journal", September 2005, pp. 44–51.

Majewski K., Sroka-Strzeszyńska M., *Ambasada Korei Południowej* (Eng. Embassy of South Korea), "Architektura. Murator" 2004, no. 2, pp. 38–41.

Pagarde J.P., Stiasny G., *Ambasada Francji w Warszawie* (Eng. French Embassy in Warsaw), "Architektura. Murator" 2005, no. 2, p. 30.

Redecke S., *Der Weg zum Licht – Französische Botschaft am Pariser Platz in Berlin* (Eng. The Path to Light - French Embassy on Pariser Platz in Berlin), "Bauwelt" 2003, no. 10, pp. 12–19.

Rzechowski K., *Polskie placówki dyplomatyczne* (Eng. Polish diplomatic missions), "Architektura. Murator" 2004, no. 2, pp. 63–70.

Sitko A., Szafarczyk S., *Technologie architektury – Ambasada Królestwa Niderlandów w Warszawie* (Eng. Architectural technologies - Embassy of the Kingdom of the Netherlands in Warsaw), "Architektura. Murator" 2004, no. 2, pp. 90–97.

Stiasny G., *Konkursy na nowe budynki ambasad w Warszawie* (Eng. Competitions for new embassy buildings in Warsaw), "Architektura. Murator" 2004, no. 2, pp. 44–59.

Ulrich P., *Die franzoesische Vertretung am Pariser Platz will trotz hoher Sicherheitsanforderungen ein offenes Haus sein: Bald bietet die Botschaft Fuehrungen durch das neue Gebaeude* (Eng. The French representation on Pariser Platz wants to be an open house despite high security requirements: Soon the embassy will offer guided tours of the new building), "Berliner Zeitung", 24 I 2003.

Internet sources

DSC1100 K8 Portable Barriers, Delta Scientific Corporation, https://deltascientific.com/product/portable-barrier-dsc1100/ [accessed: 28 V 2023].

Embassy Perimeter Improvement Concepts & Design Guidelines, Department of State Bureau of Overseas Buildings Operations, June 2011, https://www.scribd.com/document/261408078/Embassy-Perimeter-Improvement-Concepts-Design-Guidelines [accessed: 12 V 2023].

Encyklopedia humanistyczna (Eng. Encyclopedia of the humanities), http://encenc.pl/aha/ [accessed: 14 V 2023].

High Security Bollards, Delta Scientific Corporation, http://deltascientific.com/high-security/bollards/ [accessed: 28 V 2023].

http://www.google.pl/maps/ [accessed: 10 III 2015].

http://www.rogersmarvel.com/projects/NYSE/ [accessed: 28 V 2023].

https://deltascientific.com/wp-content/uploads/2021/01/90140-Rev-B-DSC207S-General-Arrangement.pdf [accessed: 9 I 2023].

https://new-european-bauhaus.europa.eu/index_en [accessed: 5 VII 2023].

IP500 High Security Portable Barriers, Delta Scientific Corporation, http://www.deltascientific.com/high-security/portable-barriers/ip500 [accessed: 28 V 2023].

Kades A., *Cypriot embassy severely damaged in Athens bomb blast*, CyprusMail, 24 XI 2015, http://cyprus-mail.com/2015/11/24/cypriot-embassns-bomb-attack/ [accessed: 24 XI 2015].

European Commission, *Security by Design: Protection of public spaces from terrorist attacks*, https://www.urbanagenda.urban-initiative.eu/news/security-design-protection-public-spaces-terrorist-attacks [accessed: 20 IV 2023].

Oakes Ch.G., *The Bollard: Crash- and Attack-Resistant Models*, Whole Building Design Guide, 9 II 2016, https://www.wbdg.org/resources/bollard-non-crash-and-non-attack-resistant-models [accessed: 9 I 2023].

Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks, series: Risk Management Series, https://www.fema.gov/sites/default/files/2020-08/fema427.pdf [accessed: 30 V 2023].

Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, series: Buildings and Infrastructure Protection Series, http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf [accessed: 16 V 2023].

Report of the Secretary of State's. Advisory Panel on Overseas Security, http://www.fas.org/irp/threat/inman/ [accessed: 5 VII 2023].

Site and Urban Design for Security. Guidance Against Potential Terrorist Attacks, series: Risk Management Series, https://www.fema.gov/sites/default/files/2020-08/fema430.pdf [accessed: 13 V 2023].

Sliding High Security Crash Rated Gates, Delta Scientific Corporation, https://deltascientific.com/high-security/sliding-gates/ [accessed: 28 V 2023].

U.S. Embassy security upgrades in Baku, Pernix Group, https://www.pernixgroup.com/project/baku-design-build-isat-security-upgrades/ [accessed: 10 I 2023].

Legal acts

Vienna Convention on Diplomatic Relations, drawn up in Vienna on April 18, 1961 (Journal of Laws of 1965, no. 37, item 232).

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0795&from=PL [accessed: 5 VII 2023].

Act of 24 July 2015 - Law on Assemblies (Journal of Laws of 2022, item 1389).

Agnieszka Dobrzyńska-Jarosz, PhD, Eng.

Architect, assistant professor in the Department of Public Utility Architecture, Fundamentals of Design and Environmental Design at the Faculty of Architecture, Wrocław University of Technology, member of the Lower Silesian Regional Chamber of Architects of the Republic of Poland.

https://doi.org/10.4467/27204383TER.23.032.18334

https://orcid.org/0000-0003-0949-6674

ANDRZEJ JARYNOWSKI

Agroterrorism involving biological agents and related threats in Poland and Europe in the context of the COVID-19 pandemic and the war in Ukraine

Abstract

With the growing threat of agroterrorism and the highest level of risk in Poland and the European region since the Biological and Toxin Weapons Convention (1972) and the Additional Protocols to the Geneva Conventions (1977) came into force, it is important to analyse the challenges in the area of biosecurity and food security and make recommendations. The analysis carried out by the author of this article indicates that the COVID-19 pandemic has contributed to the dissemination of knowledge of the basics of microbiology and epidemiology and to the increased availability of low-cost, portable microbiological diagnostics, which may also have negative effects. The analysis took into account the possibility of foreign intelligence influencing food production in Poland, e.g. through disinformation via social media. Conclusions of the analysis include: expanding monitoring of the expert community and social media, strengthening the vigilance of food producers and agricultural experts, simulating introduction scenarios, studying radicalisation processes and using epidemiological assessment tools in case of alarming events.

Keywords:

agroterrorism, bioterrorism, food security, biopolitics, INFOOPS

No event in the 21st century has changed social life in Europe as much as the COVID-19 pandemic[1] and the war in Ukraine[2]. The spread of the SARS-CoV-2 virus made microbiology and epidemiology one of the dominant topics of interest to a large part of the public for a time. Although public discourse during the COVID-19 pandemic was mainly concerned with human viruses, the knowledge gained can be extrapolated to infections caused by other pathogenic microorganisms.

Russia's war against Ukraine and rising fertiliser prices are deepening the global food crisis[3]. Russia, seeking, among other things, to undermine Ukraine's ability to export agricultural and food products, attacked Ukraine's transport infrastructure and de facto blocked Black Sea ports from the end of February to the end of July 2022 (exports of grain products from Ukrainian ports have resumed since August 2022 under cross-agreements via the UN and Turkey[4]).

The focus of the article is on the following questions[5]:

1. What impact has the COVID-19 pandemic and the war in Ukraine had on the agroterrorism phenomenon?
2. What benefits can potential terrorists achieve through agroterrorism and bioterrorism in a hybrid war environment?
3. To what extent has the previous barrier of having knowledge of microbiology and epidemiology, epizootics, epiphytic plants and having laboratory equipment and certain skills, which represents

---

[1] A. Jarynowski, M. Stochmal, J. Maciejewski, *Przegląd i charakterystyka prowadzonych w Polsce badań na temat społecznych uwarunkowań epidemii COVID-19 w jej początkowej fazie* (Eng. Overview and characteristics of ongoing research in Poland on the social determinants of the COVID-19 epidemic in its initial chase), "Bezpieczeństwo. Obronność. Socjologia" 2020, vol. 13, pp. 38–87.

[2] J. Maciejewski, *Grupy dyspozycyjne w systemie bezpieczeństwa państwa* (Eng. Deployment groups in the state security system), XXIII International Seminar series "Social systems research methodology", Wrocław, 7 IV 2022.

[3] B. Radziejewski, *Widmo krąży po świecie. Widmo głodu* (Eng. A spectre looms over the world. The spectre of hunger), Nowa Konfederacja, 25 V 2022., https://nowakonfederacja.pl/widmo-krazy-po-swiecie-widmo-glodu/ [accessed: 12 VIII 2022].

[4] *Black Sea Grain Initiative*, Wikipedia, https://en.wikipedia.org/wiki/Black_Sea_Grain_Initiative [accessed: 12 VIII 2022].

[5] The article is a continuation of the theses contained in the paper entitled: *(Re-)Emergence of agroterrorism during the food crisis*, presented by the author on 20 July 2022 for the NATO Centre of Excellence for Military Medicine, and a presentation entitled: *Agro/bio-terrorism in Europe? Analysis of selected suspicious biological events (significant from the One Health perspective) after 24.02.2022*, delivered on 25 X 2022 at the NATO BioMed Panel.

a certain limitation on the possibility of undertaking bio- and agroterrorist activities, been lowered for potential terrorists such as lone wolves and small organisations?
4. Who (inspired by whom), how and when could carry out an act of agroterrorism in Poland and the European region and what would the consequences be?
5. How can disinformation about biological weapons, food security and the COVID-19 pandemic affect the public?
6. What areas of interest related to biological weapons and biosecurity are most important in the face of contemporary threats?

Agroterrorism versus bioterrorism

The term agroterrorism[6] implies not only a biological attack on livestock and crop production (this dimension is included in the broader term bioterrorism), but also an attack on means of transport and transportation, infrastructure, agricultural inputs, as well as having a negative impact on the social determinants of production (another criminal or terrorist action of the food type). Agroterrorism can involve the use of biological, mechanical, chemical or IT means, but for the purposes of this article only biological agents (along with supporting actions) will be discussed.

Activities of an agroterrorist nature can be carried out by a variety of actors. Due to the possibility of detection, these activities can be divided into:

- small-scale activities carried out by small terrorist organisations (e.g. environmental or religious organisations) that do not have to face detection;
- hybrid actions below the threshold (i.e. actions where protective mechanisms will not be effectively implemented) of the 1972 *Biological and Toxin Weapons Convention* (BTWC[7]) and the 1977 Additional Protocols to the Geneva Conventions (on the Protection

[6] H. Keremidis et al., *Historical Perspective on Agroterrorism: Lessons Learned from 1945 to 2012*, "Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science" 2013, vol. 11, pp. 17–24. https://doi.org/10.1089/bsp.2012.0080.

[7] *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, done at Moscow, London and Washington on 10 April 1972.*

of Victims of International Armed Conflicts[8]) undertaken by states (e.g. attacks on supply chains or polarisation of food producers) or obstruction by aggressors to prove an act of terrorism. In these cases, much more weight is given to concealing the real principal.

The aforementioned legal acts are currently the two main international norms addressing the phenomenon of agro-terrorism. Pursuant to Article 1 of the Biological Weapons Convention: *Each State Party (...) undertakes never in any circumstances to develop, produce, stockpile or otherwise acquire or retain: 1) microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes*. It is worth mentioning that on 8 July 2022, contracting states to the Biological Weapons Convention were notified that Russia had triggered Article 5 of the Convention, obliging parties to cooperate with each other in resolving difficulties that may arise in connection with the purpose or application of the Convention, and called for a formal consultative meeting[9]. It took place from 1-5 September 2022 (this was the second time in history, following the 1997 Cuba vs USA case).

Article 54 of Protocol I and Article 14 of Protocol II to the Geneva Conventions concern the protection of assets essential to the survival of civilians. Pursuant to Article 14: *Starvation of civilians as a method of combat is prohibited. It is therefore prohibited to attack, destroy, remove or render useless, for that purpose, objects indispensable to the survival of the civilian population, such as foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works.*

It is known that pathogens used for agroterrorism activities were in the arsenal of the Soviet[10] and US militaries and other countries[11]. They were used before 1972, and therefore before the Biological Weapons

---

[8] *Additional Protocols to the Geneva Conventions of 12 August 1949, concerning the Protection of Victims of International Armed Conflicts (Protocol I) and the Protection of Victims of Non-International Armed Conflicts (Protocol II), drawn up in Geneva on 8 June 1977.*

[9] F. Lentzow, J. Littlewood, *Russia finds another stage for the Ukraine "biolabs" disinformation show*, Bulletin of the Atomic Scientists, 8 VII 2022, https://thebulletin.org/2022/07/russia-finds-another-stage-for-the-ukraine-biolabs-disinformation-show/ [accessed: 12 VIII 2022].

[10] M. Leitenberg, R.A. Zilinskas, *The Soviet biological weapons program: A history*, Cambridge 2012.

[11] Л.П. Жиганова, Биотерроризм *и* Агротерроризм-Реальная Угроза Биобезопасности Общества, "США и Канада: Экономика, Политика, Культура" 2004, vol. 417, no. 9, pp. 3–25 (it is worth exercising caution when analysing Russian sources, as there is a lot of propaganda in them, especially in the military field).

Convention (the Geneva Protocol of 1925 dealt only with biological agents, among other means, affecting humans in wartime[12]), including by countries that later joined NATO (this is the opinion among epizootiologists and epiphytologists). For example, in 1971, the United States most likely intentionally introduced the African Swine Fever Virus (ASFV) to Cuba[13], as confirmed by, among others, Ukrainian participants in the Soviet epizootiological mission to Cuba[14].

What is worrying is that, despite the existence of the Biological Weapons Convention, there are still at least 18 countries and territories (China, France, Iraq, Iran, Israel, Japan, Canada, North Korea, Cuba, Libya, Germany, South Africa, Russia, the United States, Syria, Taiwan, the United Kingdom and the terrorist organisation known as the Islamic State) almost certainly in possession of such weapons and in all likelihood, according to Stanisław Maksymowicz, a health expert, working on their new types[15]. The most expensive Biological Safety Level (BSL) 3 and 4 laboratories are not needed for this.

There are some important differences between bioterrorism in the narrow sense and agroterrorism. Infectious diseases can be classified according to the type of host. In Poland, the division into, among others, is used[16]:

- human hosts (diseases in this group are of greatest interest to the general population, special services and the medical community);
- animal hosts that are also vectors for diseases transmissible to humans (e.g. rabies, Lyme disease, outbreaks of highly pathogenic avian influenza in mammals, SARS-CoV-2 outbreaks in mink; they

[12] *Protocol concerning the prohibition of the use of asphyxiating, poisonous or similar gases and bacteriological agents in war*.

[13] Б. Стегній, А. Герилович, А. Бузун, *Африканська чума свиней: історія, сьогодення та перспективи*, Київ 2015.

[14] Private communication of the author of the article with current and retired employees of the Institute of Experimental Veterinary Virology in Kharkiv.

[15] S. Maksymowicz, Atak biologiczny i agroterrorystyczny na Polskę. Jakie scenariusze są prawdopodobne? (Eng. Biological and agroterrorist attack on Poland. What scenarios are likely?), Nowa Konfederacja, 31 V 2022, https://nowakonfederacja.pl/atak-biologiczny-i-agroterrorystyczny-na-polske-jakie-scenariusze-sa-prawdopodobne/ [accessed: 7 XI 2022].

[16] A. Jarynowski, A. Semenov, V. Belik, *Perception of infectious diseases with animal and humans hosts on the Polish internet*, 20th Congress of the International Society for Animal Hygiene, Berlin, 5–7 X 2022, http://interdisciplinary-research.eu/wp-content/uploads/2022/08/Abstract-form-ISAH_jarynowski_corr.pdf. [accessed: 7 XI 2022].

are of moderate interest to the general population, with some peaks of a local nature; they receive attention from the special services, medical and veterinary communities);
– animal or plant hosts (diseases affecting these host groups are of virtually no interest to the general population and of little interest to the special services; they are of interest mainly to the veterinary and phytosanitary services and to stakeholders - farmers and ranchers, foresters, hunters, environmentalists).

In some countries, such as the UK, Ireland, Australia or New Zealand, awareness of epidemiological and food security appears to be very high (which may manifest itself, for example, in the number of scientific articles being written there on these issues[17]). This is also due to certain geographical factors and Poland is unlikely to match such a level of knowledge and exemplary supervision. However, it is apparent that there is a move towards North American and Western European standards in building knowledge of food safety or bioterrorism (e.g. it is taught in agricultural and biochemistry studies[18]). In Polish society, however, knowledge of and interest in these issues are still low, despite information campaigns[19].

In the case of a biological attack, attackers may perceive the following factors as giving agroterrorism an advantage over bioterrorism[20]:
– infectious material can be collected, processed and transported with minimal risk to one's own health;
– the risk of detection in the run-up to an attack is low (relatively weak oversight by intelligence, veterinary or phytosanitary agencies of biological agents[21] that do not pose a threat to humans);

---

[17] More than half (768 out of 1,336, i.e. 57%) of the scientific papers searched in the Scopus database using the key phrases "invasive species" and "infectious" are from at least one of these countries.

[18] P. Cwynar, *Bioterroryzm – syllabus*, Wrocław University of Life Sciences, 2021, https://sylabus.upwr.edu.pl/pl/document/7562fe08-5a02-4db5-8d31-d7144fdd99bb.pdf [accessed: 1 XI 2022].

[19] A. Jarynowski, A. Semenov, V. Belik, *Perception of infectious diseases…*

[20] A. Jarynowski, Ł. Krzowski, *BIO (AGRO) Terrorism/Crime in post-covid era in context of massive scale dissemination of microbiology/epidemiology knowledge*, "DiMiMED – International Conference on Disaster and Military Medicine", Düsseldorf, 15–16 XI 2021, https://events.military-medicine.com/media/landingpage/25/attachment-1639063402.pdf [accessed: 12 VIII 2022].

[21] Harmful biological agents such as a virus, bacterium, protozoan, fungus or toxin (editor's note).

– low cost yet high economic and food security impact (highly cost--effective measure[22]);
– ideological and utilitarian motivations of potential agroterrorists[23], for example the EU Green Deal programme - attacks may be motivated by social tensions caused by the climate crisis and the associated need to reduce greenhouse gas emissions by reducing animal production; animal rights and animal welfare[24] - e.g. attacks on abattoirs or factory farms; unclean animals in Islam (e.g. pigs).

In contrast, the disadvantages of a biological attack, from the perspective of the attackers, compared to bioterrorism are[25]:

– no panic effect and little interest in animal or plant diseases among the general public[26] (so getting a terrorist not related to agriculture or animals may be difficult);
– ethical dissonance[27] for a potential agro-terrorist encouraged to act on ideological grounds.

In the context of the phenomenon of agroterrorism, it is worth mentioning the idea of One Health, according to which the concept of health should not be seen solely in human terms, but should also include the well-being of animals and the environment as a whole[28]. It is a concept that views the health of humans, animals, plants and the environment as elements of a single and interdependent system, in which human health

[22] J. Monke, *Agroterrorism: Threats and preparedness*, https://sgp.fas.org/crs/terror/RL32521.pdf, p. 1 [accessed: 7 VIII 2022].

[23] *Debata Bezpieczeństwo żywnościowe Europy w świetle nadchodzących wyzwań* (Eng. Debate on European food security in the light of upcoming challenges), Instytut Gospodarki Rolnej, 2022, https://instytutrolny.pl/debata-bezpieczenstwo-zywnosciowe-europy-w-swietle-nadchodzacych-wyzwan/ [accessed: 2 XI 2022]. Material has been archived: https://web.archive.org/web/20221104152532/https://instytutrolny.pl/debata-bezpieczenstwo-zywnosciowe-europy-w-swietle-nadchodzacych-wyzwan/.

[24] *Jedno zdrowie. Ludzie i inne gatunki* (Eng. One Health. Humans and other species), H. Mamzer, P. Białas (sci. eds.), Wrocław 2022, p. 11.

[25] A. Jarynowski, Ł. Krzowski, *BIO (AGRO) Terrorism/Crime in post-Covid era*...

[26] A. Jarynowski, A. Semenov, V. Belik, *Perception of infectious diseases*...

[27] H. Mamzer, *Choroba jako zjawisko społeczne. Analiza walki z afrykańskim pomorem świń* (Eng. Disease as a social phenomenon. An analysis of the fight against African swine fever), "Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2020, vol. 82, no. 2, pp. 281–297. https://doi.org/10.14746/rpeis.2020.82.2.19.

[28] S.Y. Essack, *Environment: the neglected component of the One Health triad*, "The Lancet Planetary Health" 2018, vol. 2, no. 6, e238-e239. https://doi.org/10.1016/S2542-5196(18)30124-4.

is inextricably linked to the wellbeing of animals and the environment, and diseases transmitted between humans, animals and the environment are strongly interconnected. Such a holistic approach is needed because there is a close relationship between human health, the condition of farm animals and wildlife and plant phytopathology, among others, and the differences between these groups have been introduced by humans and are largely artificial. Social determinants or infection control methods are in principle the same, but knowledge is built up in a siloed way (separately for fields such as medicine, veterinary medicine and plant protection). In the opinion of the author of this article, this siloed approach is maintained by officials[29] (separate laws on the prevention and control of infections and infectious diseases in humans; on the protection of animal health and the control of infectious diseases in animals; on the protection of plants against agrophages), and administrative procedures aimed at reintegration by the civil service (especially the combined administration) of knowledge from different fields are implemented in isolation from biological paradigms[30]. The idea of One Health is gaining more and more importance and popularity. Following Poland's accession to NATO, the organisational structure of the military preventive medicine centres was adapted to the counter-threat paradigm developed within the framework of this approach (in accordance with NATO models adapted to Polish conditions by, among others, Jarosław Foremny)[31].

---

[29] It is an opinion formulated on the basis of the author's experience in combating ASF, HPAI in poultry and mammals, COVID-19, work related to attempts to clarify and limit the effects of the ecological disaster on the Oder river, as well as minimising the risks of biological contamination of grain from Ukraine. In order to fully understand the issue, it is necessary to familiarise oneself with the applicable sanitary, veterinary and food law in the form of: EU regulations on the control of infectious diseases of humans, animals and plants; laws on the activities of the central government administration and local government units and the functioning of the relevant inspections; executive acts (in the form of regulations of the relevant ministers and the Prime Minister) on the cooperation of national inspections.

[30] M. Kędzierski, *Integracja czy połączenie. Analiza możliwości zwiększenia efektywności działania inspekcji weterynaryjnej oraz ochrony roślin i nasiennictwa* (Eng. Integration or merger. An analysis of options to increase the efficiency of the veterinary and plant protection and seed inspections), https://efrwp.pl/publikacje/integracja-czy-polaczenie-analiza-mozliwosci-zwiekszenia-efektywnosci-dzialania-inspekcji-weterynaryjnej-oraz-ochrony-roslin-i-nasiennictwa/ [accessed: 7 VI 2023].

[31] A list of these centres is available at: https://www.gov.pl/web/obrona-narodowa/wojskowe-osrodki-medycyny-prewencyjnej [accessed: 2 III 2023].

The impact of the COVID-19 pandemic on the phenomenon of agroterrorism

During the pandemic, many people were able to acquire knowledge related to the transmissibility of infectious diseases previously reserved for a small group of specialists. One of the counter-epidemic measures was to familiarise the public with this knowledge in order to reduce the incidence of COVID-19 (e.g. through the use of personal protective equipment or self-testing). This knowledge could be used in a variety of ways. The pandemic also forced advances in selected scientific fields, exposed global biological vulnerabilities and refocused attention on the possibility of targeted attacks using biological agents, which NATO experts identified as a possible risk factor[32]. Certain diagnostic techniques, such as point of interest/point of care (POI/POC), or portable diagnostics, have become more common, and therefore more accessible. In addition, there are advances in a number of biological, engineering and military sciences that also have the potential for dual use research of concern (DURC) and can be used to plan and execute terrorist attacks or sabotage using biological agents. In general, there have been scientific and technological advances in the fields of medicine, biology and technology for decades (as discussed, among others, at the nine BTWC review conferences), but according to the author, the changes in the last few years have been by leaps and bounds. Questions remain about the motivations for actions against the common good[33] and the processes leading to radicalisation. The COVID-19 pandemic has contributed to[34]:

– increasing the ease of obtaining infectious material (knowledge of basic microbiology and pathogenesis). This consists of practice in sample collection and preparation (widespread self-testing on COVID-19), knowledge of immunological processes, viral load dynamics, seroconversion, susceptibility of individual organs and systems. In addition, to the development of synthetic biology using computational machine learning models[35] to predict toxicity

[32] S. Clement, *Biological Threats: Technological Progress and the Spectre of Bioterrorism in the Post-Covid-19 Era*, https://www.nato-pa.int/download-file?filename=/sites/default/files/2022-01/024%20STCTTS%2021%20E%20rev.%201%20fin%20-%20%20BIOLOGICAL%20THREATS.pdf [accessed: 8 VIII 2022].

[33] A. Jarynowski, M. Stochmal, J. Maciejewski, *Przegląd i charakterystyka prowadzonych w Polsce badań...*, p. 73.

[34] A. Jarynowski, Ł. Krzowski, *BIO (AGRO) Terrorism/Crime in post-Covid era...*

[35] S. Clement, *Biological Threats: Technological Progress...*

or virulence and infectivity in different areas or ultimately genetic modification of bioagents;
- simplifying the verification of the infectious agent (access to diagnostics). The rapid advances in science resulting in the widespread availability of low-cost, portable microbiological diagnostics, e.g. in the form of cassette tests (especially the dissemination of practical skills in the use of these tools to a wider audience), although primarily used to combat the COVID-19 pandemic, also has side effects;
- increasing the ease of introduction (knowledge of basic epidemiology, including transmission pathways) - understanding the principles of the epidemiological triad (infectious agent, host and environment where conditions for transmission exist), transmissibility of infectious material, seasonality, understanding how epidemiological surveillance systems work.

The progress can be illustrated using the example of potential scenarios for the intentional introduction of ASF virus under pre-[36] and postcovid[37] conditions in Poland and Europe. It should be stressed that due to the technical drawbacks of using biological weapons against humans (the political consequences of their use against an aggressor, such as Russia, could be very serious) their use seems unlikely[38]. Agroterrorism, on the other hand, is a real threat, especially as such actions need not be spectacular in nature and can be carried out below the detection threshold. Smaller local operations using sleeper agents are possible. The scale of agroterrorism can be difficult to estimate and the repertoire of actions

[36] A. Jarynowski et al., *ASF jako zagrożenie biologiczne w Polsce i na świecie* (Eng. ASF as a biological threat in Poland and worldwide), in: *Bezpieczeństwo regionalne. Węzłowe problemy i procesy*, P. Bajor (ed.), Kraków 2021, pp. 239–254. https://doi.org/10.12797/9788381383899.14.

[37] A. Jarynowski, Ł. Krzowski, V. Belik, *Afrykański pomór świń: epizootiologia, ekonomia i zarządzanie kryzysowe w kontekście naturalnego bądź intencjonalnego wprowadzenia* (Eng. African swine fever: Epizootiology, economics and crisis management in the context of natural or intentional introduction), "Studia Administracji i Bezpieczeństwa" 2021, vol. 11, no. 11, pp. 129–153. https://doi.org/10.5604/01.3001.0015.6752.

[38] G. Kessler, *How the right embraced Russian disinformation about 'U.S. bioweapons labs' in Ukraine*, "The Washington Post", 11 III 2022, https://www.washingtonpost.com/politics/2022/03/11/how-right-embraced-russian-disinformation-about-us-bioweapons-labs-ukraine/ [accessed: 7 VIII 2022].

is truly wide. Its effect may be to undermine food production and social polarisation in Poland and in the European region[39].

Epidemiological, epizootic, epiphytic analysis in the context of food security

Biological agents that endanger humans are quite well studied by the Polish scientific community. A search conducted by the Military University of Land Forces shows that between 2009 and 2018, an average of 10 scientific papers per year were published in the Polish literature on these agents[40]. Zoonotic agents (causing zoonoses) remain a major area of research, as they are of medical importance. In contrast, the problem of infections not affecting the human population is largely overlooked. The topic of food safety is also popular (between 2009 and 2021 there were about 15 thematic papers per year by Polish authors[41]). Biological agroterrorism factors, on the other hand, are rarely discussed outside the agricultural science community. In the opinion of national experts, so far Poland has not appeared to be directly threatened by agroterrorism, especially towards plants[42], which may be evidenced by the carelessness of Poles in dealing with invasive species or seeds of unknown origin. The low level of interest in the threat of agroterrorism against plants (as opposed to actions against

[39] A. Jarynowski et al., *African Swine Fever – potential biological warfare threat*, preprint, https://easychair.org/publications/preprint/vjFf [accessed: 7 VIII 2022].

[40] *Broń masowego rażenia, broń biologiczna, broń chemiczna, broń jądrowa. Cz. 2* (Eng. Weapons of mass destruction, biological weapons, chemical weapons, nuclear weapons. Part 2), K. Mordzak (elaborated), Wrocław 2019, https://www.wojsko-polskie.pl/awl/u/96/0c/960cad22-5698-4356-b8f5-38117fb19499/bron_cbn.pdf [accessed: 7 VIII 2022].

[41] *Bezpieczeństwo żywnościowe*, K. Mordzak (elaborated), Wrocław 2021, https://www.wojsko-polskie.pl/awl/u/50/d4/50d46baf-332b-4acb-aeb3-8f5b17777590/bezpieczenstwo_zywnosciowe.pdf [accessed: 7 VIII 2022].

[42] J. Lipa, *Agroterroryzm – wyzwaniem dla kwarantanny i ochrony roślin* (Eng. Agroterrorism - a challenge for quarantine and plant protection), "Progress in Plant Protection" 2006, vol. 46, no. 1, p. 167; M. Lenda et al., *Misinformation, internet honey trading and beekeepers drive a plant invasion*, "Ecology Letters" 2021, vol. 24, no. 2, pp. 165–169. https://doi.org/10.1111/ele.13645; M. Lenda et al., *Effect of the Internet Commerce on Dispersal Modes of Invasive Alien Species*, "PLoS ONE" 2014, vol. 9, no. 6, p.e99786. https://doi.org/10.1371/journal.pone.0099786.

animals[43]), caused, inter alia, by the lack of documentation of such cases, may lead to dormant vigilance.

Potentially hostile terrorist organisations (funded by regimes such as the Russian Federation or China, or parastatal entities such as the Islamic State) can make use of a wide repertoire of tools and capabilities, such as mathematical modelling[44] and artificial intelligence, to optimise the effects of agroterrorist action. In particular, lone wolves (terrorists acting alone, not part of a larger terrorist network)[45] are worth noting whose activities are characterised by low budget and so-called kitchen microbiology or do-it-yourself microbiology. The increase in knowledge and development of technology caused by the COVID-19 pandemic may favour their agroterrorist activities. There are certain groups of medical, veterinary, agricultural or environmental and biological professions that, because of their expertise, may predispose them technically to agroterrorism. However, it is worth emphasising that the transmission patterns of infectious animal and plant diseases are relatively well known (due to the possibility of experimentation as opposed to human experimentation), and therefore a veterinary or plant protection specialist will more easily develop an effective introduction plan than a physician or representative of another medical profession. In the case of human diseases, there is less epidemiological knowledge and, despite billions of dollars spent on research, the basic characteristics of SARS-CoV-2 are still not known[46], e.g. ID50 (median infective dose)[47].

The use of the most dangerous animal and plant pathogens, such as ASFV or *Xylella fastidiosa* (a gram-negative bacterium that inhabits

---

[43] M. Wiśniewska, *The food terrorism – the essence and the methods of systemic defense*, "Journal of Modern Science" 2023, vol. 50, no. 1, pp. 331–349. https://doi.org/10.13166/jms/161535.

[44] A. Jarynowski, A. Grabowski, *Modelowanie epidemiologiczne dedykowane Polsce* (Eng. Epidemiological modelling dedicated to Poland), Portal CZM, 2015, http://www.czm.mif.pg.gda.pl/wp-content/uploads/fam/publ/jarynowski2.pdf [accessed: 7 VIII 2022].

[45] C.R. MacIntyre et al., *Converging and emerging threats to health security*, "Environment Systems and Decisions" 2018, vol. 38, no. 2, pp. 198–207. https://doi.org/10.1007/s10669-017-9667-0.

[46] S. Karimzadeh, R. Bhopal, H. Nguyen Tien, *Review of infective dose, routes of transmission and outcome of COVID-19 caused by the SARS-COV-2: comparison with other respiratory viruses*, "Epidemiology and Infection" 2021, vol. 149, e96. https://doi.org/10.1017/S0950268821000790.

[47] ID50 - the average infectious dose under natural conditions that causes 50% of those exposed to develop a disease.

the conducting tissue of plants), in disease-free areas can have serious consequences. Exports of products in infected or quarantine agrophage areas could be banned, resulting in losses of up to millions of euros per month.

Animal production

On a global scale, the main activities to supervise the risk of agroterrorism are carried out by the Food and Agriculture Organisation of the United Nations (FAO) and at European Union level by the European Food Safety Authority (EFSA). In Poland, the Veterinary Inspection is responsible for animal biosecurity[48]. The development of epizootics depends on a number of factors, such as the density and size of farms, the level of bioassurance, interactions with the environment[49]. Epizootics are characterised by an average rate of development, but usually a dozen or more kilometres per year (not taking into account the long-range leaps outside the functional area that happen via humans[50]). By means of pathogen introduction, significant disorganisation of animal production (e.g. cutting supply chains) can be achieved in the medium term.

The World Organisation for Animal Health (WOAH, formerly Office International des Epizooties, OiE) used livestock diseases for its 2018 classification (this classification has now fallen out of use). Similarly, the US Centers for Disease Control and Prevention (CDC) classifies the causative agents of animal diseases into groups based on their level of risk[51]:

– group A is the highest risk - they cause severe disease, spread rapidly, easy to acquire infectious material, e.g. ASF, FMD (Foot and

[48] At: https://bip.wetgiw.gov.pl/asf/mapa/ you can observe biohazard maps at national level, and at: https://empres-i.apps.fao.org – global.

[49] A. Jarynowski, V. Belik, *African Swine Fever (ASF) Virus propagation in Poland (Spatio-temporal analysis)*, preprint, https://www.researchgate.net/publication/338436134_African_Swine_Fever_ASF_Virus_propagation_in_Poland_Spatio-temporal_analysis [accessed: 7 VIII 2022]. https://doi.org/10.13140/RG.2.2.29807.6167.

[50] A. Jarynowski, V. Belik, *Spatio-temporal analysis of African Swine Fever Spread in Poland with network perspective*, preprint, https://www.academia.edu/43262326/Multilayer_network_approach_to_African_Swine_Fever_Spread_in_Poland [accessed: 12 VIII 2022].

[51] OiE, *Classification of diseases notifiable*, https://www.oie.int/en/animal-health-in-the-world/the-world-animal-health-information-system/old-classification-of-diseases-notifiable-to-the-oie-list-a/ [accessed: 29 VII 2022].

Mouth Disease), CSF (Classical Swine Fever), HPAI (Highly Pathogenic Avian Influenza);
– group B is medium risk - causes moderately serious diseases with low mortality rates, spreads moderately easily, e.g. brucellosis, salmonellosis.

World-class veterinary epidemiologist Dirk Pfeifer said that ASF (...) *is probably the most serious animal disease the world has had for a long time, if not ever*[52]. The ASF-induced pork shortage in China may have contributed to the transmission of SARS-CoV-2 from animals to humans, as it forced the search for alternative protein sources in wildlife[53]. Certain organisations or individuals, acting for various motives, i.e. ideological, political or economic, may benefit from the introduction of ASF. A potential agroterrorist (coming from a naturalist background or no background at all, but having studied the biological mechanisms governing infectious diseases during the two years of the pandemic) will now be able to collect material and verify its infectivity and optimally introduce the pathogen into the selected area. Scenarios for the introduction of the ASF virus, including into Western Europe and western Poland, were presented by the article's author in September 2019 at the 3rd Jagiellonian Interdisciplinary Security Conference[54] and in October 2019 at the 44th BIOMED-EP meeting via the Polish delegation at NATO headquarters in Brussels[55], i.e. before the virus 'jumps' to western Poland and Germany[56]. A distinction must be made between reports based on conspiracy theories, e.g. about helicopters dropping frozen wild boar bodies[57], and real deliberate actions by potential terrorists.

---

[52] D. Normile, *African swine fever keeps spreading in Asia, threatening food security*, "Science", 2019, https://www.science.org/content/article/african-swine-fever-keeps-spreading-asia-threatening-food-security [accessed: 12 VIII 2022]. Translations in the article are from the author (editor's note).

[53] Wei Xia et al., *How One Pandemic Led To Another: Asfv, the Disruption Contributing To Sars-Cov-2 Emergence in Wuhan*, preprint, https://www.researchgate.net/publication/349628301_How_One_Pandemic_Led_To_Another_Asfv_the_Disruption_Contributing_To_Sars-Cov-2_Emergence_in_Wuhan [accessed: 7 VIII 2022]. https://doi.org/10.20944/preprints202102.0590.v1.

[54] A. Jarynowski et al., *ASF jako zagrożenie biologiczne w Polsce*...

[55] A. Jarynowski et al., *African Swine Fever – potential biological*...

[56] A. Jarynowski, Ł. Krzowski, V. Belik, *Afrykański pomór świń*...

[57] *Zarażone ASF dziki spadają z nieba? Mające być dowodem zdjęcie budzi poważne wątpliwości* (Eng. ASF-infected wild boars fall from the sky? The supposed proof photo raises serious doubts), Lublin112.pl, 22 VII 2018, https://www.lublin112.pl/zarazone-asf-dziki-

For the sake of illustration, it is worth outlining a case study of a feasibility study for different potential introduction paths, involving the following steps[58]:

- collection of infectious material (from wild boar carcasses, pork products, delivery by secret services or own breeding);
- processing of material and preparation for optimal transport (preparation of blood, tissue, body pieces, inoculum[59]);
- introduction of infection (choosing the time and the targets and then injecting or feeding or watering wild boar or pigs) with infectious material.

The lack of success in combating infectious animal diseases became one of the reasons for the tensions between food industry representatives - government - environmentalists, which occurred in January 2019 (protests against sanitary shooting of wild boars[60]), in October 2020 (projects such as animal welfare, the Five for Animals, combating ASF and HPAI[61]) or in July 2022 (among others, the issue of importing food products from Ukraine and the solidarity of Polish farmers with Dutch farmers)[62]. The scale of the agricultural protests, despite the COVID-19 pandemic and the war, is clear. In Poland they are organised on a smaller scale, but in other EU countries they are larger in scope and more violent. Animal rights activists have already carried out acts of diversion during the full Russian invasion of Ukraine (February 2022). On 19-20 June 2022, they caused the deaths

spadaja-nieba-majace-byc-dowodem-zdjecie-budzi-powazne-watpliwosci/ [accessed: 7 VIII 2022].

58 A. Jarynowski, Ł. Krzowski, *BIO (AGRO) Terrorism/Crime in post-Covid era...*; A. Jarynowski et al., *ASF jako zagrożenie biologiczne w Polsce...*

59 *Inokulum* (Latin) – a suspension of virus particles, bacterial cells or fungal spores (sometimes fragments of filaments) pathogenic to a plant, prepared by a human being for the purpose of artificially infecting the plant (inoculation). From: Encyklopedia PWN, https://encyklopedia.pwn.pl/haslo/inokulum;3914841.html [accessed: 10 V 2023] – editor's note.

60 A. Jarynowski et al., *African Swine Fever Awareness in the Internet Media in Poland – exploratory review*, "E-methodology" 2019, vol. 6, no. 6, pp. 100–115. https://doi.org/10.15503/emet2019.100.115.

61 H. Mamzer, *Choroba jako zjawisko społeczne...*, p. 293.

62 A. Jarynowski et al., *Animal breeders protests in Polish Twitter - preliminary research*, preprint, http://interdisciplinary-research.eu/wp-content/uploads/2022/04/animal_related_protests_in_twitter_preprint_pdf.pdf [accessed: 12 VIII 2022].

of 130 animals and extensive material damage at piggeries and slaughterhouses in Bocholt and Schermbeck, Germany[63].
Climate change (and perceptions of it) is another factor that is intensifying environmental movements. Among other things, demands are being made to reduce animal production responsible for greenhouse gas emissions by reducing demand and supply. This is leading to the emergence of a new sub-category of environmentalists - potential participants in acts of agro-terrorism, as animal rights activists have so far been the main category of perpetrators[64].

Plant production

At EU level, the agrophages to be monitored or quarantined, i.e. the most dangerous pathogens, pests and weeds that reduce crop yields, are identified by the International Plant Protection Convention (IPPC) in cooperation with the FAO and EFSA. In Poland, the supervisory authority is the State Plant Health and Seed Inspection Service (PIORiN)[65]. Particular attention should be paid to the agrophages: *Xylella fastidiosa* (a bacterial pest of, inter alia, olive trees which, according to EFSA, is the most serious problem in the EU[66]), *Candidatus Liberibacter* solanacearum (a bacterium causing the potato disease known as zebra chip), *Ralstonia solanacearum* (a bacterium causing the potato disease known as slime mold) and *Colletotrichum fructicola* (a fungus causing a disease of fruit, e.g. apples). Due to specific epidemiological cycles in plant pathogenic agrophages (e.g. sowing with a seed cycle), the rate of spread of epiphytosis depends on many factors, such as crop structure, weather conditions and climate. The rate is usually slow - rarely exceeding a few kilometres per year (sometimes there are

[63] A. Deter, *50 vermummte Aktivisten blockieren Bocholter Schlachthof* (Eng 50 masked activists block Bocholt slaughterhouse), Topagrar, 20 VI 2022, https://www.topagrar.com/schwein/news/aktivisten-blockieren-bocholter-schlachthof-13131573.html [accessed: 7 VIII 2022].

[64] *Bridging the expertise of the animal health and law enforcement sectors,* https://www.woah.org/app/uploads/2023/02/building-resilience-against-agro-crime-and-agro-terrorism.pdf [accessed: 4 III 2023].

[65] At: https://www.sygnalizacja.agrofagi.com.pl agrophage risk maps can be observed at national level, and at: https://gd.eppo.int – global.

[66] European Food Safety Authority (EFSA), *Update of the Xylella spp. host plant database – systematic literature search up to 31 December 2021*, "EFSA Journal" 2022, vol. 20, no. 6, e07356. https://doi.org/10.2903/j.efsa.2022.7356.

long-range jumps due to human activity). Consequently, with the help of agrophages it is difficult to achieve results in a short time (the exception is the targeted use of locusts). However, the introduction of an invasive agrophage can have far-reaching effects on the ecosystem that are difficult to model or predict[67].

Colletotrichum fructicola is worth a closer look[68]. This pathogen spreads slowly. Infection can occur through direct contact with the mycelium and through the airborne route - spores can be carried short distances by wind and by mechanical vectors in the form of insects. Two outbreaks of infection have been reported in Italy and one in France between 2019 and 2021. Poland, which accounts for a third of EU apple production, has a high host potential. However, Colletotrichum fructicola is a climate-dependent pathogen (it is unlikely to survive winter in Poland outside of the fruit storage system), so intentional introductions for natural reasons and phytosanitary measures are only likely to be single-season.

Disinformation on biological weapons and food – a theoretical contribution

Biological weapons have enormous intimidation potential. This was demonstrated by the Russians when, with the subject of alleged secret US laboratories on Ukrainian soil, they began a series of public invectives by the Russian Ministry of Defence[69] in the form of a series of presentations in 2022 (10 and 17 March, 14 April, 27 May, 17 June, 7 July, 4 August, 3 and 19 September). It should be noted that the theme of infectious animal diseases, mainly ASF and avian influenza, ran through each of them. Igor Kirillov, commander of Russia's Radiological, Chemical and Biological Defence Forces, repeatedly stressed that the Russians had 'acquired' evidence

[67] A. Jarynowski, F. Lopez-Nunez, H. Fan, *How network temporal dynamics shape a mutualistic system with invasive species?*, preprint, https://arxiv.org/ftp/arxiv/papers/1407/1407.4334.pdf [accessed: 7 VIII 2022]. https://doi.org/10.48550/arXiv.1407.4334.

[68] EFSA Panel on Plant Health (PLH), *Pest categorisation of Colletotrichum fructicola*, "EFSA Journal" 2021, vol. 19, no. 8, e06803.

[69] И. Кириллов, *Тезисы брифинги начальника войск радиационной, химической и биологической защиты ВС РФ генерал-лейтенанта И.А. Кириллова* (material of the Ministry of Defence of the Russian Federation collected by the author from the Telegram channel, available from the author on e-mail request).

of biological experiments on humans, as well as pigs, wild boars, birds or insects, being carried out on Ukrainian territory[70]. At the UN Security Council session on 11 March 2022, there was a confrontation between the US and Russia[71]. In addition, on 8 July 2022 Russia triggered, as already mentioned, Article 5 of the Biological Weapons Convention and called for a formal consultative meeting. In August and September 2022, an inspection proceeding was held against the US and Ukraine (allegations or insinuations about Poland could have been made there, which is why the observation of a formal meeting of states parties to the Biological Weapons Convention was very important, as Poland is, after the US, Ukraine, Germany, the next target of Russian propaganda on biological weapons[72]). It is therefore worthwhile for Poland to prepare for this in advance (on 9 September 2022, at the formal meeting of states parties to the Biological Weapons Convention, the Polish representative presented a position in Geneva that coincides with that of the EU). According to US analysts, Russia may be attempting in this way to mask the use of biological agents as part of a staged incident or their use in support of tactical military operations[73]. In September 2022 Kirillov changed his stance, pointing to the nuclear threat. The reason may have been the failure of the biological weapons campaign.

The internal narrative within Russia[74] has long featured the theme of Poland developing biological weapons. Both in the media and in 'scientific' studies, there are anecdotes on the subject, some of which date back to the Polish-Moscow wars (from the 16th to the 18th century). Most allegations are based on the mythical Polish biological programme of the inter-war period developed during and after the Polish-Bolshevik war (1919–1939)[75] and as part of the activities of the Polish Underground

[70] Ibid.

[71] S. Maksymowicz, *Atak biologiczny i agroterrorystyczny na Polskę*...

[72] A. Jarynowski, Ł. Krzowski, S. Maksymowicz, *Biological mis(dis)-information in the Internet as a possible Kremlin warfare* (draft), https://zenodo.org/record/8081493 [accessed: 26 VI 2023].

[73] Ibid.

[74] I. Kiriya, *From "Troll Factories" to "Littering the Information Space": Control Strategies Over the Russian Internet*, "Media and Communication" 2021, vol. 9, no. 4, pp. 16–24. https://doi.org/10.17645/mac.v9i4.4177.

[75] There was indeed such a programme, but it concerned research into biological and toxin weapons protection, and enemy propaganda has exploited and is exploiting its existence for its own ends.

State (1939–1945). In Russia's external narrative, techniques used against Poland (mainly through Polish-language propaganda channels or channels resonating with Russian propaganda[76]) are primarily used to create anxiety[77].

To explore public engagement with biopolitical topics, it is worth using media monitoring[78]. Potentially pro-Kremlin accounts participating in the discourse on the war are also known to appear (more than 50 times more likely to be involved) in the discourse on the anti-covid and vaccine protests[79]. Consequently, quite a lot can be deduced about public sentiment from the dynamics of social media discourse, even in areas not necessarily at first sight related to the war (such as biopolitical issues). It is noteworthy that the rather unusual dynamics of interest in Germany in the COVID-19 vaccination with the Oxford/AstraZeneca vaccine[80] (and especially in vaccines' adverse events[81]) bear the hallmarks of foreign

[76] *Analiza i dekonstrukcja rosyjskich przekazów dezinformacyjnych oraz propagandowych na temat Polski i Polaków* (Eng. Analysis and deconstruction of Russian disinformation and propaganda messages about Poland and Poles), https://infowarfare.pl/realizowane-projekty/ [accessed: 25 VI 2023]; M. Marek, *Rosyjska dezinformacja w Polsce – cele i przekazy* (Eng. Russian disinformation in Poland - targets and messages), Centrum Badań nad Współczesnym Środowiskiem Bezpieczeństwa, 30 III 2022, https://infowarfare.pl/realizowane-projekty/ [accessed: 25 VI 2023].

[77] T. Helmus et al., *Russian social media influence: Understanding Russian propaganda in Eastern Europe*, Santa Monica 2018.

[78] A. Jarynowski, *Infodemiologia oraz infonadzór – doświadczenia doby pandemii* (Eng. Infodemiology and infosurveillance - the pandemic experience), in: *Epidemiologia i bezpieczeństwo CBRN. Nauka, innowacje, implikacje praktyczne*, A. Mróz-Jagiełło, J. Walczak (eds.), series: Epimilitaris, Zielonka 2022, pp. 235–248.

[79] When one draws 50 German-language Twitter accounts engaged simultaneously in anti-vaccine and anti-sanctions discourse during the COVID-19 pandemic and compares their engagement in war discourse at the start of the Russian invasion in 2022, one finds that on average 49 accounts can be classified as pro-Kremlin and only one as pro-Ukrainian. See: A. Jarynowski, *Pro-Kremlin German Twitter users are more likely to be involved in both anti-lockdown and anti-vaccine discourse than Anti-Kremlin users*, preprint, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4079045 [accessed: 7 VIII 2022]. https://dx.doi.org/10.2139/ssrn.4079045.

[80] D. Jemielniak, Y. Krempovych, *An analysis of AstraZeneca COVID-19 vaccine misinformation and fear mongering on Twitter*, "Public Health" 2021, vol. 200, pp. 4–6. https://doi.org/10.1016/j.puhe.2021.08.019.

[81] V. Belik, A. Jarynowski, *Elucidating the interplay of COVID-19 epidemic and social dynamics via Internet media in Germany*, on-line conference "Preparedness for future pandemics from a global perspective", 15 XI 2021, https://zenodo.org/record/6400773#.ZGRny3ZByUk [accessed: 7 VIII 2022].

intelligence interference (potentially Russian[82], but some analysts also point to Chinese[83] as part of overt and covert vaccine diplomacy[84]).

In Poland, distinguishing between the pro-Kremlin and anti-Kremlin narrative is not as easy as in Germany, where the invasion is supported more overtly. In Poland, it is less clear-cut[85] and requires more intensive work by services such as the Internal Security Agency, the Military Counterintelligence Service, as well as the National Security Bureau. It is worth emphasising that the way in which Russian propaganda is conducted varies from country to country or from medium to medium, so as a rule, Polish services should focus more on their own empirical analyses[86] than on the world literature (especially from the US[87]). Jarynowski and co-authors noted that certain accounts appeared in all discourses and often in atypical positions (e.g. in discourses on coronavirus[88] or lockdowns[89] appearing on the right, but acutely in the context of ASF eradication they clustered with

[82] EEAS, *Short assessments of narratives and disinformation around the Covid-19 pandemic (update December 2020 - April 2021)*, EUvsDisinfo, 28 IV 2021, https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic-update-december-2020-april-2021/ [accessed: 7 VIII 2022].

[83] A. Lipińska, *Chińskie operacje w dobie COVID-19. Dezinformacja – metody, dziedziny i ewolucja* (Eng. Chinese operations in the era of COVID-19. Disinformation - methods, fields and evolution), "Cyber Security and Law" 2022, vol. 7, no. 1, pp. 61–71.

[84] *What next for vaccine diplomacy?*, "The Economist", 3 V 2021, https://www.economist.com/podcasts/2021/05/03/whats-next-for-vaccine-diplomacy [accessed: 7 VIII 2022].

[85] *W okresie ostatnich 48 godzin dynamicznie rośnie zagrożenie dezinformacyjne w tematyce wydarzeń #Ukraina #Rosja w polskiej przestrzeni internetowej* (Eng. In the last 48 hours, the disinformation threat in the topic of #Ukraine #Russia events in the Polish online space has been growing dynamically), IBIMS, https://ibims.pl/komunikat-ws-szerzenia-dezinformacji-ws-sytuacji-na-ukrainie-w-polskiej-przestrzeni-internetowej/ [accessed: 7 VIII 2022].

[86] A. Jarynowski, *Pro-Kremlin German Twitter…*

[87] D. Broniatowski et al., *Vaccine Communication as Weaponized Identity Politics*, "American Journal of Public Health" 2020, vol. 110, no. 5, pp. 1378–1384.

[88] A. Jarynowski et al., *Attempt to understand public health relevant social dimensions of COVID-19 outbreak in Poland*, "Society Register" 2020, vol. 4, no. 3, p. 20. https://doi.org/10.14746/sr.2020.4.3.01.

[89] A. Jarynowski, D. Płatek, *Sentiment analysis: Topic modelling and social network analysis. COVID-19, protest movements and the Polish Tweetosphere*, in: *The Covid-19 Pandemic as a Challenge for Media and Communication Studies*, London 2022, pp. 210–224. https://doi.org/10.4324/9781003232049-21.

the ideological left[90]. The only pattern linking these attitudes is to work against One Health through biological denialism[91].

In view of the above, the issues of the food crisis, biological laboratories and the COVID-19 pandemic can also be viewed as the subject of information operations (INFOOPS) and psychological operations (PSYOPS)[92]. In the context of the existence of the infodemia phenomenon[93] (as we could see during the COVID-19 pandemic[94]) the involvement of foreign intelligence, through so-called bot armies, troll farms, agents of influence or useful idiots, in the discourse on infectious diseases plays a major role[95]. Unfortunately, in this information war[96] we are dealing with a very well-prepared and experienced opponent who will use food and biological agents for propaganda purposes, as this makes it easier for him to influence Polish society. However, it is worth emphasising that it is not Poland, but mainly the countries of the Global South, which depend on cheap food imports from Russia and Ukraine, that are the main theatre of information activities. Therefore, it is important to keep a close eye on what kind of moods are aroused there and whether shortages of grain supplies could trigger unrest and, consequently, a wave of migration.

---

[90] A. Jarynowski et al., *African Swine Fever – potential biological*...

[91] M. Duplaga, *Znaczenie kompetencji zdrowotnych w świecie infodemii* (Eng. The importance of health literacy in a world of infodemia), Institute of Public Health, https://izp.wnz.cm.uj.edu.pl/pl/blog/projekt-znaczenie-kompetencji-zdrowotnych-w-swiecie-infodemii/ [accessed: 7 VIII 2022].

[92] *Analiza i dekonstrukcja rosyjskich przekazów dezinformacyjnych*...

[93] According to the WHO definition, infodemia is an excess of information, including false or misleading information, during an epidemic (editor's note).

[94] G. Eysenbach, *How to fight an infodemic: the four pillars of infodemic management*, "Journal of Medical Internet Research" 2020, vol. 22, no. 6, e21820.

[95] R. Kasprzyk, *Modelowanie i analiza procesu złośliwego sterowania ludźmi* (Eng. Modelling and analysis of the process of malicious human control), in: *CyberExpert 2021 – Metody i narzędzia w procesie tworzenia cyberzdolności Sił Zbrojnych RP – wyzwania i perspektywy*, Warszawa 2022, pp. 9–28.

[96] J. Richards et al., *Introduction to the Special Issue section: Challenges for the state and international security – the current state and prognosis for the future*, "Security and Defence Quarterly" 2022, vol. 37, no. 1, pp. 1–3. https://doi.org/10.35467/sdq/147537.

Disinformation on biological weapons and food – an empirical contribution[97]

In order to perform an auxiliary analysis of media content in terms of biopolitical themes, tools designed for media monitoring were used (according to the internal definitions of these tools regarding searching, filtering and classifying online material). BuzzSumo was used to obtain a collection of materials published in media with a large reach (according to the tool's definition) in the form of passive websites of traditional broadcasters and online portals (textual form) and video materials (audiovisual form), i.e. published in so-called content media, without distinguishing the type of medium. Using Brand24, mentions were obtained with a distinction between social-content media and non-social media. Thanks to an academic account to the API, posts from Twitter were collected. Relative daily search counts for individual phrases on Google were obtained using the Google Trends tool. After analysing the Polish-language content published between 24 February and 1 August 2022 for the occurrence of the keywords "biolab", "bioweapons" and their variants, 65 articles and multimedia posted on traditional media websites, i.e. radio, television, press, and passive web portals with the largest reach, and 396 tweets were found. As many as 41% of mentions in social-content media had negative overtones (mainly expressing web users' anger at the United States and Ukraine for conducting 'illegal' research or fear of a biological attack on Poland), which testifies to the strong emotional character of the discourse. It is worth noting that the interest of the Polish public in the topics of biological laboratories and biological weapons (based on Google queries) was 2.6 times higher than in Russia and twice as high as in Germany. The waves of interest closely correlate with the uptake of Russian propaganda (which was most evident in March 2022). The peak of this activity in the Polish media was between 9 and 24 March 2022 (which is less than 10% of the total time frame). During this period, as many as 72% of queries on Google, 49% of articles on passive websites and content media and 43% of tweets were recorded. It follows that the Kremlin's influence on Polish society has had an effect in the sense that it has created a wave of interest.

Between 24 February and 1 August 2022, a monitoring of Polish language content for phrases such as "hunger", "food security", along with

[97] A. Jarynowski, Ł. Krzowski, S. Maksymowicz, *Biological mis(dis)-information in the Internet*...

their variants, was also carried out using the same tools and for the same media. 958 articles and multimedia and 59 453 tweets were found. Only 33% of non-social media and social media mentions were negative. This may be due to the fact that the discussion via these media was multithreaded, with one thread being about the support given by Polish farmers to Dutch farmers in the summer of 2022 (unity effect[98]) and the overtones of these materials were positive. In the case of hunger, there was a fairly even distribution of interest. It is interesting to note that digital traditional media slightly increased interest in the topic between 24 April and 23 May 2022 (e.g. discussions of food exports from Ukraine). The highest number of searches (13% more than the average) on Google took place between 24 February and 14 April 2022 (a symptom of anxiety related to the start of the war), above-average interest on passive websites and online portals and content media was recorded between 23 May and 24 June 2022 (discussion of Ukrainian grain and Poland's role in transport), and increased activity on Twitter between 4 and 14 July 2022 (a large proportion of tweets were about agricultural protests in the Netherlands and negotiations on access to Ukrainian grain in Poland or by unblocking the Odessa ports), reflecting the different dynamics of interest in the targeting of different media. It is noteworthy that the widespread fear of a food crisis and the overpricing of food products in Poland had already died out by April 2022[99]. Therefore, it seems that Kremlin propaganda in the first phase of the conflict in Ukraine fuelled the fear of food overpricing and later shifted the focus to the potential threat to Polish agriculture from the influx of cheap food from Ukraine. The reason for the significant increase in interest in social media in July 2022 is largely due to topics related to the arrival of Ukrainian grain in Poland and to solidarity protests with Dutch farmers against EU programmes such as the Green Deal or From Field to Table[100], conducted, for example, via accounts linked to the Agrounia organisation.

[98] A. Jarynowski et al., *Animal breeders protests in Polish Twitter*...

[99] A. Jarynowski, Ł. Krzowski, S. Maksymowicz, *Biological mis(dis)-information in the Internet*...

[100] J. Barreiro Hurle et al., *Modelling environmental and climate ambition in the agricultural sector with the CAPRI model*, JRC Publications Repository, https://publications.jrc.ec.europa.eu/repository/handle/JRC121368 [accessed: 7 VIII 2022].

Short-term perspective (2022–2023)

At the time of writing (August-October 2022), the BRAVO terrorist threat alert level was in force in Poland and it appears that it will be maintained until the end of 2023, and possibly even raised. In view of the above, it is recommended to intensify monitoring, e.g. by NATO countries' intelligence, among professionals (including medical, veterinary, agricultural personnel) towards radicalisation or agentic activities in Poland and the European region[101]. More so, research should continue, with a security dimension, into the social determinants of pandemics and war, especially in terms of people with a commitment to the current situation. The following phenomena can be expected (listed in order from most to least likely):

- polarisation of food producers towards the rest of society. It is worth noting that the farmers' protests in the Netherlands (the immediate reason for which was the commitment to reduce the meat and dairy herd as part of a wider process linked to the introduction of the Green Deal programme[102]) can be used by Russian propaganda centres to reinforce social polarisation along already existing lines of conflict[103];
- disinformation about the US (with Polish participation[104]) biological laboratories (e.g. using the UN forum to diminish the credibility of the US government and allies among their own citizens[105] and to gain the support of third countries), and it is precisely the fight against foreign propaganda (especially from the Russian Federation and ISIS) that has been identified as one of the priorities for terrorism research in Poland[106];

---

[101] A. Jarynowski et al., *African Swine Fever – potential biological…*

[102] Reducing cattle and pig populations is one of the objectives of international policies to reduce greenhouse gas emissions. Action to combat climate change or defend animal rights has the potential for dual use and may or may not also be used for hostile purposes.

[103] M. Piekarski, *Możliwe scenariusze zagrożeń terrorystycznych na terytorium Rzeczpospolitej Polskiej w kontekście zagrożeń hybrydowych* (Eng. Possible terrorist threat scenarios on the territory of the Republic of Poland in the context of hybrid threats), "Terroryzm – studia, analizy, prewencja" 2022, no. 2, pp. 71–92. https://doi.org/10.4467/27204383TER.22.019.16339.

[104] A. Jarynowski, Ł. Krzowski, S. Maksymowicz, *Biological mis(dis)-information in the Internet…*

[105] G. Kessler, *How the right embraced Russian disinformation…*

[106] D. Szlachter, *Terroryzm w Polsce i kierunki jego rozwoju. Wyniki badań ankietowych (skrócony*

– increased action against infrastructure and the agricultural supply chain (e.g. using pro-environmental organisations);
– introduction of plant or animal pathogens into disease-free areas (e.g. ASF could jump to the Netherlands, which could further intensify protests).

As a destabilising tool in the form of agroterrorism is relatively readily available, it is first and foremost necessary to ask what tactical or operational objectives, which may be part of actions at the strategic level, a hostile country, such as Russia, can achieve with it. The range of agroterrorist activities is very wide and is not limited to biological agents[107]. It is possible, for example, to use a computer virus to cause the thawing of strategic meat reserves or the contamination of water in rivers irrigating fields[108], or the spraying of chemicals onto fields in the Vistula delta by drones sent from the Kaliningrad region[109]. In countries with a strong agricultural position, but geostrategically acting very cautiously towards Russia, such as the Netherlands, France, Italy, Germany and Spain, agroterrorism supported by dis- and misinformation can be used to trigger waves of social unrest urging the governments of these countries to pressure Ukraine to end the war. Unfortunately, with the potential escalation of the situation in the Middle East and the threat of Islamic fundamentalism in Western Europe, attacks using so-called kitchen microbiology (agroterrorist agents seem to be the best means for small organisations and lone wolves in this case) are possible. On the other hand, in countries openly supporting Ukraine, such as Poland, the Baltic and Nordic countries, the Czech Republic, Slovakia, Moldova, Romania and the UK, a more important target could be the undermining of food security and the long-term reduction of food production capacity. China's capabilities and objectives in a hybrid war against the US and its allies should also be watched closely, as its

raport) (Eng. Terrorism in Poland and trends in its development. Survey results (summary report)), "Terrorism - studies, analyses, prevention" 2022, no. 2, pp. 335-363. https://doi.org/10.4467/27204383TER.22.022.16342.

[107] S. Maksymowicz, *Atak biologiczny i agroterrorystyczny na Polskę...*

[108] A. Jarynowski, *Katastrofa na Odrze ukazała dysfunkcjonalność działania instytucji państwa* (Eng. The disaster on the Oder river has demonstrated the dysfunctionality of state institutions), Nowa Konfederacja, 22 VIII 2022 r., https://nowakonfederacja.pl/katastrofa-na-odrze-ukazala-dysfunkcjonalnosc-dzialania-instytucji-panstwa/ [accessed: 7 VIII 2022].

[109] A. Jarynowski, *Disconnecting the Kaliningrad oblast and new threats from Polish perspective*, "Bre Reviews" 2022, no. 3, https://sites.utu.fi/bre/disconnecting-the-kaliningrad-oblast-and-new-threats-from-polish-perspective/ [accessed: 7 VIII 2022].

development in biotechnology has increased there in recent years, and in an even more decisive way in bioinformatics (through machine learning and artificial intelligence[110]). In a way, biotechnological progress was forced by previous epidemic outbreaks experienced in China (e.g. SARS-CoV-1 in 2002-2003, A/H5N1 influenza in 2003-2006).

Medium-term perspective (next few years)

The COVID-19 pandemic has contributed to a large increase in knowledge and development of technologies designed to combat infectious diseases, but at the same time, the same knowledge and technologies can be used to deliberately introduce pathogens. Until now, bioterrorism has been the domain of organisations with adequate financial resources and, above all, specialists and laboratories, as well as highly intelligent individuals capable of constructing a home laboratory[111]. Today, the threshold is much lower, as there has been a revolution in the availability of information and technology. Biological agents have acquired the status of "weapons of mass destruction for the poor", due to the ease of acquisition (knowledge of basic microbiology and pathogenesis), verification of the infectious agent (access to diagnostics) and introduction (knowledge of basic epidemiology, such as transmission routes).

It is interesting to note the paradox of Poland as a country where employment in the agri-food industry (15%) and food services or food trade (10%) reaches a total of 25%[112], and the level of interest in and knowledge of infectious animal or plant diseases is among the lowest in the EU (e.g. in the specific case for which international data are collected, i.e. knowledge of antibiotics[113]). This means that, on the one hand, specialist

---

[110] V. Bergengruen, *Tech Leaders Warn the U.S. Military Is Falling Behind China on AI*, Time, 18 VII 2023, https://time.com/6295586/military-ai-warfare-alexandr-wang/ [accessed: 15 VIII 2023].

[111] M. Dąbrowski, *Koronawirus, broń biologiczna a wojsko (opinia)* (Eng. Coronavirus, biological weapons and the military (opinion)), Defence 24, 15 III 2020, https://defence24.pl/sily-zbrojne/koronawirus-bron-biologiczna-a-wojsko-opinia [accessed: 8 VIII 2022].

[112] M. Kędzierski, *Integracja czy połączenie*…

[113] For example, the Q5 series of questions in: *Special Eurobarometer: Antimicrobial resistance (in the EU)*, Directorate General for Communication, European Union, 2018, https://data.europa.eu/data/datasets/s2190_90_1_478_eng?locale=en [accessed: 26 VI 2023].

knowledge is being built up separately about bioterrorism and food security, but an interdisciplinary approach to agroterrorism in its broad sense - biological, agricultural, social, economic or political - is lacking. The situation with the environmental catastrophe on the Oder river in the summer of 2022 showed the services of other countries what are the weaknesses of One Health security in Poland[114], allowing the creation of attack scenarios demonstrating the inefficiency of Polish services[115]. In the fight against the spread of diseases threatening One Health, early identification and rapid alerting of any unusual event are of paramount importance. The Oder disaster highlighted that rapid diagnosis and response appropriate to the threat may be a weakness of regional One Health inspections (i.e. State Sanitary Inspectorate, Veterinary Inspectorate, Plant Protection and Seed Inspection, Pharmaceutical Inspectorate, Environmental Inspectorate).

This poses a whole new challenge to the deployment groups[116], because until now bioterrorism could only be chosen by a small percentage of radicals, but now the number of people who have acquired the relevant competences can be even an order of magnitude higher. Actually, it is not competence that is now a barrier, but motivations. Consequently, the recommended monitoring of specialist communities (including biomedical personnel as before), carried out for example by the intelligence of NATO countries, seems no longer sufficient and it is necessary to expand this group to include veterinary, agricultural and other communities (especially as it is not clear how the war in Ukraine will end), as completely new non-professional actors have acquired sufficient potential to carry out a successful introduction of the infection into a new area. In the case of hybrid threats from states such as Russia, soft targets may be chosen (as Islamic organisations have typically done) rather than critical infrastructure or military facilities, as has been the case to date[117].

[114] A. Jarynowski, *Katastrofa na Odrze*...

[115] M. Piekarski, *Możliwe scenariusze zagrożeń terrorystycznych*..., p. 80.

[116] A. Kołodziejczyk, J. Maciejewski, P. Pieńkowski, *Grupy dyspozycyjne w dobie pandemii Covid-19* (Eng. Deployment groups in the era of the Covid-19 pandemic), XVIII Sociological Convention, Warszawa 2022, https://zjazdpts.pl/grupy/grupy-dyspozycyjne-w-dobie-pandemii-covid-19/ [accessed: 2 XI 2022].

[117] M. Piekarski, *Możliwe scenariusze zagrożeń terrorystycznych*..., p. 84.

However, there are still issues and factors that condition the face of agroterrorism in Poland and the European region that are not written about in this article. With regard to the phenomenon of agroterrorism, compensatory measures are being taken (e.g. operational measures by the services against overtly pro-Kremlin media propagating biological denialism or cracking down on radical circles) and competitive processes are taking place (e.g. with the passage of time, knowledge acquired during a pandemic is forgotten, and therefore competence capital may decrease). Countries and organisations have set their sights on acquiring resilience and will be more prepared to combat infectious diseases (and the infodemic phenomenon that may accompany them)[118]. On the one hand, the development of knowledge and technology favours the phenomenon of bioterrorism, but on the other, it allows better protection against it. The future will show which processes will occur faster.

Summary and recommendations

Depending on the method used, agroterrorism can achieve a tactical objective (e.g. to provoke protests) or an operational objective (e.g. to inflict heavy damage on the economy). This 'weapon of mass destruction for the poor' can be used by a small group of terrorists or even by a single determined person who has an agricultural, veterinary or biomedical background or has acquired basic microbiological-epidemiological knowledge during a pandemic and is able to understand scientific articles and information published on the internet and apply this knowledge in practice[119]. The weapon is only the combination of the biological agent with the means of its delivery or transport, and in the case of lone wolf operations living in an area where they want to carry out an attack, advanced engineering and technical knowledge is often not needed. In view of the importance of biosecurity (as demonstrated by, inter alia, the COVID-19 pandemic) and food security (especially as food exports contribute significantly to Poland's GDP) sensu largo (along with PSYOPS and INFOOPS), these issues should be taken into account when working

[118] *Germany open Hub for Pandemic and Epidemic Intelligence in Berlin*, World Health Organisation, 1 IX 2021, https://www.who.int/news/item/01-09-2021-who-germany-open-hub-for-pandemic-and-epidemic-intelligence-in-berlin [accessed: 12 VIII 2022].

[119] A. Jarynowski et al., *ASF jako zagrożenie biologiczne w Polsce*...

on the next editions of the National Security Strategy of the Republic of Poland[120].

The most important conclusions and recommendations from the conducted analysis are as follows:

1. The deliberate introduction of animal or plant pathogens into a disease-free area used to be relatively simple, and has now become even simpler[121].
2. Due to the food crisis and the war in Ukraine, the threat of agroterrorism is now at its highest since the signing of the Biological Weapons Convention. After the Odessa ports were unblocked, the threat has diminished, but if they are blocked again the problem could return - both in real and media terms.
3. Poland, the Nordic countries, the Baltics and the UK appear to be the most vulnerable to action by the Kremlin, and Germany and France to action by ISIS (so other introduction scenarios may apply).
4. The vigilance of food producers and veterinarians or plant protection specialists and their interest in potential agroterrorist threats should be increased (especially in the coming years).
5. It is worth conducting exercises and simulations on the basis of likely introduction scenarios (e.g. introduction of ASF in the Netherlands, FMD in Greater Poland or apple agrophages in the Lublin region) in a hybrid action paradigm[122], using ready-made introduction scenarios[123].
6. A system of constant observation of traditional and social media should be developed to monitor the potential impact of Kremlin propaganda and to detect actors resonating with it in real time[124].
7. A system should be set up to monitor the risk of radicalisation in

[120] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* (Eng. National Security Strategy of the Republic of Poland), https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [accessed: 13 III 2023].

[121] A. Jarynowski, Ł. Krzowski, *BIO (AGRO) Terrorism/Crime in post-Covid era...*

[122] A. Jarynowski, Ł. Krzowski, V. Belik, *Afrykański pomór świń...*

[123] M. Piekarski, *Możliwe scenariusze zagrożeń terrorystycznych...*, p. 80.

[124] A. Jarynowski, *Dyskurs antyszczepionkowy i koronasceptyczny a prokremlowska propaganda w niemieckim Twitterze* (Eng. Anti-vaccine and coronasceptic discourse and pro-Kremlin propaganda on German Twitter), Public Health Blog, 22 V 2022, https://izp.wnz.cm.uj.edu.pl/pl/blog/publikacja-dyskurs-antyszczepionkowy-i-koronascpetyczny-a-prokremlowska-propaganda-w-niemieckim-twitterze/ [accessed: 7 VIII 2022].

the veterinary and agricultural professions and among the new category of post-pandemic professionals.

8. The use of reliable risk assessment tools, i.e. based on scientific evidence[125], e.g. the Grunow & Finke tool (GFT)[126] or the Agricultural Index[127] should be promoted.

Bibliography

Bertrandt J., *Bioterroryzm żywnościowy – realne zagrożenia użycia patogenów biologicznych w działaniach terrorystycznych* (Eng. Food bioterrorism - the real threat of using biological pathogens in terrorist activities), "Lekarz Wojskowy" 2007, vol. 8, no. 1, pp. 33–35.

Broniatowski D. et al., *Vaccine Communication as Weaponized Identity Politics*, "American Journal of Public Health" 2020, vol. 110, no. 5, pp. 1378–1384. https://doi.org/10.2105/ajph.2020.305616.

Chen X., Chughtai A.A., MacIntyre C.R., *Recalibration of the Grunow–Finke assessment tool to improve performance in detecting unnatural epidemics*, "Risk Analysis" 2019, vol. 39, no. 7, pp. 1465–1475.

EFSA Panel on Plant Health (PLH), *Pest categorisation of Colletotrichum fructicola*, "EFSA Journal" 2021, vol. 19, no. 8, e06803. https://doi.org/10.2903/j.efsa.2021.6803.

Essack S.Y., *Environment: the neglected component of the One Health triad*, "The Lancet Planetary Health" 2018, vol. 2, no. 6, e238–e239. https://doi.org/10.1016/S2542-5196(18)30124-4.

European Food Safety Authority (EFSA), *Update of the Xylella spp. host plant database – systematic literature search up to 31 December 2021*, "EFSA Journal" 2022, vol. 20, no. 6, e07356. https://doi.org/10.2903/j.efsa.2022.7356.

[125] A. Jarynowski, *Agro/bio-terrorism in Europe?...*

[126] X. Chen, A.A. Chughtai, C.R. MacIntyre, *Recalibration of the Grunow–Finke assessment tool to improve performance in detecting unnatural epidemics*, "Risk Analysis" 2019, vol. 39, no. 7, pp. 1465–1475.

[127] R. Sequeira, *Safeguarding production agriculture and natural ecosystems against biological terrorism: A U.S. Department of Agriculture emergency response framework*, "Annals of the New York Academy of Sciences" 1999, vol. 894, no. 1, pp. 48–69. https://doi.org/10.1111/j.1749-6632.1999.tb08043.x.

Eysenbach G., *How to fight an infodemic: the four pillars of infodemic management*, "Journal of Medical Internet Research" 2020, vol. 22, no. 6, e21820. https://doi.org/10.2196/21820.

Helmus T. et al., *Russian social media influence: Understanding Russian propaganda in Eastern Europe*, Santa Monica 2018.

Jarynowski A., *Infodemiologia oraz infonadzór – doświadczenia doby pandemii* (Eng. Infodemiology and infosurveillance - the experience of the pandemic era), in: *Epidemiologia i bezpieczeństwo CBRN. Nauka, innowacje, implikacje praktyczne*, A. Mróz-Jagiełło, J. Walczak (eds.), series: Epimilitaris, Zielonka 2022, pp. 235–248.

Jarynowski A. et al., *African Swine Fever Awareness in the Internet Media in Poland – exploratory review*, "E-methodology" 2019, vol. 6, no. 6, pp. 100–115. https://doi.org/10.15503/emet2019.100.115.

Jarynowski A. et al., *ASF jako zagrożenie biologiczne w Polsce i na świecie* (Eng. ASF as a biological threat in Poland and worldwide), in: *Bezpieczeństwo regionalne. Węzłowe problemy i procesy*, P. Bajor (ed.), Kraków 2021, pp. 239–254. https://doi.org/10.12797/9788381383899.14.

Jarynowski A., Krzowski Ł., Belik V., *Afrykański pomór świń: epizootiologia, ekonomia i zarządzanie kryzysowe w kontekście naturalnego bądź intencjonalnego wprowadzenia* (Eng. African swine fever: Epizootiology, economics and crisis management in the context of natural or intentional introduction), "Studia Administracji i Bezpieczeństwa" 2021, vol. 11, no. 11, pp. 129–153. http://dx.doi.org/10.5604/01.3001.0015.6752.

Jarynowski A., Płatek D., *Sentiment analysis, topic modelling and social network analysis. COVID-19, protest movements and the Polish Tweetosphere*, in: *The Covid-19 Pandemic as a Challenge for Media and Communication Studies*, London 2022. https://doi.org/10.4324/9781003232049-21.

Jarynowski A., Stochmal M., Maciejewski J., *Przegląd i charakterystyka prowadzonych w Polsce badań na temat społecznych uwarunkowań epidemii COVID-19 w jej początkowej fazie* (Eng. Overview and characteristics of ongoing research in Poland on the social determinants of the COVID-19 epidemic in its initial chase), "Bezpieczeństwo. Obronność. Socjologia" 2020, vol. 13, pp. 38–87.

Jarynowski A., Wójta-Kempa M., Płatek D., Czopek K., *Attempt to understand public health relevant social dimensions of COVID-19 outbreak in Poland*, "Society Register" 2020, vol. 4, no. 3, pp. 7–44. https://doi.org/10.14746/sr.2020.4.3.01.

Jedno zdrowie. Ludzie i inne gatunki (Eng. One Health. Humans and other species), H. Mamzer, P. Białas (sci.eds.), Wrocław 2022.

Jemielniak D., Krempovych Y., *An analysis of AstraZeneca COVID-19 vaccine misinformation and fear mongering on Twitter*, "Public Health", 2021, vol. 200, pp. 4–6. https://doi.org/10.1016/j.puhe.2021.08.019.

Karimzadeh S., Bhopal R., Nguyen Tien H., *Review of infective dose, routes of transmission and outcome of COVID-19 caused by the SARS-COV-2: comparison with other respiratory viruses*, "Epidemiology and Infection" 2021, vol. 149, e96. https://doi.org/10.1017/S0950268821000790.

Kasprzyk R., *Modelowanie i analiza procesu złośliwego sterowania ludźmi* (Eng. Modelling and analysis of the process of malicious human control), in: *CyberExpert 2021 – Metody i narzędzia w procesie tworzenia cyberzdolności Sił Zbrojnych RP – wyzwania i perspektywy*, Warszawa 2022, pp. 9–28.

Keremidis H. et al., *Historical Perspective on Agroterrorism: Lessons Learned from 1945 to 2012*, "Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science" 2013, vol. 11, pp. 17–24. https://doi.org/10.1089/bsp.2012.0080.

Kiriya I., *From "Troll Factories" to "Littering the Information Space": Control Strategies Over the Russian Internet*, "Media and Communication" 2021, vol. 9, no. 4, pp. 16–24. https://doi.org/10.17645/mac.v9i4.4177.

Leitenberg M., Zilinskas R.A., *The Soviet biological weapons program: A history*, Cambridge 2012.

Lenda M. et al., *Effect of the internet commerce on dispersal modes of invasive alien species*, "PLoS ONE" 2014, vol. 9, no. 6, p.e99786. https://doi.org/10.1371/journal.pone.0099786.

Lenda M. et al., *Misinformation,internet honey trading and beekeepers drive a plant invasion*, "Ecology Letters" 2021, vol. 24, no. 2, pp. 165–169. https://doi.org/10.1111/ele.13645.

Lipa J., *Agroterroryzm – wyzwaniem dla kwarantanny i ochrony roślin* (Eng. Agroterrorism - a challenge for quarantine and plant protection), "Progress in Plant Protection" 2006, vol. 46, no. 1, pp. 162–168.

Lipińska A., *Chińskie operacje w dobie COVID-19. Dezinformacja – metody, dziedziny i ewolucja* (Eng. Chinese operations in the era of COVID-19. Disinformation - methods, fields and evolution), "Cyber Security and Law" 2022, vol. 7, no. 1, pp. 61–71.

Maciejewski J., *Grupy dyspozycyjne w systemie bezpieczeństwa państwa* (Eng. Deployment groups in the state security system), XXIII International Seminar series "Social systems research methodology", Wrocław, 7 IV 2022.

MacIntyre R.C. et al., *Converging and emerging threats to health security*, "Environment Systems and Decisions" 2018, vol. 38, no. 2, pp. 198–207. https://doi.org/10.1007/s10669-017-9667-0.

Mamzer H., *Choroba jako zjawisko społeczne. Analiza walki z afrykańskim pomorem świń* (Eng. Disease as a social phenomenon. An analysis of the fight against African swine fever), "Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2020, vol. 82, no. 2, pp. 281–297. https://doi.org/10.14746/rpeis.2020.82.2.19.

Piekarski M., *Możliwe scenariusze zagrożeń terrorystycznych na terytorium Rzeczpospolitej Polskiej w kontekście zagrożeń hybrydowych* (Eng. Possible terrorist threat scenarios on the territory of the Republic of Poland in the context of hybrid threats), "Terroryzm – studia, analizy, prewencja" 2022, no. 2, pp. 71–92. https://doi.org/10.4467/27204383TER.22.019.16339.

Richards J., Świeboda H., Gębska M., *Introduction to the Special Issue section: Challenges for the state and international security – the current state and prognosis for the future*, "Security and Defence Quarterly" 2022, vol. 37, no. 1, pp. 1–3. https://doi.org/10.35467/sdq/147537.

Sequeira R., *Safeguarding production agriculture and natural ecosystems against biological terrorism: A U.S. Department of Agriculture emergency response framework*, "Annals of the New York Academy of Sciences" 1999, vol. 894, no. 1, pp. 48–69. https://doi.org/10.1111/j.1749-6632.1999.tb08043.x.

Szlachter D., *Terroryzm w Polsce i kierunki jego rozwoju. Wyniki badań ankietowych (skrócony raport)* (Eng. Terrorism in Poland and trends in its development. Survey results (summary report)), "Terrorism - studies, analyses, prevention" 2022, no. 2, pp. 353–363. https://doi.org/10.4467/27204383TER.22.022.16342.

Wiśniewska M., *The food terrorism – the essence and the methods of systemic defense*, "Journal of Modern Science" 2023, vol. 50, no. 1, pp. 331–349. https://doi.org/10.13166/jms/161535.

Russian and Ukrainian literature

Кириллов И., *Тезисы брифинги начальника войск радиационной, химической и биологической защиты ВС РФ генерал-лейтенанта Игоря Кириллова* (material

of the Ministry of Defence of the Russian Federation collected by the author from the Telegram channel, available on request by e-mail).

Стегній Б., Герилович А., Бузун А., *Африканська чума свиней: історія, сьогоденна та перспективи,* Київ 2015.

Жиганова Л.П., *Биотерроризм и Агротерроризм-Реальная Угроза Биобезопасности Общества,* "США и Канада: Экономика, Политика, Культура" 2004, vol. 417, no. 9, p. 3–25.

Internet sources

Analiza i dekonstrukcja rosyjskich przekazów dezinformacyjnych oraz propagandowych na temat Polski i Polaków (Eng. Analysis and deconstruction of Russian disinformation and propaganda messages about Poland and Poles), 2022., https://infowarfare.pl/realizowane-projekty/ [accessed: 25 VI 2023].

Barreiro Hurle J. et al., *Modelling environmental and climate ambition in the agricultural sector with the CAPRI model,* JRC Publications Repository, https://publications.jrc.ec.europa.eu/repository/handle/JRC121368 [accessed: 7 VIII 2022].

Belik V., Jarynowski A., *Elucidating the interplay of COVID-19 epidemic and social dynamics via Internet media in Germany*, on-line conference "Preparedness for future pandemics from a global perspective", 15 XI 2021, https://zenodo.org/record/6400773#.ZGRny3ZByUk [accessed: 7 VIII 2022].

Bergengruen V., *Tech Leaders Warn the U.S. Military Is Falling Behind China on AI*, Time, 18 VII 2023, https://time.com/6295586/military-ai-warfare-alexandr-wang/ [accessed: 15 VIII 2023].

Bezpieczeństwo żywnościowe (Eng. Food security), K. Mordzak (elaborated), Wrocław 2021, https://www.wojsko-polskie.pl/awl/u/50/d4/50d46baf-332b-4acb-aeb3-8f5b17777590/bezpieczenstwo_zywnosciowe.pdf [accessed: 7 VIII 2022].

Black Sea Grain Initiative, Wikipedia, https://en.wikipedia.org/wiki/Black_Sea_Grain_Initiative [accessed: 7 VIII 2022].

Broń masowego rażenia, broń biologiczna, broń chemiczna, broń jądrowa. Cz. 2 (Eng. Weapons of mass destruction, biological weapons, chemical weapons, nuclear weapons. Part 2), K. Mordzak (elaborated), Wrocław 2019, https://www.wojsko-polskie.pl/awl/u/96/0c/960cad22-5698-4356-b8f5-38117fb19499/bron_cbn.pdf [accessed: 7 VIII 2022].

Building resilience against agro-crime and agro-terrorism, World Organisation for Animal Health, https://www.woah.org/en/document/building-resilience-against-agro-crime-and-agro-terrorism/ [accessed: 5 III 2023].

Clement S., *Biological Threats: Technological Progress and the Spectre of Bioterrorism in the Post-Covid-19 Era*, https://www.nato-pa.int/download-file?filename=/sites/default/files/2022-01/024%20STCTTS%2021%20E%20rev.%201%20fin%20-%20%20BIOLOGICAL%20THREATS.pdf [accessed: 8 VIII 2022].

Cwynar P., *Bioterroryzm – syllabus*, Wrocław University of Life Sciences, 2021, https://sylabus.upwr.edu.pl/pl/document/7562fe08-5a02-4db5-8d31-d7144fdd99bb.pdf [accessed: 1 XI 2022].

Debata Bezpieczeństwo żywnościowe Europy w świetle nadchodzących wyzwań (Eng. Debate on European food security in the light of upcoming challenges), https://instytutrolny.pl/debata-bezpieczenstwo-zywnosciowe-europy-w-swietle-nadchodzacych-wyzwan/ [accessed: 2 XI 2022]. Material has been archived: https://web.archive.org/web/20221104152532/https://instytutrolny.pl/debata-bezpieczenstwo-zywnosciowe-europy-w-swietle-nadchodzacych-wyzwan/.

EEAS, *Short assessments of narratives and disinformation around the Covid-19 pandemic (update December 2020 - April 2021)*, EUvsDisinfo, 28 IV 2021, https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic-update-december-2020-april-2021 [accessed: 7 VIII 2022].

Dąbrowski M., *Koronawirus, broń biologiczna a wojsko* (Eng. Coronavirus, biological weapons and the military), Defence 24, 15 III 2020, https://defence24.pl/sily-zbrojne/koronawirus-bron-biologiczna-a-wojsko-opinia [accessed: 7 VIII 2022].

Deter A., *50 vermummte Aktivisten blockieren Bocholter Schlachthof* (Eng. 50 masked activists block Bocholt slaughterhouse), Topagrar, 20 VI 2022, https://www.topagrar.com/schwein/news/aktivisten-blockieren-bocholter-schlachthof-13131573.html [accessed: 7 VIII 2022].

Duplaga M., *Znaczenie kompetencji zdrowotnych w świecie infodemii* (Eng. The importance of health literacy in a world of infodemia), Public Health Institute, https://izp.wnz.cm.uj.edu.pl/pl/blog/projekt-znaczenie-kompetencji-zdrowotnych-w-swiecie-infodemii/ [accessed: 7 VIII 2022].

Germany open Hub for Pandemic and Epidemic Intelligence in Berlin, World Health Organisation, 1 IX 2021, https://www.who.int/news/item/01-09-2021-who-germany-open-hub-for-pandemic-and-epidemic-intelligence-in-berlin [accessed: 12 VIII 2022].

Jarynowski A., *Agro/bio-terrorism in Europe? Analysis of selected suspicious biological events (significant from the One Health perspective) after 24.02.2022*, presentation, NATO BioMed Panel, 25 X 2022, http://interdisciplinary-research.eu/wp-content/uploads/2022/10/agro_BIOTERRORISM_aj_warsaw_2022.pdf [accessed: 2 XI 2022].

Jarynowski A., *Disconnecting the Kaliningrad oblast and new threats from Polish perspective*, "Bre Reviews" 2022, no. 3, https://sites.utu.fi/bre/disconnecting-the-kaliningrad-oblast-and-new-threats-from-polish-perspective/ [accessed: 7 VIII 2022].

Jarynowski A., *Dyskurs antyszczepionkowy i koronascpetyczny a prokremlowska propaganda w niemieckim Twitterze* (Eng. Anti-vaccine and coronasceptic discourse and pro-Kremlin propaganda on German Twitter), Public Health Blog, 22 V 2022, https://izp.wnz.cm.uj.edu.pl/pl/blog/publikacja-dyskurs-antyszczepionkowy-i-koronascpetyczny-a-prokremlowska-propaganda-w-niemieckim-twitterze/ [accessed: 7 VIII 2022].

Jarynowski A., *Katastrofa na Odrze ukazała dysfunkcjonalność działania instytucji państwa* (Eng. The disaster on the Oder river has demonstrated the dysfunctionality of state institutions), "Nowa Konfederacja", 22 VIII 2022, https://nowakonfederacja.pl/katastrofa-na-odrze-ukazala-dysfunkcjonalnosc-dzialania-instytucji-panstwa/ [accessed: 2 XI 2022].

Jarynowski A., *Pro-Kremlin German Twitter users are more likely to be involved in both anti-lockdown and anti-vaccine discourse than Anti-Kremlin users*, preprint, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4079045 [accessed: 7 VIII 2022]. https://dx.doi.org/10.2139/ssrn.4079045.

Jarynowski A., *(Re-)Emergence of agroterrorism during the food crisis*, presentation, NATO Centre of Excellence for Military Medicine, 20 VII 2022, https://zenodo.org/record/6969341 [accessed: 2 XI 2022].

Jarynowski A., Belik V., *African Swine Fever (ASF) Virus propagation in Poland (Spatio-temporal analysis)*, preprint, https://www.researchgate.net/publication/338436134_African_Swine_Fever_ASF_Virus_propagation_in_Poland_Spatio-temporal_analysis [accessed: 7 VIII 2022]. https://doi.org/10.13140/RG.2.2.29807.6167.

Jarynowski A., Belik V., *Spatio-temporal analysis of African Swine Fever Spread in Poland with network perspective*, preprint, https://www.academia.edu/43262326/Multilayer_network_approach_to_African_Swine_Fever_Spread_in_Poland [accessed: 12 VIII 2022].

Jarynowski A., Grabowski A., *Modelowanie epidemiologiczne dedykowane Polsce* (Eng. Epidemiological modelling dedicated to Poland), Portal CZM, 2015, http://www.czm.mif.pg.gda.pl/wp-content/uploads/fam/publ/jarynowski2.pdf [accessed: 7 VIII 2022].

Jarynowski A. et al., *African Swine Fever – potential biological warfare threat*, preprint, https://easychair.org/publications/preprint/vjFf [accessed: 7 VIII 2022].

Jarynowski A. et al., *Animal breeders protests in Polish Twitter - preliminary research*, preprint, http://interdisciplinary-research.eu/wp-content/uploads/2022/04/animal_related_protests_in_twitter_preprint_pdf.pdf [accessed: 7 VIII 2022].

Jarynowski A., Krzowski Ł., *BIO (AGRO) Terrorism/Crime in post-covid era in context of massive scale dissemination of microbiology/epidemiology knowledge*, "DiMiMED – International Conference on Disaster and Military Medicine", Düsseldorf, 15-16 XI 2021, https://events.military-medicine.com/media/landingpage/25/attachment-1639063402.pdf [accessed: 7 VIII 2022].

Jarynowski A., Krzowski Ł., Maksymowicz S., *Biological mis(dis)-information in the Internet as a possible Kremlin warfare* (working version), https://zenodo.org/record/8081493 [accessed: 26 VI 2023].

Jarynowski A., Lopez-Nunez F., Fan H., *How network temporal dynamics shape a mutualistic system with invasive species?*, preprint, https://arxiv.org/ftp/arxiv/papers/1407/1407.4334.pdf, [accessed: 7 VIII 2022]. https://doi.org/10.48550/arXiv.1407.4334.

Jarynowski A., Semenov A., Belik V., *Perception of infectious diseases with animal and humans hosts on the Polish internet*, Proceedings of 20th Congress of the International Society for Animal Hygiene, Berlin, 5–7 X 2022, http://interdisciplinary-research.eu/wp-content/uploads/2022/08/Abstract-form-ISAH_jarynowski_corr.pdf [accessed: 7 XI 2022].

Kessler G., *How the right embraced Russian disinformation about 'U.S. bioweapons labs' in Ukraine*, "The Washington Post", 11 III 2022, https://www.washingtonpost.com/politics/2022/03/11/how-right-embraced-russian-disinformation-about-us-bioweapons-labs-ukraine/ [accessed: 7 VIII 2022].

Kędzierski M., *Integracja czy połączenie. Analiza możliwości zwiększenia efektywności działania inspekcji weterynaryjnej oraz ochrony roślin i nasiennictwa* (Eng. Integration or merger. An analysis of options to increase the efficiency of the veterinary and plant protection and seed inspections), https://efrwp.pl/publikacje/integracja-czy-polaczenie-analiza-mozliwosci-zwiekszenia-efektywnosci-dzialania-inspekcji-weterynaryjnej-oraz-ochrony-roslin-i-nasiennictwa/ [accessed: 7 VIII 2022].

Kołodziejczyk A., Maciejewski J., Pieńkowski P., *Grupy dyspozycyjne w dobie pandemii Covid-19* (Eng. Deployment groups in the era of the Covid-19 pandemic), XVIII Sociological Convention, Warszawa, 2022, https://zjazdpts.pl/grupy/grupy-dyspozycyjne-w-dobie-pandemii-covid-19/ [accessed: 2 XI 2022].

Lentzow F., Littlewood J., *Russia finds another stage for the Ukraine "biolabs" disinformation show*, Bulletin of the Atomic Scientists, 8 VII 2022, https://thebulletin.org/2022/07/russia-finds-another-stage-for-the-ukraine-biolabs-disinformation-show/ [accessed: 12 VIII 2022].

Maksymowicz S., *Atak biologiczny i agroterrorystyczny na Polskę. Jakie scenariusze są prawdopodobne?* (Eng. Biological and agroterrorist attack on Poland. What scenarios are likely?), Nowa Konfederacja, 31 V 2022, https://nowakonfederacja.pl/atak-biologiczny-i-agroterrorystyczny-na-polske-jakie-scenariusze-sa-prawdopodobne/ [accessed: 7 XI 2022].

Marek M., *Rosyjska dezinformacja w Polsce – cele i przekazy* (Eng. Russian disinformation in Poland - targets and messages), Centrum Badań nad Współczesnym Środowiskiem Bezpieczeństwa, 30 III 2022, https://infowarfare.pl/2022/03/30/rosyjska-dezinformacja-w-polsce-cele-i-przekazy/ [accessed: 7 VIII 2022].

Monke J., *Agroterrorism: Threats and preparedness*, https://sgp.fas.org/crs/terror/RL32521.pdf [accessed: 7 VIII 2022].

Normile D., *African swine fever keeps spreading in Asia, threatening food security*, "Science", 2019 r., https://www.science.org/content/article/african-swine-fever-keeps-spreading-asia-threatening-food-security [accessed: 7 VIII 2022].

OiE, *Classification of diseases notifiable*, https://www.oie.int/en/animal-health-in-the-world/the-world-animal-health-information-system/old-classification-of-diseases-notifiable-to-the-oie-list-a/ [accessed: 29 VII 2022].

Radziejewski B., *Widmo krąży po świecie. Widmo głodu* (Eng. A spectre looms over the world. The spectre of hunger), Nowa Konfederacja, 25 V 2022, https://nowakonfederacja.pl/widmo-krazy-po-swiecie-widmo-glodu/ [accessed: 7 VIII 2022].

Special Eurobarometer: Antimicrobial resistance (in the EU), Directorate General for Communication, European Union, 2018, https://data.europa.eu/data/datasets/s2190_90_1_478_eng?locale=en [accessed: 26 VI 2023].

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (Eng. National Security Strategy of the Republic of Poland), https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [accessed: 13 III 2023].

Tajemnicze nasiona w paczkach z Chin (Eng. Mystery seeds in packages from China), Polsat News, 5 VIII 2020, https://www.polsatnews.pl/wiadomosc/2020-08-05/tajemnicze-nasiona-w-paczkach-z-chin-zidentyfikowano-14-gatunkow-roslin/ [accessed: 7 VIII 2022].

What next for vaccine diplomacy?, "The Economist", 3 V 2021, https://www.eiu.com/n/campaigns/q2-global-forecast-2021/ [accessed: 7 VIII 2022].

Wojskowe Ośrodki Medycyny Prewencyjnej (Eng. Military Preventive Medicine Centres), https://www.gov.pl/web/obrona-narodowa/wojskowe-osrodki-medycyny-prewencyjnej [accessed: 2 III 2023].

W okresie ostatnich 48 godzin dynamicznie rośnie zagrożenie dezinformacyjne w tematyce wydarzeń #Ukraina #Rosja w polskiej przestrzeni internetowej (Eng. In the last 48 hours, the disinformation threat in the topic of #Ukraine #Russia events in the Polish online space has been growing dynamically), IBIMS, https://ibims.pl/komunikat-ws-szerzenia-dezinformacji-ws-sytuacji-na-ukrainie-w-polskiej-przestrzeni-internetowej/ [accessed: 7 VIII 2022].

Xia Wei et al., *How One Pandemic Led To Another: Asfv, the Disruption Contributing To Sars-Cov-2 Emergence in Wuhan*, preprint, https://www.researchgate.net/publication/349628301_How_One_Pandemic_Led_To_Another_Asfv_the_Disruption_Contributing_To_Sars-Cov-2_Emergence_in_Wuhan [accessed: 7 VIII 2022]. https://doi.org/10.20944/preprints202102.0590.v1.

Zarażone ASF dziki spadają z nieba? Mające być dowodem zdjęcie budzi poważne wątpliwości (Eng. ASF-infected wild boars fall from the sky? The supposed proof photo raises serious doubts), Lublin112.pl, 22 VII 2018, https://www.lublin112.pl/zarazone-asf-dziki-spadaja-nieba-majace-byc-dowodem-zdjecie-budzi-powazne-watpliwosci/ [accessed: 7 VIII 2022].

Legal acts

Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, done at Moscow, London and Washington on 10 April 1972 (Journal of Laws 1976 No. 1 item 1).

Additional Protocols to the Geneva Conventions of 12 August 1949, concerning the Protection of Victims of International Armed Conflicts (Protocol I) and the Protection of Victims of Non-International Armed Conflicts (Protocol II), drawn up in Geneva on 8 June 1977 (Journal of Laws 1992, No. 41, item 175.).

Protocol concerning the prohibition of the use of asphyxiating, poisonous or similar gases and bacteriological agents in war (Journal of Laws 1929, No. 28, item 278).

Andrzej Jarynowski, PhD

Specialist in modelling the spread of infectious diseases. His interests include social network analysis, One Health, telemedicine, infodemiology and bioterrorism. He collaborates as an epidemiological consultant for Eastern Europe with the Bloomberg agency, "The Washington Post", "The New Confederation".

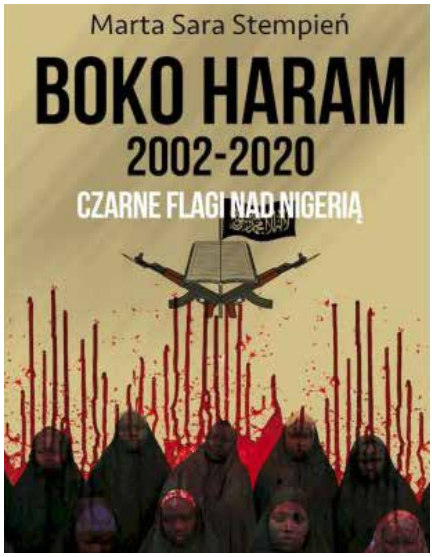
Contact: ajarynowski@gmail.com

REVIEWS

https://doi.org/10.4467/27204383TER.23.033.18335
https://orcid.org/0000-0001-9815-6035

KRZYSZTOF IZAK

Book review: Marta Sara Stempień, **Boko Haram 2002–2020. Czarne flagi nad Nigerią**[1]



May 2021 saw the death of Abu Bakr Shekau, the charismatic leader of Boko Haram (in English: Western education is forbidden), one of the bloodiest terrorist organisations, second only to the Islamic State in terms of the number of people killed in the second decade of the 21st century. Shekau died - according to one version - as a result of wounds sustained in combat with the rival group Islamic State in West Africa Province, ISWAP, also known as Wilajet Gharb Ifriqijja. According to another version, he blew himself up

[1] M.S. Stempień, *Boko Haram 2002–2020. Czarne flagi nad Nigerią* (Eng. Boko Haram 2002-2020. Black flags over Nigeria), Warszawa–Siedlce 2020, Rytm, 206 pp.

using a shahid belt, which is why his corpse was not found. At the time, opinions were confirmed that Boko Haram members would move to ISWAP, with which the organisation merged in 2015. Later, however, through ideological differences, their paths diverged, and eventually there was a conflict that ended with the death of the Boko Haram leader. The proper name of this organisation is: Association of Sunni People for Missionary Activities and Jihad (Jama'atu Ahlis Sunna Lidda'Awati wal-Jihad in Hausa written in Arabic or Jama'at Ahl al-Sunna li ad-Dawa wa al-Jihad in Arabic). Its activity seems to have ceased, as there is no new information about its criminal activities. The organisation used to openly admit to it as part of its propaganda strategy. The scale of ISWAP activity has also decreased significantly, which does not mean that it is safer in Nigeria. The activity of various groups and organisations has shifted from the north-east of Nigeria (Borno, Yobe, Adamawa states), the motherland of both groups, to the west and south of the country. Statistically, the situation is as follows: in 2021, more than 2 600 civilians were killed in the north of Nigeria in attacks carried out by groups other than Boko Haram and ISWAP, significantly more than were killed by these two organisations in the same period and three times more than in 2020. In contrast, 2968 people were killed in Nigeria in the first quarter of 2022. 86 per cent of these deaths were recorded in the northern part of the country.

Let this digression serve as an introduction to the review of Marta Sara Stempień's publication, which is a monograph on the most criminal organisation of Islamic extremists in Nigeria's history. The author, as one can read in the biographical note, is an assistant professor at the Institute of Security Sciences at the Siedlce University of Life Sciences and Humanities and deputy editor-in-chief of the scientific journal "Die Securitate et Defensione. On Security and Defence". In addition to her peer-reviewed monograph, she has published books such as *Islamic State: the new face of terrorism* (2018) and, together with Malina Kaszuba, *Middle East: still on fire* (2019).

The monograph *Boko Haram...* consists of five chapters of varying substantive value. They fulfil the stated purpose, define the problem and the research hypothesis formulated in the introduction, but in the reviewer's opinion, it would be appropriate to speak here of theses based on well-documented facts rather than the research hypothesis[2].

[2] As the author indicated, the purpose of the monograph is to try to determine the evolution of the Boko Haram terrorist structure. The main research problem was contained in the answer to the question: what are the consequences for Nigeria, including security,

There is a lack of even distribution of emphasis in many places. Serious issues are downplayed and less important matters receive more attention. Furthermore, mental shortcuts cause the reader to miss the most important issues. These criticisms relate primarily to Chapter 1, entitled *Nigeria*, which includes in separate subsections information on the historical and geopolitical background, the country's population, the development of Salafism in northern Nigeria, the idea of liberal democracy, and the political and economic situation. The chapter totals 33 pages. The author has given a disproportionate and selective treatment to the issues it addresses. The most important issue, Islam, is dealt with in less than six pages (pp. 26-31), while the economic situation is dealt with in eight pages (pp. 43-51). Unfortunately, there was no information on the Sokoto Caliphate, which had a huge impact on the formation of Islam in Nigeria in the early 19th century, and on the contemporary influence of Hezbollah. The former is only mentioned by the author on pages 56, 84 and 143-144. On page 144 she writes: *There were twenty caliphs in power from the time of Usman dan Fodio until the British conquest in the early 20th century.* This is not in line with Nigeria's history and contemporary times, as the twentieth caliph and Sultan of Sokoto, Muhammad Saad Abubakar, has been in office (purely representative, but highly respected) since 2006 to the present day. Writing in Chapter 1 about the Biafran War (1967-1970), the author mentioned, among other things, the states involved in the conflict: *The world powers of the time were involved in the war. Britain and the Soviet Union supported the Nigerian government. Biafra, on the other hand, received support from France and Israel* (p. 22). This is incomplete because the government forces were also supported by the United States, and Biafra by Portugal and the Vatican. It is worth adding that the Biafran air force was commanded by Jan Zumbach, former commander of 303 Squadron. Also missing is the important information that Biafran separatism is still active in south-eastern Nigeria. It is mainly represented by the Indigenous People of Biafra, an organisation accused by the authorities of terrorist activities. It fights primarily for the interests of the Ibo (Igbo) people. The author uses both these two names and the incorrect term Ikbo, but does not clarify that they refer to the same ethnic group. This may create a misconception in the reader that two

of Boko Haram activity? Stempień also adopted the following research hypothesis: Boko Haram in recent years has become an important representative group of the Salafist community and a significant military force in Nigeria.

different communities are being referred to. A similar problem applies to the Fulani, a pastoralist nomadic Muslim people living throughout the Sahel. They are also known by the names: Fulbeje, Peul or Bororo.

In describing the political situation in Nigeria after independence, the author mentions that Gen Olusẹgun Ọbasanjọ, president and one of the leaders of the first military junta, transferred power to civilian hands in 1979. What was missing, however, was the important observation that this change of power was accompanied by a major reduction in the armed forces. Thousands of soldiers left the army at that time and were left with their weapons. This became the cause of an incredible increase in banditry and terror in Nigeria, especially on the streets of Lagos, the former capital.

The author's cursory treatment of the issue of Islamic development in Nigeria is very evident in the work. This leaves one feeling quite unsatisfied. The memory of events in West Africa in the nineteenth century, when various religious leaders declared jihad, is still alive in the Islamic tradition and religion of many African countries, including Nigeria.

There is a very glaring lack of reference in the work to the excellent monograph by Stanisław Piłaszewicz, *The Power of the Book and the Sword of Truth*[3]. The author most likely did not use it, as she did not mention this title in the bibliography. She also devoted little space to the problem of Salafism in northern Nigeria and Muslim radicalism, but drew attention to the activities of the bloody Maitatsine sect and mentioned the Ombatse cult. In the case of the latter, however, a few sentences should have been devoted to bringing the reader closer to the issue, if only because of its bloody nature linked to the traditional beliefs of the Eggon community in central Nigeria.

On p. 31 the statement appears: *The role of the so-called Fulani militant group, which is more widely unknown in the world, has also increased in recent years*. One cannot agree with this. No such armed group exists in Africa; the author is referring to the fighters of the aforementioned Fulani people. In her justification, it should be noted that in describing the activities of this 'group', she relied on information published by the Institute for Economics and Peace in its Global Terrorism Index (GTI) for 2014. According to the GTI, Fulani militants were then the fourth most dangerous terrorist group behind Boko Haram, the Islamic State and the Taliban. The GTI thus

[3] S. Piłaszewicz, *Potęga Księgi i Miecza Prawdy. Religia, cywilizacja i kultura islamu w Afryce Zachodniej*, Warszawa 1994.

treated the Fulani as an organisation rather than as a people where men, as in most pastoralist peoples, become fighters when necessary, but that does not mean they are terrorists. The Fulani and related Tukuler population totals more than 40 million people living from the Atlantic coast to Sudan and the Central African Republic. They speak the Fulde language and are renowned for their puritanism, neophyte zealotry and belief in ethnic and linguistic superiority. The organisations they have established are well known. These include Ansar al-Islam in Burkina Faso, closely linked to the Jama'at Nasr al-Islam wa al-Muslimin (Islamic and Muslim Support Group)[4], Al-Jabhat li Tahrir al-Macina (the Macina Liberation Front), also known as Katiba Macina (Macina Battalion) or Retour, Reclamation et Réhabilitation, 3R (Return, Reclamation, Repair), a movement controlling an area in the Central African Republic along the border with Cameroon. The Fulani were and are also present in the Jama'at at-Tawhid wa al-Jihad fi Gharbi Ifrikija (Group of Unity and Jihad in West Africa) or Ad-Dawla al-Islamijja fi as-Sahra al-Kabira (Islamic State in the Greater Sahara). The GTI report lacks information on these organisations, especially Ansar al-Islam and Katiba Macina, which is perhaps due to an oversight. The former is responsible for massacres of people in the north and east of Burkina Faso and the flight from their homes of 1.9 million people. Its leaders, brothers Ibrahim Malam Dicko and Jafar Dicko, have since the organisation's inception in 2016 referred to the emirate of Djelgaudji, the historic Fulani kingdom in the north of Burkina Faso. The Macina Liberation Front was founded in 2015 by the Fulani charismatic preacher Amadu Kuffa, known for his criticism of the Malian authorities. Such rhetoric in turn alluded to the emirate of Macina. The grouping is notorious for its attacks on the villages of farmers of the Bambara and Dogon peoples in Mali's Mopti region. The latter formed the armed militia Dan Na Ambassagu (Hunters who trust in God) to defend the inhabitants. In March 2019, in retaliation for numerous attacks, its members invaded the Fulani-inhabited village of Ogossogu and killed 160 people, including the village leader and his grandchildren. The massacre caused shock across the state and forced the government to resign in April 2019.

[4] The organization formed in March 2017 by: Tanzim al-Qaeda bi Bilad al-Maghrib al-Islami (Al-Qaeda Organization in the Islamic Maghreb Countries) operating in the Sahel zone, Ansar Dine (Supporters/Defenders of Religion), Al-Murabitun (Guardians) and Al-Jabhat li Tahrir al-Macina (Macina Liberation Front).

In the final subsection entitled: *Economic situation* there is confusion in the dates and events cited, especially on pages 46-47. In this section, the author has also addressed the issue of the jihadists taking control of food production in north-eastern Nigeria and charging levies on food products. It seems that a discussion of this topic should have been included in the fourth subsection *Financing activities* of Chapter 2. It is entitled: *The organisational structure of Boko Haram* and contains a lot of interesting information and presents a large body of knowledge by the author, but even there one notices misspelled names of organisations or not very accurate terms. In the lede to this chapter, Stempień reports: *In 2012, a group called the Front for the Defence of Muslims in Black Africa, known as Ansaru and less commonly referred to as Al-Qaeda in Lands Beyond the Sahel, broke away from Boko Haram* (p. 52). The named organisation was called the Jama'atu Ansarul Muslimina fi Biladis Sudan (Association for the Defence of Muslims in the Black Lands). The full name is not given until p. 59, but 'Ansaril' was erroneously used instead of the noun 'Ansarul', similarly 'Ahlus' instead of 'Ahlis' or 'Afriqiya' instead of 'Ifriqija'. The structure of the chapter itself was also not well thought out. The subsequent subsections *Genesis and evolution of Boko Haram*, *What Boko Haram means* and *Organisational structure and authority* have been filled with content in such a way that many events are repeated and the chronological and factual order has been largely disrupted, giving the impression of chaos. It is difficult to sort out the succession of events and how the relationships linking the main actors were arranged during the periods in question. The author distinguished five periods in the evolution of Boko Haram: 1970-1990, 2001-2009, 2010-2013, 2013-2015 and the post-2015 period. In contrast, she listed other phases of Boko Haram's evolution in Chapter 4. on p. 119: the Kanama phase (2003-2005), the dawah phase (2005-2009), and the reorganisation phase (since 2009). It seems that it would have been more correct to merge these two chapters, especially since it is in Chapter 2 that the author writes about Kanama in Yobe State, where the first camp of Islamic extremists dubbed 'Afghanistan' was established and where members of the group were referred to as the Nigerian Taliban.

The author devotes much space to the concept of takfir, or exclusion from the ummah. Muhammad al-Maghili (1440-1505) is considered to be its founder. His teachings were used by Usman dan Fodio, the founder of the Sokoto Sultanate in 1809. Today, many Muslim terrorist organisations use this concept to exclude from the ummah those Muslims who do not

share their views and do not wish to join them. Among them were Boko Haram and the Islamic State. The main idea preached by Ustaz Mohammad Yusuf, founder of the former, was to overthrow the Nigerian government and impose a literal interpretation of the Koran. The movement was called Yusufiya after his name. An important event in the history of Boko Haram was the rejection of the Western education system as destructive of belief in one God and the acceptance of the one correct truth that the author of all phenomena and things is God. In 2009, members of the organisation staged an uprising in the city of Maiduguri, the capital of Borno State, to overthrow the government and declare the state a caliphate. Street fighting spread from Maiduguri not only across the state, but also to neighbouring Yobe and further afield - Bauchi and Kano. The beginning of the unrest can be seen as July 2009, when the Boko Haram militia attacked a police station in Bauchi town. Subsequently, Islamic extremists carried out violent attacks in other cities in northern Nigeria. Targets of the attacks included police stations, prisons, government buildings, local administration facilities and churches. In September 2009, more than 700 prisoners were freed during an attack on the federal prison in Bauchi. There has been an escalation of conflict between Muslims and Christians. More than 700 people were killed in Boko Haram attacks and many families abandoned their belongings and fled their homes. The government has deployed military forces to pacify the extremists and protect the population. In Maiduguri, approximately 500 people were killed as a result of the fighting. Police demolished a Boko Haram mosque where extremists were resisting. Hundreds of followers were arrested, including Yusuf. A few days later, his corpse was found on one of the streets in Maiduguri. Police said he had died while trying to escape. The authorities announced that the Boko Haram movement had been destroyed once and for all, which turned out not to be true.

Following Yusuf's death, leadership of the organisation was assumed by Shekau. Since 2010, there has been progressive armed activity and escalating violence by Boko Haram. The organisation is recruiting more and more excluded young people living on the margins of society. On 6 June 2011, a Boko Haram militant carried out an attack on the police headquarters in Abuja. This was the first suicide attack in Nigeria in which a booby-trapped car was used. The attack was in response to the Nigerian police chief's stay in Maiduguri, which called for the group's eradication. In 2012, some of its members, led by Khalid al-Barnawi alias Abu Ussamata

al-Ansary (arrested in early April 2016), left Boko Haram. The reason for the break-up was the secessionists' opposition to the murder of Muslims. The latter considered, according to the concept of takfir, as infidels and deviants from the faith, deserved only death, according to Shekau. Mass murders were the order of the day. Al-Barnawi's organisation adopted the aforementioned name: Jama'atu Ansarul Muslimina fi Biladis Sudan, relocated its base to neighbouring Cameroon and established cooperation with Tanzim al-Qaeda bi Bilad al-Maghrib al-Islami (Al-Qaeda Organisation in the Islamic Maghreb). On p. 60, the author reports another split in Boko Haram, which occurred in mid-2015. At that time (...) *Mamman Nur and Abu Musab al-Barnawi, son of Mohammed Yusuf, split from Boko Haram and took an oath of allegiance to the Islamic State, proclaiming the West Africa Province (Wilayat Gharb Afriqiya - WGA)*. She elaborates on this thesis on p. 74. However, it was the Shekau that accepted the supremacy of the Islamic State in early 2015, officially changing the name of their organisation to the Islamic State's West Africa Province. It should not be forgotten that the headquarters in Iraq wanted to take control of Boko Haram and sought to weaken Shekau's position. This was due to his opposition to Caliph Abu Bakr al-Baghdadi's plans to expand Boko Haram's activities beyond Niger and Cameroon under the idea of global jihad and to entrust the leadership of the group to a collegiate body (*the Majlis Ash-Shura*). It would include the self-appointed caliph Mamman Nur and Abubakar Adam Kambara, which would deprive Shekau of his one-man command of Boko Haram. Reducing his influence was also served by Al-Baghdadi's ordered division of Boko Haram fighters into three groupings, which were dislocated to northern Cameroon, the Lake Chad area and eastern Niger. Shekau would be tasked with coordinating these activities, mainly in northern Nigeria. Disagreements between the leaders over the territorial scope of operations and powers led to Shekau's refusal to fully submit to the Islamic State's central command, which removed him from his position as conductor of the West African Province in August 2016. Shekau broke from his subordination to the central command in Iraq, retaining leadership over Boko Haram fighters loyal to him. In contrast, Abu Musab al-Barnawi (who died in August 2021) became the leader of the West African Province. The dispute between the two organisations escalated into an armed confrontation. It resulted in the death of Shekau in May 2021.

In subsection four, Stempień writes about the financing of Boko Haram's activities, and in subsection five about the ideological foundations

of the organisation. In the reviewer's opinion, it would have been better to swap them in places, and to weave into subsection five parts of the text from subsection three (*Organisational structure and authority*), a large part of which is also devoted to the ideological foundations of the organisation. The last subsection, on the other hand, deals with Boko Haram's media apparatus and propaganda.

Much better than the first two chapters is Part 3 of the monograph: *Victims of Boko Haram*. It is written in a clear and structured manner, and the various subsections are filled with interesting content. Noteworthy among others is the inclusion of information that in 2014, Boko Haram and the Islamic State were responsible for more than half of the fatalities in terrorist attacks. In the same year, however, the Nigerian organisation overtook the Islamic State in terms of fatalities. The ratio was 6644 to 6073 deaths. It is estimated that from its inception until the end of 2020 Boko Haram is responsible for the deaths of around 40 000 people, mostly civilians. Sexual violence by members of the organisation, to which the author devoted a separate subsection, was linked to the kidnapping of schoolgirls from schools and boarding schools. Women and girls were forced into marriages. They were also a reward for new fighters joining the ranks of the organisation. This phenomenon, which is so prevalent in the Islamic State within Iraq, came to prominence in April 2014, when Boko Haram abducted 276 schoolgirls aged between 12 and 17 from a school in the town of Chibok in Borno State, as described in a separate subsection. This incident provoked an international response, but was no exception. A few months later, jihadists kidnapped 300 schoolchildren and another 100 women and children in the town of Damasak, an incident that the media had already kept quiet about. The fact is that the kidnapping of the girls in Chibok made the eyes of the world look at Nigeria with concern. A 'Return our girls' campaign swept through social media, with even US First Lady Michelle Obama joining in. This was meant to put pressure on Nigerian forces. However, despite the promises of African politicians and the passage of eight years since that incident, the fate of more than 100 girls, now women, is unknown. Freedom was regained by those who managed to escape on their own. One of them, with a child, was found on 14 June 2022 by a squad of Nigerian armed forces patrolling near the village of Ngoshe in Borno State. Stempień reports that the total number of abductions during the conflict is not known, but it is estimated that between 500 and 2 000 women and children have been abducted since 2012. These estimates are,

however, highly underestimated, as according to Amnesty International, from early 2014 to April 2015 alone. Boko Haram has abducted at least 2,000 women and children. The women are used as sex slaves, kitchen helpers, as bargaining chips in negotiations to secure the release of prisoners and for terrorist attacks. It should be noted that the practice of kidnapping schoolchildren from schools and boarding schools is still being carried out by other bandit groups operating in the northern states of Nigeria, outside the area of Boko Haram activity. On 6 April 2022, the Nigerian authorities labelled these gangs as terrorist groups that deserve the same treatment as Boko Haram. President Muhammadu Buhari named two organisations: Yan Bindiga (Members of Bindiga) and Yan Ta'adda (Members of Ta'adda). They kidnap people for ransom.

The following five subsections characterise the major terrorist attacks from 2016 to 2020. Complementing the information on each year are clear tables listing terrorist attacks that killed more than 20 people, detailing the date, location and manner of the attack, as well as the number of fatalities. The final subsection looks at Boko Haram activity in 2020 and the impact of the coronavirus pandemic on the organisation's activities.

Chapter 4 is entitled *Military evolution*. Its separation as a separate section results in a duplication of information contained in the previous chapters. Avoiding these repetitions would have resulted in much ambiguity and fragmentation of the narrative structure. However, they detract from the scientific value of the book, although they certainly contribute to the reader's consolidation of knowledge. This remark applies in particular to subchapter one: *Political-military strategy*. In the reviewer's opinion, it would have been more beneficial to discuss the issues contained therein in subchapter one of chapter 2: *The origins and evolution of Boko Haram*. The same comment applies to subchapter two: *Methods and tools of action* and in part also the others. Thus, it can be concluded that the construction of the book has not been well thought out. However, it should be noted that the information contained in this section is of great cognitive value. They fully reveal Boko Haram's tactics and methods of operation, which in many cases may have been surprisingly innovative in relation to the Islamic State's strategy.

Women and children played a huge role in the carrying out of terrorist attacks by Boko Haram. Although the use of female suicide bombers by the Nigerian organisation was no novelty, the scale of this practice is unmatched by any other terrorist group. This is illustrated by the graph

on p. 130, which shows that Boko Haram women were responsible for as much as 48 per cent of suicide terrorist attacks worldwide from 1985 to 2018. This scale is even more appealing when one considers that the first suicide attack was carried out by Boko Haram in 2011.

Far more controversial is the use of children to carry out suicide attacks. In 2015, 44 children were forced to do so in Nigeria, Cameroon and Chad, compared to 'only' four the year before. The total number of suicide attacks in these three countries and in Niger carried out by Boko Haram and the Black Muslim Defenders Association rose from 32 in 2014 to 151 in 2015. To add to this striking statistic, it should be mentioned that 83 children, including 55 girls, were blown up between 1 January 2017 and 16 August 2017 alone. Most of them were less than 15 years old. To one of them, an infant was additionally attached with tape to distract the police. The terrorists usually attached an explosive device to the child and then left it in some crowded public place. The bomb was then detonated remotely. In several cases, the children managed to escape to police patrols, who removed the explosives from them and secured them. In March 2015, a teenage girl who managed to foil the bombing said she was one of the students kidnapped from the school in Chibok. Boko Haram is the first organisation in the world where a higher percentage of the attackers are children and women. Besides, the organisation's activities, like no other, have also had disastrous effects on education. Boko Haram has completely destroyed more than 900 schools and led to the closure of twice that number. More than 600 teachers and school staff were killed and 19 000 were forced to flee.

The fourth subsection discusses Boko Haram's links with other groups, including its relationship with the Al-Qaeda Organisation in the Islamic Maghreb, as well as with the Movement for Unity and Jihad in West Africa (Arabic: Jama'at at-Tawhid wa al-Jihad fi Gharbi Ifrikija, known as MUJAO from the French name Mouvement pour l'Unicité et le Jihad en Afrique de l'Ouest), which was formed in Mali in October 2011 as a result of the secession of some fighters from Al-Qaeda. They were led by Muhammad Kheiru alias Abu Kumkum. In August 2013, MUJAO merged with the organisation Katibat al-Mulassamin (Masked Battalion), also known as Muwakaun bi ad-Dima (Signed in Blood), led by the notorious Mokhtar Belmokhtar, to form the organisation Al-Murabitun (Guardians).

In the fifth subsection, *Links to the Islamic State and the establishment of an African caliphate*, the author revisits the issue of the emergence

of the Islamic State's West African Province, listing, among other factors, factors that may lead to divisions within the jihadist movement, as was the case with Boko Haram. Since 2016, Boko Haram and the West African Province have engaged in a bloody, terrorist rivalry, committing increasingly vicious and senseless killings. The victims were ordinary residents of towns and villages. It seems that the religiously radicalised perpetrators killed them for entertainment because they believed they were acting in the name of Allah. It is Allah in their view who dispenses justice on Earth. For example, on 9 June 2016, the Boko Haram group murdered 81 people in Gubio. On the same day, a local faction of the Islamic State killed 69 villagers in Felo, in retaliation for the military's earlier thwarting of a cattle theft from the village. Both villages are located in Borno State in north-eastern Nigeria. Many more similar examples can be found. However, over time, the rivalry turned into an open conflict between these organisations, in which the Islamic State emerged victorious. A reading of this subsection leads one to conclude that one could merge some of the content it contains with Chapter 2, entitled *Methods and tools of action*. Such a remark is all the more justified as it is only here that the author defines the phenomenon of jihadism and writes about the jihad waged in the early 19th century by Usman dan Fodio and the Sultanate of Sokoto.

The last section characterises the activities of Boko Haram in Cameroon, Niger and Chad. It is worth noting that the borders of these countries and Nigeria converge on Lake Chad. On its shores, fishing villages were attacked, buildings burned, people killed and abducted. According to the author, there has been no attack carried out by Boko Haram in Chad in which at least 20 people were killed (p. 147). Meanwhile, Table 12 on p. 115, which lists terrorist attacks carried out by the organisation in the first half of 2020, with a death toll of more than 20 people under the date of 23 March, lists an attack on a military base in Chad in which 98 soldiers were killed. On page 114, the author devotes only two sentences to this incident. It deserves a little more coverage also because, when discussing human rights violations and war crimes on p. 170, she devotes a little more space to the deaths of 44 people who died in prison. They were arrested in March 2020 after the 'Wrath of Boma' operation. However, the author does not elaborate on this, so the reader is left in the dark as to which operation Stempień had in mind. The reviewer feels obliged to complete this thread.

On the night of 22-23 March 2020, jihadists attacked a Chadian army base in Boma located on an island in Lake Chad. The siege lasted about

seven hours. 98 soldiers of the Chadian army, considered the most battle-hardened in the Sahel zone, were killed and 47 wounded. The attackers also attacked arriving reinforcements. They destroyed 24 vehicles, including armoured cars, and captured large quantities of weaponry, which they loaded onto speedboats and fled to Nigeria. It was one of Boko Haram's most spectacular attacks, inflicting the single greatest casualties on Chad's army in the 21st century. Chadian President Idriss Déby arrived on the scene and announced a retaliatory operation codenamed 'Wrath of Boma'. It lasted from 31 March to 8 April. At the time, Chadian soldiers drove Boko Haram militants from islands in Lake Chad, destroyed its numerous bunkers and entered the Nigerian province of Borno, where they freed several Nigerian soldiers held by the terrorists in the village of Magumeri. It was reported that around 1 000 Islamic extremists were killed. Fifty-eight jihadists were arrested and taken to a prison in the capital N'Djamena. There they were placed in a single cell. They were denied food and water for three days. On 18 April, it was revealed that 44 prisoners were found dead. This was an extrajudicial execution carried out by Chadian security forces.

At the end of the chapter, the author draws the conclusion that, given the areas of Islamic State activity, attacks in Niger, Burkina Faso or Mali should be attributed to the Islamic State in the Greater Sahara, while those in the Lake Chad region should be attributed to the Islamic State in the West African Province. However, this is a gross oversimplification, as part of Lake Chad belongs to Niger. Other terrorist organisations are also active in some of these states, and bandit groups have furthermore been organised in north-western Nigeria. The Diffa region in south-eastern Niger, on the border with Nigeria, was attacked by Nigerian armed groups that could not be identified. Attacks in the region were attributed to Boko Haram or the Islamic State. However, the author's prediction of the intensification of activities and militarisation of the Boko Haram faction subordinate to the Islamic State headquarters came true. In 2021, West Africa Province defeated the 'mother' faction of Boko Haram and took over a central role in the jihadist movement in Nigeria.

The final chapter, *Countering the expansion of Boko Haram*, consists of four subchapters. The first two deal with counter-terrorism activities by Nigeria's armed forces and allies. The author draws attention to the initial downplaying of Boko Haram's activities by the Federal Government of Nigeria, which led to the loss of control over three provinces - Borno, Yobe and Adamawa - and its ability to act as a security guarantor. The legal

basis for the fight against terrorism was supposed to be the Prevention of Terrorism Act of 2011, but it was only two years later that a state of emergency was declared in the aforementioned states and President Goodluck Jonathan gave notice of an offensive against Boko Haram. It was conducted in a low-key manner. Successes in one place were accompanied by spectacular failures in others. Although it succeeded in pushing the militants out of some towns, the rural areas were under their control, not to mention the Sambisa forest and the mountainous region of Gwoza and the Mandara massif, where the organisation had deployed permanent bases that still function practically today, but were taken over by the West African Province in 2021. The central states of Nigeria, not excluding the capital Abuja, where the police headquarters was attacked, were threatened by terrorist attacks. The armed forces were accused of human rights violations, including numerous arrests of innocent people, torture and extrajudicial executions of real and alleged Boko Haram members. Pacifications of entire villages suspected of favouring the organisation were the order of the day. Many residents fled from the jihadists and the army.

Stempień gives figures for arrests and crimes committed by the armed forces. They also compromised with the abduction of 276 schoolgirls from a school in Chibok, mentioned earlier. The incident itself was not a challenge to the authority of the security forces, but the inability to find and recapture the abducted girls was. The next president, Muhammadu Buhari, a retired general who went into the 2015 elections with the slogan of eradicating the jihadist insurgency in the north-east of the country within one year, failed to deliver on his promise. Instead, civilian institutions teamed up with the army to form the Civilian Joint Task Force. Volunteers trained and armed by the army, however, suffered heavy losses in clashes with militants, although there were some victorious battles of anti-jihadist militias. The author writes about the initiatives of the international community in fighting Boko Haram, including the activities of the Multinational Joint Task Force, which brought together the military forces of Nigeria, Niger, Cameroon and Chad, supported by the US, France and the UK. What it did not mention were the mercenaries recruited by the South African security company Pilgrim Africa. The owners of Pilgrim offered the Nigerian government to come in early 2015 with their own troops, weapons, South African armoured vehicles and post-Soviet Mi-24 helicopters, piloted by experienced crews from Ukraine. According to the Nigerian press, the mercenaries, officially hired to train the government's military, have

been cushioning them in the war against the jihadists. They fought at night, equipped with state-of-the-art night-vision equipment. In the morning, they would retreat to bases, allowing themselves to be replaced as liberators by Nigerian soldiers. Nigerian authorities announced that they had recaptured about 40 villages from Boko Haram, but made no mention of mercenary assistance.

Subsection three addresses, among other things, the problem of deradicalisation of militants. The Nigerian authorities have for many years taken advantage of amnesties, leniency and agreements with various insurgent groups. In 2015, a controversial programme was created for 'repentant' lower-ranking Boko Haram deserters. A reintegration plan called Operation Safe Corridor, initiated by the army and facilitating desertion, was also launched. Other projects for the rehabilitation and reintegration of 'repentant' fighters and girls and women kidnapped by Boko Haram who have regained their freedom but have been excluded by their family or village community by having children with the fighters have also been launched.

Boko Haram's activities have led to a humanitarian crisis in Nigeria, to which the last subsection is devoted. This crisis has been compounded by, among other things, human rights violations and war crimes. The author provides statistics from Amnesty International's research and information contained in the Global Peace Index. In the context of documented war crimes, she mentions the deaths of 44 temporary detainees in N'Djamena prison. These were Boko Haram fighters captured by Chadian armed forces during the aforementioned Wrath of Boma operation. The terrorist activities of Boko Haram, the Islamic State and counter-terrorism operations have caused several million people to flee their homes and be displaced in north-eastern Nigeria and neighbouring countries. In many camps, displaced people have faced starvation and lack of access to hygiene and basic medical care. The scale of the destruction wrought by Boko Haram has been unimaginable, as satellite images have shown that many villages have been burnt to the ground. Their inhabitants were killed and those who survived fled or were displaced early. The crisis over Boko Haram's activities has been exacerbated by the security forces. Their operations to break up the jihadists often led to extrajudicial executions. The victims were captured militants or people suspected of belonging to the organisation. The military also destroyed villages that had coercively or voluntarily supported the extremists.

In conclusion, the author briefly summarised the issues raised in the book and presented her conclusions. She confirmed the hypothesis adopted in the introduction that the expansion of Boko Haram has significantly contributed to the deepening destabilisation of Nigeria. However, it is worth noting that this is the case in any country where major terrorist organisations operate. From African countries, by way of example, we can mention: Somali, Mozambique, Congo, Mali or Burkina Faso. Stempień stated, among other things, that as part of the research process, she was able to show the evolution of Boko Haram and to point out possible directions for the further activities of this organisation. As she rightly pointed out earlier, it has been dominated by the Islamic State in West Africa. In contrast, one cannot agree with the conclusion that the armed struggle against the jihadists is important but secondary, because (...) *the priority should be to 'invest' in the non-military aspects of the fight against the jihadists, i.e. deradicalisation, rehabilitation and reintegration programmes. One of the main challenges will be to convince Nigerians to trust such initiatives*. In the reviewer's view, only military action against terrorist organisations and the physical elimination of leaders should be the priority, rather than "pushing jihadists out of occupied areas", as the author states. The experience of many countries shows that deradicalisation of Islamist militants yields little results. It is very difficult to verify whether a person has actually moderated his views and whether his repentance is sincere. It is also not easy to predict the subsequent behaviour of such people. Very often they only pretend to change their behaviour in order to divert the attention of the security services.

The French have openly admitted that they are helpless in the face of the radicalisation of Muslim youth. In 2017, the French Senate published a report on government programmes to deradicalise Muslims. It unequivocally stated that they had been a complete failure. Also in the opinion presented by the French prosecutor's office on the occasion of the announcement of the sentences for the attacks in Paris on 13 November 2015, there can be no illusions about the possibility of rehabilitation and deradicalisation of Islamic extremists. Fanatics rarely abandon their ideology during stay in prison. However, imprisonment is the only acceptable way to protect society from those who pit so-called divine justice against justice, and by murdering, inflict what they believe to be just punishments.

The reviewed publication is accompanied by photographs, maps, charts and tables. At the end of the book there is an extensive bibliography divided into: dictionaries and encyclopaedias, compact studies, articles, legal acts, netography. The monograph is supplemented by a list of illustrations and tables and indexes: of names and geographical names. Marta Sara Stempień's study is a valuable study of Boko Haram. In the text, the author of the review mentions, among other things, inaccuracies in the translation of some terms. However, these do not affect the content of the work. A bigger shortcoming, however, is starting a given thread in one section only to continue it in the next chapter. This forces the reader to return to the material already read in order to take a holistic view of the issue addressed, such as the history of Islam in Nigeria or the evolution of Boko Haram. Nevertheless, the reviewer strongly encourages the reader to read this publication, which is important from the point of view of the terrorist threat in Africa and illustrates difficulties and failures of counter-terrorism operations.

Krzysztof Izak

Retired Internal Security Agency officer.

https://doi.org/10.4467/27204383TER.23.034.18336
https://orcid.org/0000-0001-6716-3224

MARCIN WIELEC

Book review: **Legal aspects of the European intelligence services' activities** edited by Piotr Burczaniuk, PhD[1]

At the end of 2022, the publishing house of the Internal Security Agency released an English-language multi-author monograph entitled *Legal aspects of the European intelligence services' activities*) scientifically edited by Piotr Burczaniuk, PhD. It focuses on the functioning of special services within the legal systems of 19 European countries, i.e. Austria, Belgium, Bulgaria, Croatia, the Czech Republic, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Romania,

[1] *Legal aspects of the European intelligence services' activities,* P. Burczaniuk (scientific editor), Warszawa 2022, Agencja Bezpieczeństwa Wewnętrznego.

Slovakia, Spain and Sweden. The book discusses the organisational models, structure and scope of competences of the special services in the mentioned countries, as well as selected problems related to their activities.

The book is 302 pages long and consists of 20 chapters and an extensive bibliography. It begins with a foreword by the Head of the Internal Security Agency, Colonel Krzysztof Wacławek, and an introduction by Burczaniuk. Then, within the framework of 19 chapters devoted to individual countries, analyses concerning the issues indicated in the title are presented, carried out on the basis of a clear scheme proposed by the scientific editor of the publication. According to this scheme, the chapters consist of two main parts. In the first, the authors discuss: the place of a given service in the national legal system, the legal definition of special services, their position and role in the public administration system, the activities they carry out, control and supervision of services, the legal status of officers and employees of services. The second part is devoted to issues selected by the authors related to the activities of such entities, including: the tasks and mandate of the services, especially their investigative powers, the role of the services in criminal proceedings, information collection, protection of classified information and personal data, and international cooperation. Given the multiplicity of the countries in question, the diversity of their legal systems and the issues to be analysed, the introduction of a common structural template should be viewed positively.

The only chapter that deviates from the pattern described and provides a valuable complement to the previous considerations is the twentieth chapter, entitled *National Security Clause in the EU Law and Its Implications for Intelligence and Security Services*. It presents selected issues related to the policies of the European Union countries and their secret services in the context of national security, and the concept of national security itself is put into a broader perspective, taking into account recent case law of the Court of Justice of the European Union.

It appears that the legal systems of the states described in the publication have, despite their differences regarding the models and location of the special services, many features in common. Among the issues that are universal and yet most controversial are the supervision and control of such state structures and the status of their officers.

The book in question should be rated very highly. Not only the collection in one place of comprehensive analyses concerning special services of so many countries deserves appreciation, but also the selection

of authors. These are persons who are experts in their respective fields and, above all, are directly involved in the activities of special services in individual states and who use the legal acts described in the book in practice. As a result, the analyses presented are credible, reliable and concrete, and the issues raised are up-to-date. They also touch on issues as vital as cyber security, *big data* and disinformation.

In the literature of legal sciences, political sciences and national security, the monograph *Legal aspects of the European intelligence services' activities* is a unique publication. It can be of great use to professionals dealing with the issues of special services and to academics due to the fact that it brings together and discusses many important issues related to the functioning of special services in as many as 19 European countries.

Marcin Wielec, Assoc. Prof.

Deputy Dean of the Faculty of Law and Administration of Cardinal Stefan Wyszyński University in Warsaw, Head of the Chair of Criminal Proceedings of the Faculty of Law and Administration of Cardinal Stefan Wyszyński University in Warsaw, Director of the Justice Institute. Author and co-author of several books and many scientific articles on criminal proceedings. Member of the Programme and Scientific Council of the quarterly "Probation". Graduate of the IESE Business School and the National School of Public Admini stration.

AWARDED THESES

https://doi.org/10.4467/27204383TER.23.035.18337
https://orcid.org0009-0009-3421-6399

JAKUB TUSZYŃSKI

Effectiveness of selected AI models in predicting victims of terrorist attacks[1]

Abstract

Terrorism continues to be a problem for many countries around the world. The article compares the effectiveness of selected machine learning algorithms in predicting the victims of terrorist attacks in order to answer the question of whether they can serve as one of the anti-terrorist tools. An exploratory data analysis was carried out, and selected trends and characteristics of terrorist attacks were discussed. Some measures for evaluating the classification algorithms used in the study are presented, and potential directions for further research are indicated.

Keywords:

AI,
machine learning,
terrorism,
victims,
classification

[1] The article is based on a master's thesis entitled *Effectiveness of selected AI models in predicting victims of terrorist attacks*, defended at the Faculty of Journalism, Information and Bibliology, University of Warsaw. The author used excerpts from chapters 3 and 6. The thesis was awarded in the 12th edition of the competition of the Head of the Internal Security Agency for the best doctoral, master's or bachelor's thesis concerning state security in the context of intelligence, terrorist, economic threats.

Investigation of terrorist attacks

Due to definitional disputes, for the purposes of this article, a terrorist attack is assumed to be (...) *an intentional act or threat of violence by a non-state actor*[2]. As part of this article, a study was conducted to compare the effectiveness of different artificial intelligence algorithms in predicting the victims of terrorist attacks. The study used the Global Terrorism Database (hereafter: GTD) maintained by researchers from the START consortium[3], which contains information on terrorist attacks.

The GTD has adopted three criteria, at least two of which must be met for an event to be considered a terrorist attack. These are:

- the act of violence was intended to achieve a political, economic, religious or social objective;
- the act of violence contained evidence of intent to coerce, intimidate or otherwise convey a message to a wider audience other than the immediate victims;
- the act of violence fell outside the scope of international humanitarian law[4].

Events where the amount of information was insufficient to clearly determine whether the event was a terrorist attack or not and are filterable by the user were also flagged.

Assumptions

In order to eliminate, as accurately as possible, cases in which an event was misclassified as a terrorist attack, those observations that did not meet all three criteria described above and those about which the authors of the database had doubts were excluded.

Victims of an attack are considered to be any non-terrorist person injured or killed as a result of the incident. Several machine learning models were built and compared using appropriate metrics.

---

[2] *Data Collection Methodology*, Global Terrorism Database, http://www.start-dev.umd.edu/gtd/using-gtd/ [accessed: 21 V 2022].

[3] *History of the GTD*, Global Terrorism Database, https://start.umd.edu/gtd/about/History.aspx [accessed: 11 V 2022].

[4] *Data Collection Methodology*...

Exploratory data analysis

During the exploratory data analysis, the focus was on understanding the dataset under study. First, a structural analysis was carried out.

Figure 1 distinguishes the following features of the collection:

- more than 200 000 lines of recorded attacks;
- 135 columns containing characteristics describing the event in question;
- The *dtypes* describe the data types of the individual columns. These are categorical data, having a finite number of categories - 9, columns containing floating point numbers - 53, integers occurring in 24 columns and 49 columns containing data that can be both strings and numbers. The data type *object* is assigned when no other data type can be explicitly assigned;
- the collection takes up approximately 200 megabytes of memory.

```
Int64Index: 201183 entries, 0 to 201182
Columns: 135 entries, eventid to related
dtypes: category(9), float64(53), int64(24), object(49)
memory usage: 197.1+ MB
```

Figure 1. Basic statistics describing the dataset.

Source: own elaboration.

Next, data that did not meet all three criteria for a terrorist attack and those about which the authors of the database had doubts were filtered out. Columns in which 50 per cent or more of the rows were empty were also removed. The purpose of reducing the dataset was to speed up the operations performed on it. In addition, most of the machine learning algorithms used in the study require the dataset to have no empty values. Complementing them with the mean, median or most frequent value with such a large number of empty observations would result in an unauthorised generalisation from a small amount of data. This operation reduced the dataset to 154 260 rows and 60 columns, with a file size of just under 70 megabytes.

In the next step, the basic values of the individual columns were checked. The x-axis shows the column names and the y-axis shows

the calculated statistics: number of observations, mean, standard deviation, minimum value, first quartile, median, third quartile and maximum value.

In Figure 2, it can be seen that the *latitude* and *longitude* variables contain missing values, which were appropriately reprocessed by removing the rows with missing values in these variables, so they were used during modelling. It is also worth noting the minimum value of the *vicinity* variable, which is -9 (this is visible in the last row of the *min* column). The authors of the database mark cases of missing data in this way. This is described in the so-called *Codebook*[5].

	count	mean	std	min	25%	50%	75%	max
eventid	154260.0	2.005463e+11	1.294940e+09	1.970000e+11	1.995042e+11	2.012022e+11	2.015091e+11	2.019123e+11
iyear	154260.0	2.005397e+03	1.294946e+01	1.970000e+03	1.995000e+03	2.012000e+03	2.015000e+03	2.019000e+03
imonth	154260.0	6.443965e+00	3.392222e+00	0.000000e+00	4.000000e+00	6.000000e+00	9.000000e+00	1.200000e+01
iday	154260.0	1.553523e+01	8.803117e+00	0.000000e+00	8.000000e+00	1.500000e+01	2.300000e+01	3.100000e+01
extended	154260.0	5.527032e-02	2.285079e-01	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	1.000000e+00
country	154260.0	1.297654e+02	1.110024e+02	4.000000e+00	7.800000e+01	9.700000e+01	1.600000e+02	1.004000e+03
region	154260.0	7.321360e+00	2.838782e+00	1.000000e+00	6.000000e+00	8.000000e+00	1.000000e+01	1.200000e+01
latitude	151329.0	2.369732e+01	1.798608e+01	-5.315461e+01	1.184079e+01	3.153824e+01	3.451689e+01	7.403355e+01
longitude	151329.0	3.227138e+01	5.485520e+01	-1.578583e+02	9.735686e+00	4.414823e+01	6.914701e+01	1.793667e+02
specificity	154259.0	1.447591e+00	9.567426e-01	1.000000e+00	1.000000e+00	1.000000e+00	1.000000e+00	5.000000e+00
vicinity	154260.0	6.333463e-02	2.803160e-01	-9.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	1.000000e+00

Figure 2. Extract from statistics on numerical variables.

Source: own elaboration.

Figure 3 shows the statistics for the text variables: number of observations, number of unique values, most frequent value and its frequency.

In the dataset, some of the variables appear in both numeric and text form. This is, for example, the variable *region_txt* (Figure 3) and the variable *region* (Figure 2). This was taken into account before modelling because of the possible correlation between the same variables and the unnecessary complexity of the dataset, which translates into a slower model training process.

[5] *Codebook: Inclusion Criteria and Variables*, Global Terrorism Database, August 2018, https://www.start.umd.edu/gtd/downloads/Codebook.pdf [accessed: 30 V 2022].

	count	unique	top	freq
country_txt	154260	202	Iraq	23407
region_txt	154260	12	Middle East & North Africa	43858
provstate	154260	2380	Baghdad	7563
city	153874	34443	Unknown	7594
summary	112205	109189	09/00/2016: Sometime between September ...	100
attacktype1_txt	154260	9	Bombing/Explosion	79879
targtype1_txt	154260	22	Private Citizens & Property	43145
targsubtype1_txt	144441	112	Unnamed Civilian/Unspecified	11599
corp1	123010	32224	Unknown	18458
target1	153807	73022	Civilians	7489
natlty1_txt	152648	209	Iraq	23077

Figure 3. Extract from statistics on categorical variables.

Source: own elaboration.

There is also an apparent problem with the high number of unique values of some variables, such as *city*, which may have affected the performance of the models built. This problem was resolved during data processing by removing such variables from the dataset.

In the next step, empty values were removed from the variables affecting the number of injured and killed. The problem of giving the total number of victims killed and injured by the incident with the number of terrorists killed and injured was then solved. The number of terrorists was subtracted from the total number of killed and injured to obtain the number of non-terrorist casualties.

After this operation, new variables were created: *ncasualites*, which is the sum of killed and injured, and *cas_class*, where zero was used to denote cases where there were no casualties and one to denote those events where there were casualties. The preprocessed data were then saved to a new file.

Trends in the number of terrorist attacks and the number of victims

Visualisations of some of the variables were produced, allowing for a more in-depth analysis. The charts show the number of terrorist attacks carried out between 1970 and 2019 and their victims.

From the second half of the 1970s to the early 1990s, there was an increase in the number of attacks (Chart 1) as well as their victims (Chart 2). The marked increase in the number of victims in 2001 is due to the 11 September attack on the World Trade Center (WTC). Another noticeable upward trend in both occurred in 2005 and continued until

2014-2015. With, as already mentioned, the increase around 2012 is partly due to a change in data collection methodology[6], however, this increase started even before 2005. Since 2015, a decreasing trend in the number of both attacks and victims can be seen. As of 4 June 2022[7], researchers from the START consortium have not published data from 2020-2021, so the impact of the COVID-19 pandemic on the dynamics of the incidence of terrorist attacks is unknown.

Chart 1. Number of terrorist attacks 1970-2019.

Source: own elaboration.

Chart 2. Number of victims of terrorist attacks 1970-2019.

Source: own elaboration.

[6] Identifying terrorist incidents to the GTD prior to 2012 required the use of approximately 300 unique news sources. After the 2012 update, more than 1,500 unique news sources were used. These sources included international news agencies and English translations of local newspapers published in various foreign languages.

[7] Update - as of 15 July 2023, data from the first half of 2021 are available.

The number of terrorist attacks and their victims was then visualised by region (Charts 3 and 4).

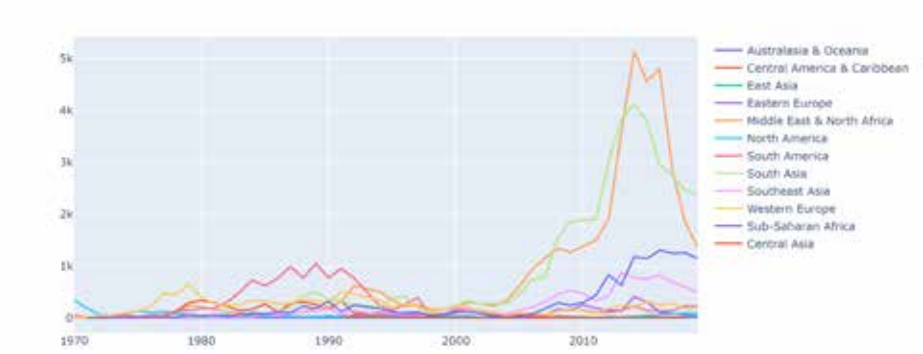


Chart 3. Number of terrorist attacks 1970-2019 by region.

Source: own elaboration.

In Western Europe, most attacks took place in the second half of the 1970s, which did not translate into an increase in the number of victims. A similar situation can be observed in South America between 1980 and 1995, when there was a dynamic increase in the number of attacks (also not translated into casualties). In the 1990s, there was a decline in the number of attacks in all regions. Nevertheless, an increase in casualties was observed in Sub-Saharan Africa, the Middle East and North Africa, and South Asia and East Asia. The sharp increase in casualties in 2001 in North America is not a data entry error, as that was when the attack on the WTC took place.

The Middle East and North Africa region, South Asia and Sub-Saharan Africa also saw an increase in the number of attacks and casualties in the early 2000s. The growth curve in the Middle East stands out in particular, being steeper than the curves of the two previously mentioned regions. This may be related to the US intervention in Afghanistan and Iraq. In the Middle East, the number of casualties in 2000 was around 900, and in 2005 it was almost 9,000. Since 2015, there has been an apparent downward trend in the number of both terrorist attacks and victims (with the exception of South Asia, where upward trend in the number of casualties is observed).

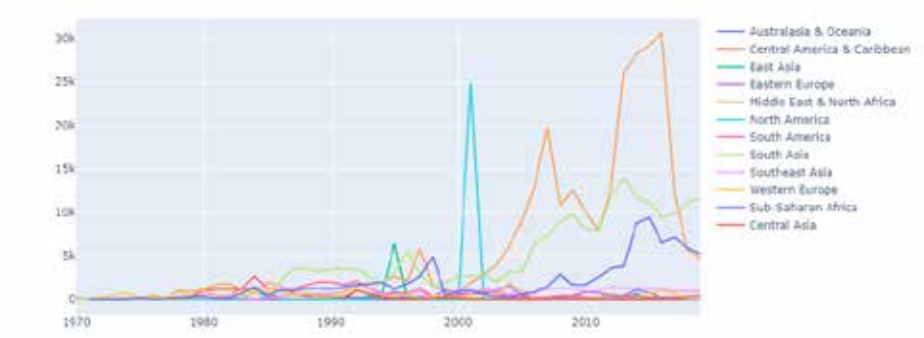


Chart 4. Number of victims of terrorist attacks 1970-2019 by region.

Source: own elaboration.

It is worth noting the Western European area during this period, as despite the migration crisis of 2015, there has been no marked increase in terrorist attacks there (Chart 5).

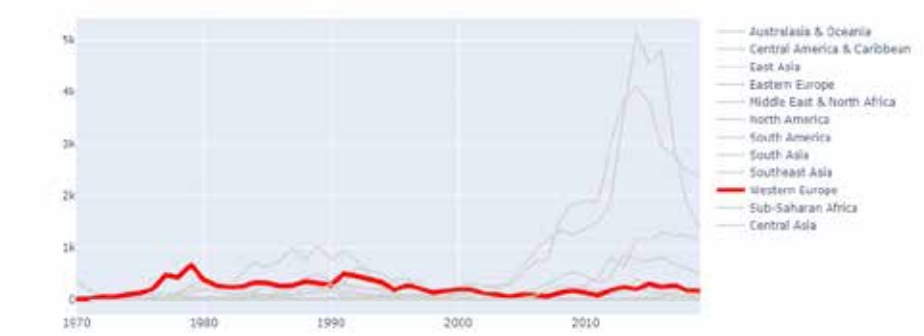


Chart 5. Number of terrorist attacks in Western Europe 1970-2019.

Source: own elaboration.

Table 1 and Chart 6 provide information on the ratio of casualties to attacks, hereafter referred to as the casualty ratio, which is a more meaningful indicator than directly comparing data.

Table 1. Comparison of terrorist attack casualty rates by region.

Region	Casualty rate
East Asia	19.6:1
North America	10.7:1
Middle East and North Africa	7.0:1
Sub-Saharan Africa	6.9:1
Central Asia	6.2:1
South Asia	5.0:1
Eastern Europe	4.0:1
South-East Asia	3.0:1
Central America and the Caribbean	2.7:1
South America	2.3:1
Western Europe	1.8:1
Australasia and Oceania	1.7:1

Source: own elaboration.

Chart 6. Number of terrorist attacks and number of victims by region.

Source: own elaboration.

Attacks in the Middle East and North Africa and South Asia - despite the highest absolute numbers - are not the most deadly. The highest casualty

rate occurs in East Asia and almost doubles that of North America, which is in second place. Sub-Saharan Africa is in third place. On average, attacks in Australasia and Oceania and Western Europe have the lowest casualty rate. It is clear from these statistics that, when it comes to terrorism, the divide between the rich north and the poor south does not translate directly. Some of the poorer regions, such as South America, South-East Asia or Central America and the Caribbean, do not have a significantly higher casualty rate than the richer regions. This may indicate non-economic factors that influence the effectiveness of terrorists.

After analysing the data, the ten countries with the highest number of terrorist attacks carried out between 1970 and 2019 (Chart 7) and the 10 countries with the highest number of victims of these attacks (Chart 8) were identified in turn.

These countries (by region[8]) are:

- Middle East and North Africa: Iraq, Yemen, Syria;
- South Asia: Afghanistan, Pakistan, India, Sri Lanka;
- Southeast Asia: Philippines, Thailand;
- South America: Colombia, Peru;
- North America: United States;
- Sub-Saharan Africa: Nigeria.

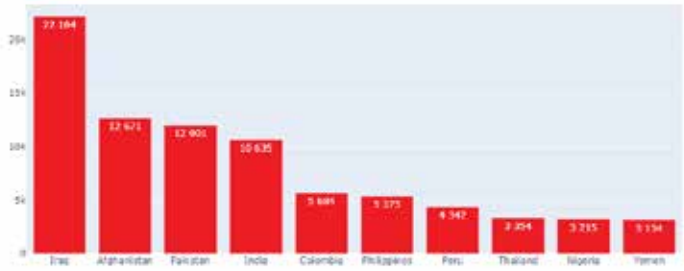


Chart 7. Number of terrorist attacks in countries ranking in the top 10 in terms of number of such attacks.

Source: own elaboration.

[8] Countries are assigned to their regions according to the *Codebook*.

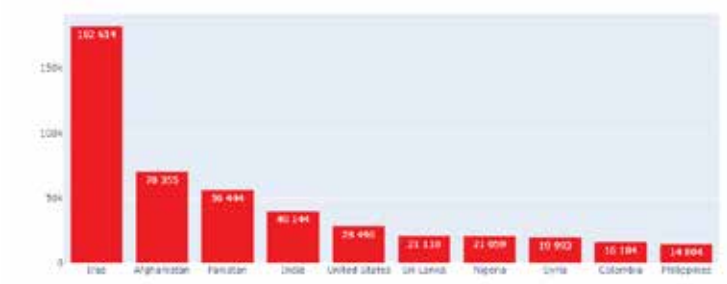


Chart 8. Number of victims of terrorist attacks in countries ranking in the top 10 in terms of such victims.

Source: own elaboration.

Due to the relatively low number of attacks and casualties compared to other countries, no East Asian country is on the list (despite a high casualty rate). Iraq is the most affected, with almost twice as many terrorist attacks as Afghanistan, which translates into more than twice as many victims. The other countries included already have more similar values in terms of both the number of terrorist attacks and the victims of these incidents.

Table 2 indicates the casualty rate for the countries with the highest number of casualties. The highest ratio are 12.8 for Syria, 12.0 for the United States and 11.2 for Sri Lanka. On average, the least number of victims of the attack was in Colombia and the Philippines.

Table 2. Comparison of the casualty rate of terrorist attacks for the 10 countries with the highest number of such casualties.

Country	Casualty rate
Syria	12.8:1
United States	12.0:1
Sri Lanka	11.2:1
Iraq	8.2:1
Nigeria	6.6:1
Afghanistan	5.6:1
Pakistan	4.7:1
India	3.8:1
Columbia	2.8:1
Philippines	2.8:1

Source: own elaboration.

It can therefore be concluded that geographical factors have a bearing on whether or not a terrorist attack will result in casualties. They were therefore taken into account during the modelling and their impact on the prediction result has been analysed.

Activity of selected terrorist groups

An analysis of the activity of the groups responsible for terrorist attacks was then carried out. Chart 9 shows the most active terrorist groups between 1970-2019. The top ten places are occupied by groups linked to Islamic terrorism: Taliban, Al-Shabaab, Boko Haram, Islamic State (ISIS) also known as Islamic State of Iraq and the Levant (ISIL) and far-left terrorism: Basque Fatherland and Freedom (ETA), the New People's Army (NPA), the Revolutionary Armed Forces of Colombia (FARC), the Maoists, Shining Path (Spanish: Sendero Luminoso (SL), Communist Party of India-Maoist (CPI-Maoist). This may indicate some correlation between a group's motivation to carry out an attack and its high level of activity; however, in the GTD, individual groups are not assigned characteristics. This may be a clue for the START consortium researchers to update the GTD in this regard.

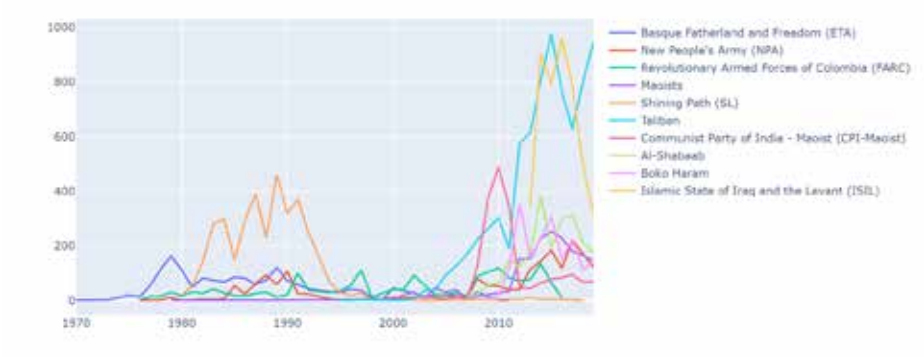


Chart 9. Number of terrorist attacks carried out between 1970 and 2019 by the 10 most active terrorist groups.

Source: own elaboration.

The oldest group of all those mentioned above is ETA, which, during the period under study, was most active between 1970 and 1980 and has been increasingly inactive since the early 1990s. The last recorded attack in the GTD carried out by this group was in 2011. This is most likely related to the end of the organisation's armed activities in October of the same year[9]. ETA finally self-dissolved in 2018[10].

Also active to a fairly high degree was the Shining Path, whose activity was mainly between 1980 and 1990. Thereafter, there was a marked decline in the number of attacks carried out by this group. This was probably due to the arrest of its successive leaders in the 1990s and in 2012[11]. One faction of the Shining Path, the Militarised Communist Party of Peru, which in 2018 splintered from the SL, remained active[12].

Another group whose increased activity occurred in the 1980s is the New People's Army operating in the Philippines. It was formed in 1969 as the armed arm of the Communist Party of the Philippines[13]. The decline in the group's activity after 1990 may be due to the arrest of key figures in the organisation and internal purges[14]. Various ceasefires and negotiations from 1986 and 2010, among others, were broken by the NPA[15]. Another increase in the group's activity has been recorded since 2013. The NPA, unlike the SL and ETA, remains active.

The FARC was founded in 1964. The original aim of the organisation was to overthrow the government of Colombia[16]. Between 2008 and 2015 there was an increase in its terrorist activity. Although the government has attempted to negotiate with the FARC since 2012, including ceasefires,

---

9 *Basque group Eta says armed campaign is over*, BBC News, 20 X 2011, https://www.bbc.com/news/world-europe-15393014 [accessed: 6 VI 2022].

10 I. Binnie, *Basque separatist group ETA says it has "completely dissolved"*, Reuters, 2 V 2018, https://www.reuters.com/article/us-spain-eta-idUSKBN1I31TP [accessed: 6 VI 2022].

11 S. Saffón, *Peru in Familiar Stalemate With Shining Path Rebels*, InSight Crime, 4 IX 2020, https://insightcrime.org/news/brief/peru-stalemate-shining-path/ [accessed: 8 VI 2022].

12 Ibid.

13 *Communist Part of the Philippines – New People's Army*, Stanford University, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/communist-party-philippines-new-peoples-army [accessed: 11 VI 2022].

14 Ibid.

15 Ibid.

16 *Revolutionary Armed Forces of Colombia (FARC)*, Stanford University, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/revolutionary-armed-forces-colombia-farc [accessed: 8 VI 2022].

the group has regularly broken them[17]. In 2016, an agreement was reached between the government and the FARC, which transformed itself into a political party and ceased its armed activities[18]. According to GTD data, not a single attack has been carried out by this organisation since 2016.

The Communist Party of India (Maoist), on the other hand, is a group outlawed by the Indian government[19]. The increase in CPI-Maoist activity in 2009 and its subsequent decline may be linked to "Green Hunt" counter-terrorism operation targeting the organisation[20]. Despite the efforts made, the CPI-Maoist could not be dismantled. The Maoists, in turn, is the collective name for terrorist far-left groups not part of the CPI-Maoist[21].

The Taliban emerged as an organisation in 1994 and ruled Afghanistan from 1996 to 2001[22]. A surge in their activity can be seen after 2001, when they were defeated militarily, but the organisation was not dismantled. The Taliban returned to power in 2021.

Al-Shabab is a Somali-origin organisation operating in East Africa and Yemen. Activity peaked in 2014. However, there was a decline a year later, which can be linked to the killing of one of the organisation's leaders by the US in 2014, a major loss for the group[23]. Despite efforts to combat the organisation by the Somali government and the US, it remains active.

Boko Haram was established in Nigeria in 2002[24] and began its activities as a terrorist organisation in 2009, when a shootout took place between

---

17 Ibid.

18 Ibid.

19 *Left Wing Extremism Division*, Ministry of Home Affairs, https://web.archive.org/web/20220707070953/https://www.mha.gov.in/division_of_mha/left-wing-extremism-division [accessed: 8 VI 2022].

20 A. Sethi, *Green Hunt: the anatomy of an operation*, The Hindu, 6 II 2010, https://www.thehindu.com/opinion/op-ed/Green-Hunt-the-anatomy-of-an-operation/article16812797.ece. [accessed: 8 VI 2022].

21 *Deaths in Maoist attacks down by 21%: Shah at CMs' meeting*, The Times of India, 27 IX 2021, https://timesofindia.indiatimes.com/india/deaths-in-naxal-attacks-down-by-21-shah-at-cms-meeting/articleshow/86543018.cms [accessed: 8 VI 2022].

22 *The Afghan Taliban*, Stanford University, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/afghan-taliban [accessed: 8 VI 2022].

23 *Pentagon confirms death of Somalia terror leader*, The Washington Times, 5 IX 2014, https://www.washingtontimes.com/news/2014/sep/5/pentagon-confirms-death-of-somalia-terror-leader/ [accessed: 10 VI 2022].

24 H. Matfess, *Boko Haram: History and Context*, in: *Oxford Research Encyclopedia of African History*, Oxford University Press 2017, p. 1.

its members and the police[25]. It is difficult to predict trends in the group's activity, as it is influenced by the actions of the authorities in the form of, for example, the use of armed forces, but also by Boko Haram's resilience to these actions[26].

The last group discussed is the Islamic State. Originally founded in 1999 under the name Jama'at al-Tawhid wal-Jihad, the organisation was renamed Al-Qaeda in Iraq after the US intervention in Iraq[27]. The group was strengthened after the American withdrawal from Iraq. Taking advantage of this fact and the outbreak of civil war in Syria, it began successively taking over areas of both countries in 2013 and 2014[28]. During this period, the organisation changed its name first to Islamic State in Iraq and Syria, then in June 2014 it announced the creation of a caliphate and finally adopted the name Islamic State[29]. The dynamics of change in the group's activity are clearly linked to its progress in taking over the territories of the above-mentioned countries. It reached its peak in 2014 and was highly active until 2017, at times surpassing the Taliban. The apparent decline in activity in 2018 and 2019 is most likely linked to the group's loss of most territories. In 2017, ISIS was pushed out of the urban centres it controlled, and two years later the organisation lost control of its last territories in Baghuz province in Syria[30]. With the loss of territories, and thus the means to conduct operations, ISIS activity has gradually decreased. There is a clear downward trend in this respect, but despite the efforts of Kurdish, Iraqi and Syrian forces or the involvement of the US army, the group remains active.

It is noteworthy that all of the most active groups, despite the various actions and measures taken, continue to be active, excluding those that have self-dissolved as a result of the negotiations undertaken with these groups by their respective governments.

A casualty rate was calculated for the most active terrorist groups. It is shown in Table 3.

[25] Ibid, p. 7.

[26] Ibid, p. 15.

[27] *The Islamic State*, Stanford University, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/islamic-state [accessed: 11 VI 2022].

[28] Ibid.

[29] Ibid.

[30] Ibid.

Table 3. Casualty rates for the most active terrorist groups.

Terrorist group	Casualty rate
Islamic State	11.0:1
Boko Haram	10.0:1
Al-Shabab	5.8:1
Taliban	5.8:1
Revolutionary Armed Forces of Colombia	3.6:1
Shining Path	2.7:1
Communist Party of India (Maoist)	1.9:1
New People's Army	1.8:1
Basque Country and Freedom	1.6:1
Maoists	1.4:1

Source: own elaboration.

It can be seen that the casualty rate for Islamist groups is significantly higher than for far-left groups. This could be another argument for adding a new feature to the dataset - indicating the religious or political affiliation of the group in question and exploring this further. This could have a positive impact on the improvement of machine learning models for the prediction of victims of terrorist attacks.

Most common targets of terrorist attacks

The characteristics of terrorist attacks including their targets and types were then visualised. Chart 10 shows the most common targets of terrorist attacks carried out between 1970 and 2019, which were, in order: civilians and property, police, government institutions (general), business, public transport, energy infrastructure, military, religious leaders or religious institutions, schools, government institutions (diplomats).

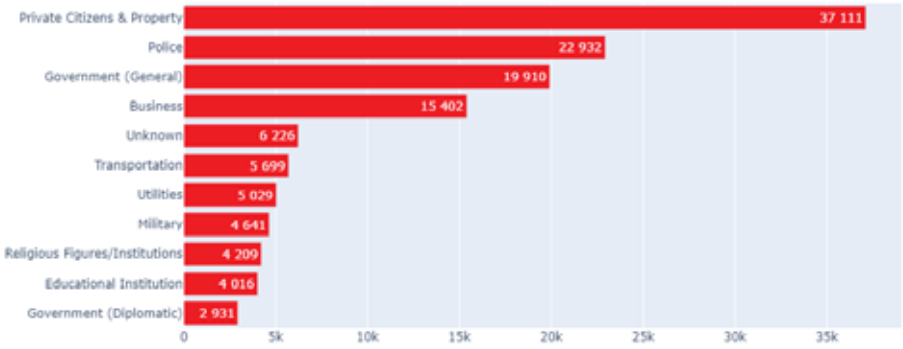


Chart 10. Most frequent targets of terrorist attacks by number of attacks carried out against them.

Source: own elaboration.

A high number of attacks targeting civilians and property may reflect a desire to intimidate public opinion in a country and thus influence the actions of its government. Conversely, attacks on the police, the military or government institutions, may reflect the frequent political motivation of terrorist groups that regard state authorities as an enemy to be fought. Attacks on the private sector in the broadest sense, carried out for example by the FARC, may indicate the extreme left-wing motivations of such groups, whose aim in the longer term may be to bring about the abolition of private property.

Types of terrorist attacks

It also examined which type of terrorist attack was carried out most frequently (Chart 11). A regional breakdown was made, which allowed the specifics of attacks carried out in different parts of the world to become more apparent.

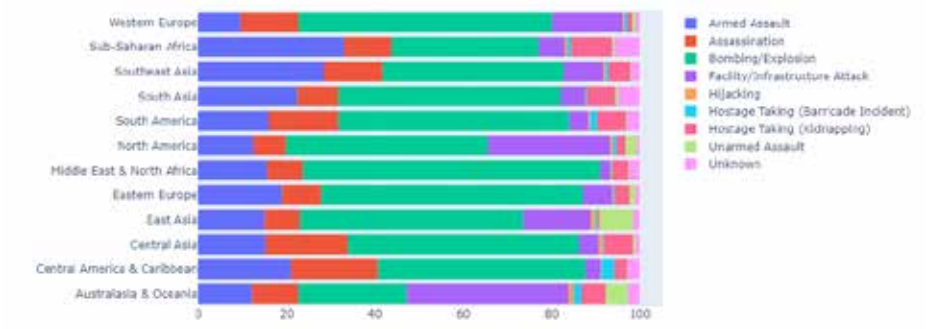


Chart 11. Percentage of different types of terrorist attacks by region.

Source: own elaboration.

Attacks using explosives accounted for the largest proportion in all regions surveyed, excluding Australasia and Oceania. In addition, armed robbery and homicide and, in some regions, attacks on infrastructure were common. This can provide an indication to state governments as to what type of attack state institutions should be prepared for. They can then review whether the services competent to deal with the terrorist threat have developed adequate procedures for the type of event, and whether the health services will be efficient enough to effectively care for the injured (this could reduce the number of fatalities). Such an evaluation of the current capacities of state institutions would indicate certain gaps in resilience to these types of events.

Data processing

In the next step, data processing was carried out. First, the final variables used for modelling were selected. These are presented in Table 4.

Table 4. Description of variables used in the survey.

Variable name	Variable description
Extended	determines whether the duration of the incident exceeded 24 hours
Country_txt	identifies the country in which the event occurred
Region	identifies the region in which the event occurred

Latitude	determines the latitude of the place where the event occurred
Longitude	determines the longitude of the place where the event occurred
Specificity	defines the geospatial resolution of the latitude and longitude fields. The most detailed resolution available across the dataset is the centre of the city, village or town where the attack occurred. Higher resolution coordinates, although possible, are not systematically included in the database
Vicinity	determines whether the event occurred in the immediate vicinity of the city concerned
Multiple	determines whether a terrorist attack is linked to other attacks
Success	the success of a terrorist attack is defined by its tangible effects. Success is not assessed in terms of the perpetrators' broader goals. For example, a bomb that exploded in a building would be considered a success even if it did not succeed in destroying the building or provoking government retaliation
Suicide	determines whether an attack was a suicide bombing
Attack type1	identifies the type of terrorist attack
Targ type1	identifies the type of terrorist target
Targ subtype1	defines the objective category in more detail
Natlty1	is the nationality of the target attacked, not necessarily the same as the country in which the incident occurred, although in most cases this is the case. In the case of aircraft hijacking, the nationality of the aircraft is recorded, not the nationality of the passengers
Gname	includes the name of the group that carried out the attack
Guncertain1	determines whether information provided by sources about the group responsible for the attack is based on speculation or questionable claims of responsibility
Individual	determines whether the attack was carried out by a person or several persons not known to be associated with a terrorist group or organisation

Nperps	determines the total number of terrorists involved in the incident
Claimed	is used to indicate whether a group or individual(s) has admitted to an attack
Weaptype1	identifies the type of weapon used
Weapsubtype1	defines the category of weapons in more detail
Property	determine whether property has been damaged as a result of the incident
Ishostkid	determines whether the victims were taken hostage or abducted during the incident
Int_log	indicates whether, in order to carry out the attack, the group of perpetrators crossed the border
Int_misc	indicates whether the group of perpetrators attacked a target of a different nationality
Int_any	determines whether all conditions for variables with the prefix *int* are met
Cas_class	determines whether an incident has caused casualties

Source: own elaboration based on: Codebook: Inclusion Criteria and Variables, Global Terrorism Database, August 2018, http://www.start-dev.umd.edu/gtd/downloads/Codebook.pdf [accessed: 30 V 2022].

This reduced the number of columns from 60 to 28. Constraint the number of features will speed up the training process for the machine learning models. Due to the fact that some of the columns are in numeric or text form such as *region* and *region_txt,* it was decided to select only one column in such a case, in order to simplify the dataset. Columns containing metadata such as the unique event identifier or the original data source were also removed. Variables specifying the conditions for the inclusion of an event in the GTD were not taken into account because, as already mentioned, those attacks that did not meet all the conditions and those for which there was doubt were filtered out. Thus, these variables do not carry meaningful information for the machine learning models to influence prediction, and would only prolong the training process. The last group of features removed are variables that specify the number of victims or injured in order to avoid data leakage, which would have made the results of the study unreliable.

The number of terrorist attacks that ended in casualties was then examined. About 59 per cent of cases resulted in at least one non-terrorist being killed or injured. This means that there is an imbalance of classes in the predicted variable, which can negatively affect the prediction result. This problem was addressed when building the machine learning models by setting the *class weight* parameter to a *balanced* value. This allows the models to pay more attention to the lesser class, which helps to balance the impact of each class on the model, increasing the overall prediction performance.

A further split was made into a training set (80 per cent of the data) and a test set (the remaining 20 per cent). Stratified sampling was used to ensure that the classes of the predicted variable were similarly distributed throughout the dataset.

In the next step, a pipeline was created performing the final transformations on the dataset.

The first step is to transform the *country_txt* and *gname* variables from textual to numeric form, as the machine learning models built can only work on data in this form. Due to the large number of unique values in both columns, it was decided to code them based on the number of occurrences. This method - as opposed to the 1-of-n (one-hot encoding) method, which results in as many columns as there are unique values - does not have the side-effect of increasing the dimensionality of the data.

The blank values were then replaced with -9. This is how the GTD codes values for which the researchers did not have sufficient information to explicitly assign a specific value to an event characteristic[31].

In the final step, the data was normalised due to the fact that some of the models built, such as logistic regression and support vector machines, are sensitive to extremely different value scales. This method solves this problem and can translate into better performance of these models and speed up the learning process.

It is worth pointing out that the calculation of the number of occurrences of a given value should only take place on the training set. On the test set, on the other hand, transformations are made on the basis of calculations from the training set. This is an important point, because a different procedure leads to data leakage and thus affects the test results. For this reason, it was decided to use the pipeline available in the Scikit-

[31] *History of the GTD...*

learn library, which makes it easy to control the transformation steps and thus reduce the risk of error (Figure 4).

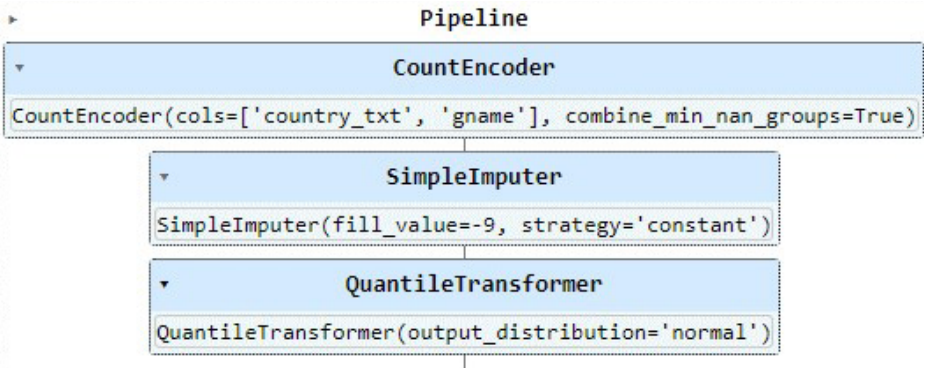


Figure 4. Pipeline performing transformations on a data set.

Source: own elaboration.

At the end of the processing stage, the training and test sets were saved to separate files in order to save the transformations carried out and to be able to proceed directly to modelling afterwards.

The process of training machine learning models

All models were trained on a desktop computer with parameters: 16 GB RAM, AMD Ryzen 5 3600 processor. Each model was trained in an analogous way: hyperparameters were queried using the Optuna framework, and metrics were written using the MLFlow library. To avoid unnecessary repetition, the training process will only be shown using the decision tree as an example (Figure 5).

```
def objective(trial):
    params = {
        "max_depth": trial.suggest_int("max_depth", 15, 50),
        "min_samples_leaf": trial.suggest_int("min_samples_leaf", 1, 40),
        "class_weight": trial.suggest_categorical("class_weight", ["balanced"]),
        "criterion": trial.suggest_categorical("criterion", ["gini", "entropy"])
    }

    model = DecisionTreeClassifier(**params)

    scoring = ["accuracy", "precision", "recall", "f1"]

    preds = cross_validate(model, X_train, y_train, cv=5, n_jobs=-1, scoring=scoring)

    accuracy = np.mean(preds["test_accuracy"])
    precision = np.mean(preds["test_precision"])
    recall = np.mean(preds["test_recall"])
    f1 = np.mean(preds["test_f1"])

    return accuracy, precision, recall, f1
```

Figure 5. Code fragment responsible for searching for hyperparameters.

Source: own elaboration.

The first line defines a function whose name and accepted arguments follow the convention adopted in Optun. In lines 2-7, the space of hyperparameters was defined, which in a later stage was searched to find the best possible combination of them. In the case of lines 2-3, the interval in which the values of these hyperparameters are to be searched was marked and in this case it will be an integer. Particularly noteworthy is line 5, which indicates that the class weight should be balanced. This is one of the methods to solve the previously mentioned problem of unbalanced classes. This was followed by the initialisation of the model on line 9, and then the metrics used to evaluate the models were specified, namely accuracy, precision, recall and F1. These will be discussed in detail further on in the article. In line 13, the model is trained on the training set using cross validation, and then the scores for the individual variables are calculated, which are finally returned by this function.

In the next step, a so-called *study* was created, in which its name and the direction of optimisation of the metrics are specified. As the metrics used relate to the classification problem, they have been maximised. This is followed by a search of the hyperparameters (Figure 6), which are stored using MLFlow (Figure 7).

```
study = optuna.create_study(study_name="decision_tree",
                            directions=["maximize", "maximize", "maximize", "maximize"])
study.optimize(objective, n_trials=100, callbacks=[mlflow_callback])
```

Figure 6. Initialisation of hyperparameter searches by Optuna.

Source: own elaboration.

	Metrics				Parameters				
	accuracy	f1	precision	recall	criterion	max_depth	max_features	min_samples_le	min_samples_sp
	0.849	0.868	0.892	0.845	entropy	21	-	38	-
	0.848	0.868	0.887	0.849	entropy	37	-	15	-
	0.848	0.868	0.89	0.846	entropy	33	None	20	82
	0.848	0.867	0.888	0.848	entropy	25	-	17	-
	0.848	0.867	0.89	0.846	entropy	18	None	34	31
	0.848	0.867	0.89	0.846	entropy	18	None	34	31

Figure 7. Excerpt from the MLFlow dashboard with stored metrics and decision tree parameters.

Source: own elaboration.

For each model, several hundred iterations were performed to search for the optimal hyperparameters. All models with the optimal hyperparameters for them were then trained on the entire training set and validated on the test set. Those models that achieved the highest values of the F1 metric were selected for training. The parameters of these models and their results will be presented later. The individual quality metrics of the classification models used during the study are described earlier.

Selected quality measures of classification models

Due to the multitude of different quality measures used in the evaluation of classification models, only those measures used during the study are described.

The accuracy of a classifier is a measure of how many cases are classified correctly[32]. It can be represented by the following formula:

[32] S. Raschka et al., *Machine Learning with PyTorch and Scikit-Learn: Develop machine learning and deep learning models with Python*, Birmingham 2022, p. 13.

$$\text{accuracy} = \frac{TP + TN}{FP + FN + TP + TN}$$

where:

- TP (true positive), where the model has correctly classified an event as causing casualties;
- TN (true negative) cases, where the model has correctly classified an event as not causing casualties;
- FP (false positive) cases, where the model has incorrectly classified an event as causing casualties;
- FN (false negative) cases, where the model has incorrectly classified an event as not causing casualties[33].

Two further measures, precision and recall, are directly related. Precision promotes a situation in which the classifier is confident in its decisions and makes as few false-positive errors as possible, but at the cost of this is an increase in false-negative predictions[34]. The opposite is true with regard to recall, since the situation is promoted in which the classifier makes as few false-negative errors as possible, but at the expense of increasing false-positive cases[35]. Thus, if we optimise the classifier so that it minimises the chances of incorrectly classifying an event as a non-victory, it will have high recall. The formula of recall is as follows:

$$\text{recall} = \frac{TP}{FN + TP}$$

However, this will come at the expense of precision. The formula of precision is as follows:

$$\text{precision} = \frac{TP}{TP + FP}$$

[33] Ibid, p. 195.

[34] Ibid, p. 196.

[35] Ibid.

In order to balance precision and sensitivity, the F1 measure is used, which is the harmonic mean of precision and recall[36]. This means that in order to achieve a high F1 measure, the classifier must have high scores in both precision and sensitivity, as the harmonic mean attaches more importance to low values[37].

$$F1 = 2\,\frac{\text{precision} \times \text{recall}}{\text{precision} + \text{recall}}$$

Test results for individual models

In Tables 5–8 the hyperparameters for each machine learning model are indicated. Table 9 presents the results of their validation on the test set. It should be noted that only those hyperparameter values that were previously searched for are shown. If a hyperparameter is not in the table, it means that it takes a default value according to the documentation of the relevant library. Since the voting classifier and the stacked classifier are composed of other built models, their hyperparameters are identical to those shown in tables.

Table 5. Hyperparameter values for logistic regression.

Hyperparameter name	Value
C	9.58649376280703
class_weight	balanced
max_iter	500

Source: own elaboration.

Table 6. Hyperparameter values for a linear support vector machine.

Hyperparameter name	Value
C	0.0036775852394361204

[36] A. Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*, Sebastopol 2019, p. 140.

[37] Ibid.

class_weight	balanced
dual	false
penalty	L1

Source: own elaboration.

Table 7. Hyperparameter values for the decision tree.

Hyperparameter name	Value
criterion	entropy
class_weight	balanced
max_depth	21
min_samples_leaf	38

Source: own elaboration.

Table 8. Hyperparameter values for the random forest.

Hyperparameter name	Value
criterion	entropy
class_weight	balanced
max_depth	42
min_samples_split	6
n_estimators	551
max_features	sqrt

Source: own elaboration.

Table 9. Hyperparameter values for the XGBoost model.

Hyperparameter name	Value
colsample_bylevel	0.6783261477402747
colsample_bytree	0.23127225599162296
gamma	0.4906870500968865
learning_rate	0.0675784773135259
max_delta_step	5
max_depth	22
min_child_weight	1
n_estimators	1475

reg_alpha	0.12263684424466229
reg_lambda	1.9559489540115411
scale_pos_weight	0.9676022078596858
subsample	0.976706655475712

Source: own elaboration.

Table 10 shows the results of each model along with their training times. The best results from each category are shown in bold.

Table 10. Results of individual machine learning models.

Model name	Training duration	Accuracy	Precision	Sensitivity	F1
Logistic regression	2.8 s	0.765	0.823	0.762	0.792
Support vector machines	10.4 s	0.765	0.824	0.763	0.792
Decision tree	**1.0 s**	0.845	0.894	0.835	0.864
Random forest	1.3 min	0.876	0.891	0.898	0.895
XGBoost	1.4 min	**0.879**	0.890	**0.905**	**0.898**
Voting classifier	3.6 min	0.870	0.888	0.891	0.889
Stacked classifier	7.8 min	**0.879**	**0.904**	0.889	0.896

Source: own elaboration.

The best model in terms of quality measure values is XGBoost. Evidently inferior results were achieved by linear models, namely logistic regression and support vector machines. It is therefore probably better to focus on tree models in further research. It is worth noting that the difference in performance between XGBoost and the stacked classifier is small, however, XGBoost's training time is more than five times shorter. Such results suggest that further research should focus on tree-based models based on gradient enhancement.

No model has managed to exceed the 90 per cent performance threshold on the F1 metric, despite many iterations when looking for hyperparameters. It is likely that an expansion of the dataset with new variables, such as the political/religious affiliation of the terrorist group in question, the incidence of ethnic/political/religious tensions in the country, the distance of the incident site from the nearest hospital, would be needed to achieve results of around 95 per cent.

It was also decided to calculate the feature importance for the model based on the XGBoost library, in order to determine which features were most relevant to the model when making the prediction. This is presented in Chart 12, in which the y-axis shows the features described earlier and the x-axis shows the value of the feature for the prediction. The most important features were targets and weapon subtype. When evaluating contingency plans for a terrorist attack, these two factors should be considered particularly carefully. A set of geographical factors, such as region or longitude and latitude, for example, indicate that terrorism is a problem for some areas of the world and has different characteristics.

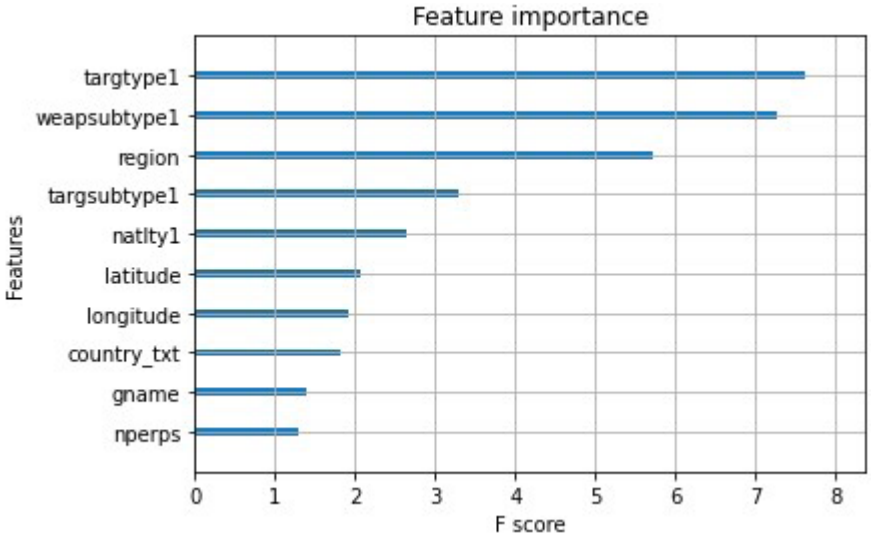


Chart 12. Key features for the XGBoost model.

Source: own elaboration.

Conclusions

A study of terrorist attacks occurring between 1970 and 2019 was conducted, including an in-depth analysis of trends in the activity of selected terrorist groups. The collaborative models built performed significantly better than linear models.

The results indicate that future focus should be on models based on collaborative learning, as linear models, such as logistic regression, performed noticeably worse. In particular, tree-based models based on gradient reinforcement should be looked at, as XGBoost achieved better results with shorter training times compared to the voting classifier and the stacked classifier. Further considerations could also investigate the effectiveness of models similar to XGBoost, such as CatBoost, LightGBM, or see how deep neural networks would handle such a task.

When the START consortium researchers publish the full data for 2020-2021, it would be worthwhile to analyse whether terrorist activity has changed, and to characterise their activities during the COVID-19 pandemic. Also, supplementing the GTD with new variables, such as, for example, information on ethnic or religious tensions, the economic condition of a country, or the religious or political affiliation of a given terrorist group, could positively influence the classification results, including helping to surpass the 90 per cent barrier.

This article shows that it is possible to use machine learning effectively in the field of security. This can assist the relevant authorities in developing crisis management plans in the event of a terrorist incident. The state can also take educational measures in the form of information campaigns or teaching in schools how to behave during a terrorist attack depending on the type of attack. As shown through the significance values of the variables, it was the target of the attack that was the most important factor for the XGBoost model, and as indicated earlier, civilians are most often attacked. With educational measures it would probably be possible to reduce the number of victims of terrorist attacks to some extent. The second most important factor turned out to be the subtype of weapons, so that after an in-depth analysis by the relevant services of the means used by particular terrorist groups in a given area, new regulations could be developed to make it more difficult for terrorists to obtain weapons.

Bibliography

Géron A., *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*, Sebastopol 2019.

Matfess H., *Boko Haram: History and Context*, in: *Oxford Research Encyclopedia of African History*, Oxford University Press 2017.

Raschka S. et al., *Machine Learning with PyTorch and Scikit-Learn: Develop machine learning and deep learning models with Python*, Birmingham 2022.

Internet sources

Basque group Eta says armed campaign is over, BBC News, 20 X 2011, https://www.bbc.com/news/world-europe-15393014 [accessed: 6 VI 2022].

Binnie I., *Basque separatist group ETA says it has "completely dissolved"*, Reuters, 2 V 2018, https://www.reuters.com/article/us-spain-eta-idUSKBN1I31TP [accessed: 6 VI 2022].

Codebook: Inclusion Criteria and Variables, Global Terrorism Database, August 2018, https://www.start.umd.edu/gtd/downloads/Codebook.pdf/ [accessed: 30 V 2022].

Communist Part of the Philippines – New People's Army, Stanford University, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/communist-party-philippines-new-peoples-army [accessed: 11 VI 2022].

Data Collection Methodology, Global Terrorism Database, http://www.start-dev.umd.edu/gtd/using-gtd/ [accessed: 21 V 2022].

Deaths in Maoist attacks down by 21%: Shah at CMs' meeting, The Times of India, 27 IX 2021, https://timesofindia.indiatimes.com/india/deaths-in-naxal-attacks-down-by-21-shah-at-cms-meeting/articleshow/86543018.cms [accessed: 8 VI 2022].

History of the GTD, Global Terrorism Database, https://start.umd.edu/gtd/about/History.aspx [accessed: 11 V 2022].

Left Wing Extremism Division, Ministry of Home Affairs, https://web.archive.org/web/20220707070953/https://www.mha.gov.in/division_of_mha/left-wing-extremism-division [accessed: 8 VI 2022].

Pentagon confirms death of Somalia terror leader, The Washington Times, 5 IX 2014, https://www.washingtontimes.com/news/2014/sep/5/pentagon-confirms-death-of-somalia-terror-leader/ [accessed: 10 VI 2022].

Revolutionary Armed Forces of Colombia (FARC), Stanford University, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/revolutionary-armed-forces-colombia-farc [accessed: 8 VI 2022].

Saffón S., *Peru in Familiar Stalemate With Shining Path Rebels*, InSight Crime, 4 IX 2020, https://insightcrime.org/news/brief/peru-stalemate-shining-path/ [accessed: 8 VI 2022].

Sethi A., *Green Hunt: the anatomy of an operation*, The Hindu, 6 II 2010, https://www.thehindu.com/opinion/op-ed/Green-Hunt-the-anatomy-of-an-operation/article16812797.ece [accessed: 8 VI 2022].

The Afghan Taliban, Stanford University, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/afghan-taliban [accessed: 8 VI 2022].

The Islamic State, Stanford University, https://cisac.fsi.stanford.edu/mappingmilitants/profiles/islamic-state [accessed: 11 VI 2022].

Jakub Tuszyński

University of Warsaw graduate with a master's degree in Big Data Management.

OTHER

https://doi.org/10.4467/27204383TER.23.036.18338
https://orcid.org/0009-0005-0658-0901

Counter-intelligence in anti-terrorist operations

Essay on relations

Tomasz Białek

Game

Many years ago, during a lecture on the sociology of internal security, I was asked by students to answer the question: what are the special services? This apparent attempt by the sociology students to systematise their knowledge provoked a lively discussion. I asked them to try to provide an answer themselves. All the definitions turned out to be more or less accurate. Almost every time, the word "secret" or a synonym thereof - "classified" - appeared. The most difficult part was trying to include operational activities (which, unlike the special services, are after all described in detail in legislation) in the definition, as the sheer number of services with powers to do so is impressive. I remembered an interesting statement that "special" are such services as the Central Anti-Corruption Bureau or the State Protection Service, because (note!) they "specialise" in fighting corruption or protecting the authorities. Another definition does not mention services with investigative powers (Central Anti-Corruption Bureau, Internal Security Agency). The argument? *Because they are simply police services*. However, the most interesting thing in one definition was

the exclusion of the Foreign Intelligence Agency, the Military Intelligence Service and the Military Counterintelligence Service from the catalogue of special services. It has been argued that these are not special services, but intelligence services (this point of view is also prevalent in the literature[1]).

Just when it seemed that the group was reaching an agreement on a definition, someone questioned one of the elements of the proposal under discussion. The more inquisitive looked for other meanings of the words making up the definition, and those with better scientific skills wondered whether it could not also be applied to other elements of the state security system and beyond. One student asked: *Why only states? And can't a criminal organisation or a large corporation have its own secret service?* The final result of the work did not fully satisfy everyone, but for all that, everyone learned and understood what special services are.

Over the years, I have encouraged this game for both students at universities and officers in training. The discussion has always gone the same way and ended with the same conundrums. For fortunately, there are equally wise definitions in wise textbooks by wise professionals, which wise lecturers demand from wise (!) listeners.

Signboard

The history of secret, special, intelligence and similar services is as old as the history of the organisation of people into close-knit social groups. Historians, however, find it difficult to reconstruct the process of formation and operation of such services in ancient Egypt, the Roman or Macedonian Empires, or in Poland in the times of the Piasts or Jagiellons. This is probably because, for example, the noble Chancellor Mikołaj Trąba, the right hand of King Władysław Jagiełło, when he set up intelligence services, did not give them such names as the Crown Intelligence Agency, the Excellent Royal Counterintelligence Service or the Bureau for Exceptional and Special Monarchial Tasks. Instead, in the twentieth century, services of all kinds entered the heyday of signboards. Agencies, services, bureaus. Intelligence, counterintelligence, security. Special, exceptional,

[1] See: R. Faligot, R. Kauffer, *Służby specjalne. Historia wywiadu i kontrwywiadu na świecie* (Eng. Special Services. A history of intelligence and counterintelligence in the world), Warszawa 2006; Z. Siemiątkowski, A. Zięba, *Służby specjalne we współczesnym państwie*, (Special services in the modern state), Warszawa 2016.

extraordinate. Nowadays, it takes longer to come up with a good name and logo than it does to draft a piece of legislation creating a service. And there are countless services.

In many countries, colleges of services - like professional parliaments - are being set up with marshals as coordinators at a very high level. It has come to the point where heads of service make foreign visits and hold talks, sometimes bypassing foreign ministers. The change of service chief is a news event and by the time he enters his office for the first time, his CV can already be seen in the media. The secret services are no longer secret, but mainstream. Gone are the days when, for example, an "office supplies warehouse manager" would enter a discreet meeting with a head of state through the back door and provide reliable intelligence.

Basis for operation

Let us consider further (absolutely not of a definitional nature!) that the essence of special services is specialised or operational activities focused on a specific phenomenon (e.g. Central Anti-Corruption Bureau, State Protection Service), and the essence of intelligence services is the acquisition of information and exerting influence in a covert manner (e.g. Foreign Intelligence Agency, Military Intelligence Service, Internal Security Agency, Military Counterintelligence Service). Therefore, the question should be asked, where to place anti-terrorist activities in this system? Unfortunately, there is no clear answer to this question, and it is related to two elements. The first is the strategic objective that the state sets for itself in relation to anti-terrorist activities, and the second is the main location of the anti-terrorist division. If the state's strategic objective is to arrest members of a terrorist group and the operations are concentrated in the police, then of course the anti-terrorist division will be a police service. If the state's strategic objective is to take control of a terrorist group and activities are concentrated in counter-intelligence, then the anti-terrorist division will be an intelligence service. If, on the other hand, the strategic objective is to dismantle a terrorist group and activities are concentrated in a separate service dedicated to this task, the anti-terrorist division will be a special service.

Does such an assignment matter? From the perspective of scientific and journalistic studies[2] it certainly does, but in terms of the direct execution of tasks it is not an issue that would preoccupy the minds of officers and soldiers of anti-terrorist divisions.

Relations

Anti-terrorist divisions often have their roots in counter-intelligence divisions, and in some countries they are still located there. In other models, the burden of performing tasks in this area falls mainly on the shoulders of the police services. In both cases, each service has something to say about terrorist threats. Accordingly, coordination points, such as the Counter-Terrorism Centre of the Internal Security Agency, have been established over the years. Analysing the solutions adopted (here, the extensive analyses available, among others, in the journal "Terrorism - studies, analyses, prevention"), one may be tempted to make the banal but correct statement that the measure that determines the best solution is its effectiveness. Attempts to implement any of the external models in one's own backyard may prove to be flawed, as it is above all the appropriateness of the solutions to the system in place that can produce results.

Let us return to the relationship between the anti-terrorist division and the counter-intelligence division. It should be noted that the forms and methods of action developed in counter-intelligence in the counter-terrorist division had to be modified. Although they have elements in common, their actions are determined by the nature of the threats that each division has to face and, above all, by the objective guiding them. For example, terrorist activities always aim to culminate in an attack, while espionage activities generally do not have a climax. Therefore, in the counter-intelligence division, the so-called race against time is an occasional occurrence, but it is a permanent feature of work in the anti-terrorist division. The latter will aim to dismantle the group in order to prevent an attack, while the counter-intelligence division will want to use the identified group for disinformation for as long as possible. Such examples could of course be multiplied, but this one is particularly illustrative.

[2] See. S. Sabataj, *Byłem szefem Mosadu* (Eng. I was the head of Mossad), Wrocław 2020; *Dwie dekady walki z terroryzmem* (Eng. Two decades of fighting terrorism), P. Piasecka, K. Maniszewska, R. Borkowski (sci. eds.), Warszawa 2022.

Cooperation between the divisions seems indispensable, but is it frequent? The counter-intelligence division primarily fights attempts to influence, and the anti-terrorist division fights attempts to subvert. So they have different motives and operate in different environments, which makes them not at all drawn towards each other. Unless there is a situation where foreign intelligence services support or even create a terrorist group. Then there is undoubtedly scope for cooperation between the verticals, although this may be difficult due to the divergence of objectives.

By definition, the counter-intelligence division's adversary is another state, the anti-terrorist division's adversary is a terrorist group. This has a huge impact on the range of consequences of their actions. The consequences of the counter-intelligence division's actions are always international, while the consequences of the anti-terrorist division's actions are mainly related to the internal security of the state.

Another issue is the initiation of the detection process. The counter-intelligence division focuses on information access points and decision-making centres, places that are particularly vulnerable to espionage activity. This includes people with access to information, key decision-makers, institutions relevant to the decision-making process, government, parliament, ministries, business people. The anti-terrorist division, on the other hand, focuses on direct access to objects of importance. The problem is that this will occasionally involve critical infrastructure, rarely state facilities, and most often soft, public targets. Unlike the anti-terrorist division, counter-intelligence always knows where to look.

An essential part of the work of both divisions is analytics, but this is of a different nature for each. The counter-intelligence division focuses on analysing what has already happened and why it happened, while the anti-terrorist division focuses on what, where and how it might happen. While in the former case the analysis of the consequences of events and how they can be exploited is most important, in the latter the analysis is about the potential damage to be prevented.

Case I – Germany

In 2020, it was revealed in Hesse that the authors of threatening letters to politicians supporting a liberal approach to the refugee issue were people with access to police archives. The letters were signed "NSU 2.0", a reference

to a German far-right terrorist group called Nationalsozialistischer Untergrund (NSU), which was active between 2000 and 2011. The group carried out ten racially motivated murders and numerous bomb attacks that left many people seriously injured. The victims were immigrants living in Germany.

During the same period, as a result of internal police action in North Rhine-Westphalia, a group of around 30 police officers active on Nazi internet forums were unmasked and, in addition, many items associated with Nazi symbolism were found in their possession. Similar situations occurred in Mecklenburg-Vorpommern, Saxony-Anhalt and Saxony[3].

In 2020, an entire company in the Bundeswehr's elite anti-terrorist unit called Kommando Spezialkräfte (KSK) was also disbanded for, among other things, displaying fascist salutes. The number of cases of ideologically influenced individuals in this unit was several times higher than in other units of the German army[4].

It was estimated that in 2020 there were around 600 soldiers in the Bundeswehr who were supporters of the organisation Reichsbürger (Reich Citizens), which denied the existence of the Federal Republic of Germany and its organs. They openly threatened acts of terror. Their views were based on right-wing extremism, racism and anti-Semitism[5]. The movement had around 20,000 supporters within Germany (!). In 2020, its activities were outlawed. Between 2016 and 2021, more than 1,000 gun ownership permits were revoked for members and former members of the organisation. Around 1,200 of them were classified as right-wing extremists.

The subject of the Reich Citizens organisation resurfaced when, on 7 December 2022, more than 25 people were arrested in Germany as part of a large-scale anti-terrorist operation. Most of the detainees were linked to the organisation. They planned to overthrow the existing state order and seize power by means of a coup d'état. To begin with, they intended to capture the Reichstag and Bundestag parliamentary centres and sabotage

---

[3] *Ein Beamter machte stehend auf zwei Dienstwagen den Hitlergruß* (Eng. A civil servant made the Hitler salute while standing on two official cars), "Die Welt", 30 XII 2020.

[4] *Hitlergruß und fliegende Schweineköpfe* (Eng. Hitler salute and flying pig heads), "Die Zeit", 17 VI 2017.

[5] K. Benhold, *Germany Disbands Special Forces Group Tainted by Far-Right Extremists*, "The New York Times", 1 VII 2020.

the power grids. The new authorities were to be led by Prince Heinrich XIII Reuss.

The conspiracy involved representatives from various walks of life, including from the world of politics, the media and business[6]. Also in this case, several Bundeswehr soldiers were detained, including again commandos from the special unit KSK[7]. Arrests were made in Baden-Württemberg, Bavaria, Hesse, Lower Saxony, Saxony, Thuringia and Berlin. Facilities in Brandenburg, North Rhine-Westphalia, Rhineland-Palatinate and Saarland were also searched. These included more than 140 flats, offices, warehouses and the barracks of the special forces command in Calw, Baden-Württemberg. The suspects had amassed weapons, explosives and considerable cash.

Commentary

Every citizen has the right to his or her own opinions. However, he cannot break the law in connection with them, especially an officer and a soldier. It is obvious! The service also makes much higher demands in this respect. There is a limit to this freedom of thought that is difficult to accept if crossed, and that is the promotion of fascism. This ideology has not only been completely discredited, it has also been banned by law, which is not often the case with ideologies as such. As such, the situation (especially as it relates to Germany) is of considerable concern and gives food for thought in the context of similar threats, which can, after all, emerge in the services of other countries and go undetected for a long time. What has happened and is happening in this regard in Germany should be a warning that other services, also in Poland, should take advantage of. Of course, this is not limited to fascism. Racism, communism, radical religious movements or homophobia or simple partisanship, for example, can be just as dangerous. In a "healthy" service there is only room for the state, the law and honesty. It is obvious! Just that and that much.

No service functions outside society. Social, political, economic and ideological tensions are always more or less reflected within the security system, or rather among the people who make it up. Of course, the smaller

[6] *Gefährliche Mischung* (Eng. Dangerous mixture), "Tagesschau", 8 XII 2022.

[7] Ibid.

the scale of this phenomenon, the better, but it would be a bad thing if it did not occur at all. The people who make up the system - officers, soldiers, civil servants - are not allowed, because of their views, to take actions aimed at illegally interfering with the state system they guard. Nor do they have the right to serve any party or ideology.

The dissolution by the Germans of part of an elite special unit is not enough. Any service where the influence of ideology appears should be completely disbanded, because this means that for years no one has recognised the threat or, worse, identified it but failed to react. In both cases, this is embarrassing for the service. A unit like KSK loses its unwritten status of "elitism" immediately after such an incident and forever.

But what if this problem concerns police structures? Neither the police nor the army can be disbanded in any country. However, it is necessary to build up their structures and personnel resources with the greatest care. At present, it is easier, for example, to punish a police officer for breaking traffic rules than for promoting a discredited ideology or homophobic or racist behaviour. This does not bode well.

Protection of classified information

The internal security of the services and the related counter-intelligence activities are often controversial and are also negatively perceived by the officers themselves. Few people like to have someone looking at their hands while they are working. However, this must not have any impact on the execution of tasks - internal counter-intelligence activities are a necessity and an indispensable part of threat prevention. The appearance in the service of persons susceptible to dangerous ideologies, corrupt, prone to breaking the law, disposed to political parties will always have a destructive effect on the service, and on many levels.

In this context, it is important to mention the relationship between the counterintelligence division and the protection of classified information division. The interaction of the two is a necessity, as the latter is the one that performs the most extensive personnel checks and has the greatest knowledge of officers and soldiers. It is the one that issues the decisive document for an officer and soldier to enter the high-risk group, the security clearance. Anyone given access to classified information automatically has to be subjected to greater oversight and vetting. It is a mistake to think that

a security clearance is a certificate of honesty and integrity. It is a document that increases the risk to the system because another person is allowed access. The very name of the document therefore seems inappropriate.

The work of the protection of classified information division must not end with the issuing of a certificate, but should begin with it. It is precisely in this respect that cooperation is essential with the counter-intelligence division, which, with the issuing of each clearance, has more threats to verify. Within the security of the service, the functional organisational arrangements and relationships of the protection of classified information, counter-intelligence and internal security divisions are the most important element of a properly functioning system.

The specifics of the operation, and especially the consequences of an error (assassination), generate the need for internal measures also in the anti-terrorist division. As it too will be subject to verification by the system, there is a need to develop its internal mechanisms accordingly.

Systemic solutions

"Systemic solutions are the foundation for the efficient functioning of the state security apparatus. Precise definition of the scope of responsibility between the elements of the system is an essential condition for effective operation". In how many studies can one find such phrases. They are so obvious that justifying them could offend many specialists, which I wish to avoid. However, it is also worth talking about systemic disparities. Let us look from this angle at the involvement of the services in the various areas of the state security system:

a) government protection – State Protection Service,
b) border protection – Border Guard,
c) organized crime – Police,
d) intelligence – Foreign Intelligence Agency, Military Intelligence Service,
e) counter-intelligence – Internal Security Agency, Military Counter-intelligence Service,
f) corruption – Central Anti-Corruption Bureau, Military Counterintelligence Service, Police, Border Guard, Internal Security Agency, Military Police,

g) terrorism – Internal Security Agency, Military Counterintelligence Service, Foreign Intelligence Agency, Military Intelligence Service, State Protection Service, Police, Border Guard, National Revenue Administration, Military Police.

This is only a brief overview, but it shows where, according to the Polish system, the greatest threats to the state lie. One might be tempted to conclude that since terrorism is such a great threat (like corruption), a specialised anti-terrorist service (e.g. such as the Central Anti-Corruption Bureau in the area of corruption) should have been established long ago. Is it really?

In mid-2022, the Norwegian Security Police (Politiets Sikkerhetstjeneste, PST) decided on personnel transfers within the service. A group of officers from the counter-terrorist division were transferred to the counter-intelligence division. There are many indications that measures have also been taken in other services to shift the main burden of involvement, as is evident from the analysis of press material and interviews with specialists from other countries. However, this does not mean that the need for efficient anti-terrorist divisions has diminished, as terrorism is invariably doing well. Counter-intelligence threats, on the other hand, are even 'better', which is why it is necessary to react. The natural fluctuation of personnel between these divisions is proving to be a necessity, but can also be a bonding factor between the internal structures of the services and an element of in-service training.

In October 2022, a US Senate committee concluded that the National Counterintelligence and Security Center (NCSC), part of the Office of the Director of National Intelligence, should become a separate national counter-intelligence unit from the existing structure. It would thus take over the FBI's counter-intelligence role. In the United States, a multiplicity of services is the order of the day.

Case II – Afghanistan

Humam Khalil al-Balawi was a Jordanian doctor born in Kuwait. He became associated with extreme Islamist groups operating in Turkey, where he ran his practice and lived with his wife and children. In 2007, he was detained by Jordanian special forces, who decided to 'turn' the terrorist and send him to Afghanistan. The Jordanians worked closely with the US CIA. Al-

Balawi's goal was to help infiltrate Al-Qaeda. In 2009, he was invited to a meeting at the CIA base at Camp Chapman in Khost province. Upon arrival, he detonated the explosives he was wearing, killing many people. It was one of the worst 'reversals' of agents in history.

Commentary

The events surrounding Khalil al-Balawi made it perfectly clear that even the most sophisticated verification systems do not provide certainty. In the operation of both anti-terrorist and counter-intelligence divisions, working with personal sources of information is of fundamental importance. It is this type of activity that brings positive results, but at the same time involves the greatest risks. Despite multi-level checks of the source, i.e. the person they will be working with, it is impossible to avoid the risk of deconspiration, disinformation or simply failure. In the work with sources carried out by the counter-terrorist divisions, it is necessary to draw on the experience of the 'big brother', i.e. counter-intelligence, despite the different specifics of work in these two divisions.

Permeation

The question is to what extent the counter-intelligence and anti-terrorist divisions should operate in parallel and to what extent they should intermingle. This problem can be discussed using three areas of service activity as an example. The first is counter-intelligence activity focusing on counteracting interference of external entities (state - foreign services, and private - corporations or criminal groups) in the structure of the state (political, economic, security). The second sphere, closely related to the first, is activities aimed at countering interference in the services themselves. There is also a third sphere that seems somewhat neglected - counteracting the emergence within the services of phenomena and groups whose views and goals are contrary to the legal order or may have a negative impact on the functioning of the democratic state.

While the participation of the counter-intelligence division in the first two activities is not in doubt, it seems that in many structures the activities in the third area have been ceded to the internal security cells. This model,

one could say: the classic model, is obviously not a bad solution. However, the question remains of the saturation of activities and the purpose of their implementation. In most cases, internal security cells are based on police-type activities - suspicion of a crime, collection of evidence, criminalisation. However, it is worth remembering that more benefits than a quick closure of the case are provided by properly conducted counter-intelligence activities and active prevention.

In the case of the anti-terrorist division, the situation is quite different. It never targets its own structure and leaves these issues to the internal security cells. Neglecting this element can entail very negative consequences and a serious threat to state security.

Case III – Sweden

In November 2022, the trial of Iranian-born brothers, 42-year-old Peyman Kia and 25-year-old Payam Kia, who worked for the Russian military intelligence service GRU for many years, began in Sweden. The brothers came to Sweden as children in the 1980s. They obtained citizenship in 1994. Payam studied at the police academy, but dropped out after the first semester.

The older brother Peyman studied at Uppsala University, after which he joined the customs service. He then worked for more than three years in the Swedish Security Police (Swedish: Säkerhetspolisen, SÄPO). In 2011 he moved to the military intelligence service MUST (Swedish: Militära underrättelse- och säkerhetstjänsten). He performed tasks in the top-secret Office of Special Intelligence (Swedish: Kontoret för särskild inhämtning, KSI), which recruits spies outside Sweden. He then returned to the SÄPO. The next stage of his career was as head of the security department at the Swedish Food Agency. He was probably spying for the GRU from 2011 onwards and involved Payam, who became a liaison officer. The brothers were arrested in 2021 after a nearly six-year investigation.

In the past, Swedish services did not employ people born in 'hostile' countries, for fear that they might be vulnerable to recruitment by their home authorities or their allies. Several other countries in the region still follow this policy, but Sweden has in recent years softened its approach to this problem.

Commentary

The Swedish case triggered a discussion about the recruitment process in the services. Particularly noteworthy were the voices that foreigners should not be admitted to them. Two things are worth emphasising at this point. Firstly, the Kia brothers were not foreigners, but Swedish citizens. Secondly, an analysis of the work of the Swedish services shows that there were many Swedes born in Sweden working for the Russians at the same time. Thus, it was not the Iranian roots of the Kias that became an issue, but their individual characteristics and the decisions they alone made. However, the most important conclusion that emerges from the analysis of this case is the diagnosed weakness of the internal security of the Swedish services, which is admitted by those involved themselves. They have learned from the incident, by no means restricting access to the service for Swedes born in other countries. They have strengthened the internal security system and counterintelligence. For this reason, among others, they are one of the best services in Europe, which, in the Russian direction, remains without doubt among the leaders in counter-intelligence activities, and with leaders it is worth cooperating.

Recruitment

Not the system, not the equipment, not the facilities, but the person. Every good service, whether it is an anti-terrorist department or counter-intelligence, must focus on selecting the best possible personnel. In the age of the progressive digitalisation of life and the integration of modern technical solutions into the work of the services, the obvious principle that the strength and efficiency of a service is determined by the team of people it has managed to recruit and properly prepare may be overlooked.

There is absolute discretion and autonomy in the world of services when it comes to recruitment and training. Moreover, every few years they modify their recruitment systems and reform their training programmes. This is, of course, the right direction, provided it is the result of an analysis of the experience and needs of the service in question. If, on the other hand, it is the result of some kind of fashion or copying foreign solutions, then it results in a lowering of the value of cadres. There is nothing wrong with this discretion, provided that the best possible results are achieved. This is why recruitment and training processes are such important and

sensitive stages. Evaluation comes with results, and these have to wait. Unless modifications and reforms are introduced too often. It is then difficult to verify what had a decisive influence on the final results.

Given the contemporary conditions of service work, two elements are worth analysing. The first is psychological testing and the second is active recruitment. Psychological testing is undoubtedly the Achilles' heel of the recruitment process. While other elements of the process have clear indicators of suitability or unsuitability for the service (e.g. education, health, criminal record, language skills, fitness), the results of psychological examinations and the conclusions drawn from them depend on the psychologist conducting the examination. Psychology is not an exact science, and the ability to assess candidates can vary as much as psychologists can vary. There is no service that has never once rejected an excellent candidate on examination or never accepted one who was a total failure. And all this just on the basis of a psychologist's opinion.

Active recruitment are activities in which the service openly seeks candidates. Nowadays, the services advertise with posters at bus stops, talks at universities, stands at job fairs. Apparently "such are these times". What a challenge such a method of recruitment poses to counter-intelligence! A self-respecting intelligence service would be happy to install itself at such a stall or university chat to type out people to work on, such as those who have been talking to the recruiter or the recruiter himself for the longest time. This method of recruitment has undoubtedly increased the involvement of the counter-intelligence division. The anti-terrorist division is exempt from such involvement. Where have those days gone when the service looked for a candidate and only after vetting did it undertake an interview and possibly further steps, the days when a candidate applied for the service, silently hoping that "maybe they will call"... The labour market (for that is now what the area of candidate sourcing is called) is forcing actions that are rather associated with the recruitment of a boys band. What quality is being created by this in the service? Adequate to the quality of recruitment. This is probably why, for example, there are cases of people resigning from the service after the entry level course. Such candidates prove to be particularly troublesome for the counter-intelligence division. They acquire knowledge, get to know people inside the service and... leave it quickly, leaving with such knowledge outside.

Training is inextricably linked to recruitment. To illustrate this, one could say that admitting an excellent mathematician to the Academy of Fine

Arts would be as misguided as admitting an excellent painter to the Faculty of Physics and Astronomy. Successful recruitment is the foundation of effective training. It is worth asking ourselves, then, where the so-called basic training should end, and where the counter-intelligence and anti-terrorist divisions should begin the process of shaping an officer or soldier to perform tasks. Moreover, there are forms and methods of action that are the same in the work of the different divisions. Taking into account the specifics described earlier, one can risk saying that the training process should be common, extended by optional classes for candidates for service in the different divisions. This is both possible and necessary, as the delegation of tasks is supposed to result from the current needs of the service, and these, as the Norwegian case described earlier shows, can change.

Opponents

Finally, in order to understand who the verticals in question come to face, it is necessary to briefly characterise their opponents. The counter-intelligence division will have as its opponent a foreign intelligence service, i.e. a criminal group with a powerful background. Why criminal? Because if intelligence is to carry out covert operations outside its own country, it will be operating there illegally under the laws of other countries. Such a group has a state with all its apparatus and resources behind it, which makes it a serious adversary.

The anti-terrorist division will be fighting a terrorist group, i.e. a group operating outside the law, without such a background as intelligence. However, the situation only apparently looks a little better, as the direction of counteraction will be much more diffuse. This still leaves the most dangerous variant, in which the terrorist group is supported by intelligence, with all its resources, which is another element forcing close cooperation between the two divisions.

Summary

After the Madrid attack, I was sent to Madrid - for lessons learned. After the attack in London, I was sent to London - for lessons learned. After

the attack in Baghdad, I was sent to Baghdad - for lessons learned. After the coup in Kabul I was sent to Kabul - for lessons learned. It is always good to know more or to listen more to those who know. I hope that we will continue to draw conclusions from events outside Poland, so that they never happen in Poland.

Bibliography

Benhold K., *Germany Disbands Special Forces Group Tainted by Far-Right Extremists*, "The New York Times", 1 VII 2020.

Dwie dekady walki z terroryzmem (Eng. Two decades of fighting terrorism), P. Piasecka, K. Maniszewska, R. Borkowski (sci. eds.), Warszawa 2022.

Działania kontrwykrywcze zorganizowanych grup przestępczych i organizacji terrorystycznych (Eng. Counter-detection activities of organised crime groups and terrorist organisations), P. Chlebowicz, T. Safjański, P. Łabuz, (sci. eds.), Warszawa 2021.

Ein Beamter machte stehend auf zwei Dienstwagen den Hitlergruß (Eng. A civil servant made the Hitler salute while standing on two official cars), "Die Welt", 30 XII 2020.

Faligot R., Kauffer R., *Służby specjalne. Historia wywiadu i kontrwywiadu na świecie* (Eng. Special services. A history of intelligence and counterintelligence in the world), Warszawa 2006.

Gefährliche Mischung (Eng. Dangerous mixture), "Tagesschau", 8 XII 2022.

Hitlergruß und fliegende Schweineköpfe (Eng. Hitler salute and flying pig heads), "Die Zeit", 17 VI 2017.

Kahneman D., *Pułapki myślenia* (Eng. Thinking traps), Poznań 2012.

Marshall T., *Potęga geografii, czyli jak będzie wyglądał w przyszłości nasz świat* (Eng. The power of geography, or what our world will look like in the future), Poznań 2021.

Piasecki B., *Kontrwywiad. Atak i obrona* (Eng. Counter-intelligence. Attack and defence), Łomianki 2021.

Sabataj S., *Byłem szefem Mosadu* (Eng. I was the head of Mossad), Wrocław 2020.

Schuman Tomas D., *Agentura wpływu. Tajniki działalności wywrotowej KGB* (Eng. Agents of influence. Secrets of KGB subversive activities), Kraków 2021.

Siemiątkowski Z., Zięba A., *Służby specjalne we współczesnym państwie* (Eng. Special services in the modern state), Warszawa 2016.

Staniuk W., *Współczesny wywiad. Humint* (Eng. Contemporary intelligence. Humint), Warszawa 2023.

Szlachter D., *Walka z terroryzmem w Unii Europejskiej. Nowy impuls* (Eng. The fight against terrorism in the European Union. New impetus), Toruń 2006.

Terroryzm i antyterroryzm w opiniach ekspertów w XX rocznicę zamachów na WTC i Pentagon (Eng. Terrorism and anti-terrorism in the opinions of experts on the 20th anniversary of the WTC and Pentagon attacks), J. Stelmach (sci. ed.), Warszawa 2021.

"Terrorism - studies, analyses, prevention" 2022, no. 1, no. 2.

"Terrorism - studies, analyses, prevention" 2023, no. 3.

The contents of the essay are the result of the author's experience of serving the Polish anti-terrorist community and represent his personal views.

Lt. Col. Tomasz Białek, PhD, Eng.

Former commander of special subdivisions of the Polish Army, former director of the Security Prevention and Internal Security Directorate of the Government Protection Bureau and of the Security Department of the Central Anti-Corruption Bureau. Auditor and expert in the field of security systems, with particular emphasis on information security and high-risk persons and facilities. Academic lecturer specialising in the sociology of security. Expert of the Polish Chamber of Security.

https://doi.org/10.4467/27204383TER.23.037.18339

Survey on terrorism in Poland and directions of its development

Expert commentary

Lorenzo Vidino

Seen from an external viewpoint, the survey conducted among 94 local terrorism experts and practitioners sheds an important light on the perceptions of key Polish stakeholders[1]. Some of the results are arguably in line with those one would reach when interviewing counterparts in other European countries. This is true, for example, when it comes to identifying Daesh and Al-Qaeda - in that specific order - as the two organizations posing the greatest security threat to both the EU and Poland; or concerns about the misuse of various technologies for terrorism purposes or likely terrorist targets.

At the same time, a couple of results do stand out as arguably reflecting a more peculiar Polish perspective. The first is the concern about the actions of Russian special services, an element not likely to receive the same kind of attention in Western Europe but that understandably worries a substantial portion of the Polish security establishment (and, one could guess, also before the Russian invasion of Ukraine).

[1] The results of the study were published in: "Terrorism - studies, analyses, prevention" 2022, no. 2, pp. 335-363.

A second result that appears noteworthy are the somewhat limited concerns expressed in relation to extreme right wing terrorism. While results might be different if questions had been phrased not by asking to identify a single organization but, rather, an ideological movement, the fact that only one right wing extremist organizations (Atomwaffen) is identified as a major threat and only by a substantially inferior number of respondents compared to those that pointed to Daesh and Al-Qaeda is indicative of a certain gap with Western Europe. While dynamics change from country to country, over the last three/four years the security establishments of most Western European countries have increasingly identified right wing extremism as equally as if not more dangerous than jihadism.

Finally, it is particularly striking that a substantial percentage of respondents believe that Poland is likely to become an attractive country for terrorist. While there are only limited indications that the country has been so in recent years, the belief that things will change for the worse in the near future seems quite widespread. Some of the answers seem to indicate that these concerns are at least partially related to threats emanating from Russia.

Overall, the results of the survey are very interesting and provide a good sense of "the pulse" of the Polish counterterrorism community. It is a commendable exercise and one that should be replicated in other countries.

Prof. Lorenzo Vidino

Expert on Islamism in Europe and North America, Director of the Program on Extremism at George Washington University in Washington, DC. For the past 20 years, he has conducted research on the dynamics of jihadist network mobilisation in the West, government counter-radicalisation policies and the activities of Muslim Brotherhood-inspired organisations in the West.

https://doi.org/10.4467/27204383TER.23.038.18340

Spanish Presidency of the EU High Risk Security Network

held by the Guardia Civil through the Grupo de Acción Rápida

Gregorio Salazar

It is not so much about the need for knowledge as it is about the willingness to share it.
Martin Schieffer, Head of Unit DG HOME-D2

In recent years, radical terrorism has targeted extremely violent attacks against critical (civilian) infrastructure, sensitive targets and transport hubs across Europe. In order to avoid this type of violence, or at least to prevent an increase in its occurrence, the Member States of the European Union are taking more and more preventive action, realising the need to implement more robust security measures and ensure better preparedness. Achieving a higher level of preparedness and security requires the development of a common cross-border strategy and joint actions and the involvement of state authorities, professional associations and private actors. It is important to extend this cooperation to as many countries as possible - both European and non-European.

In response to these needs and objectives, the EU High Risk Security Network (EU-HRSN) - an EU network of uniformed special forces for high-risk operations - was established as part of the implementation of the *EU*

Action Plan "Union for Security: Protection of Public Spaces" (announced in October 2017).

Figure 1. EU High Risk Security Network logo.

Source: Grupo de Acción Rápida's own materials.

This announce stated:

> In the last three years, the European Union and its Member States have taken decisive steps to prevent terrorists from executing attacks, share information between Member States, counteract radicalization and better manage our borders. But as the terrorist attacks carried out in Europe show, it is necessary to reinforce preventive actions to prevent the perpetration of future attacks such as those that occurred in the streets of Barcelona, Berlin, London, Manchester, Nice, Paris or Stockholm; which have had as their common denominator their execution in open public spaces. Although the risk of such attacks can never be completely eliminated, there are concrete operational measures which Member States can take with the support of the EU to better protect public spaces from the threat of terrorism. The Commission is committed to providing specific funding of more than 118 milion €, 11 million € over the next year, to intensify the exchange of best practices, to publish guidance material for Member States and to foster cooperation between local actors and the private sector (...). The Commission will establish a Professionals Forum where law enforcement professionals and existing law enforcement networks can share knowledge on the protection of public spaces. The Commission will also establish a High Risk Security Network to organize joint training and joint exercises for law enforcement

agencies to improve their preparedness and increase their response capacity[1].

EU-HRSN concept

The EU-HRSN was officially inaugurated on 1 November 2018. Its mandate is to integrate representatives of European uniformed high-risk special operations forces (civilian and military) that are part of law enforcement agencies or units performing operational or protective support tasks, in order to ensure the protection of public places, soft targets and critical infrastructure from acts of a terrorist nature and the detection and prosecution of their perpetrators. The establishment of the network is intended to facilitate the exchange of developed tactics, techniques, and procedures (TTPs) and to build better resilience to attacks. The exchange is intended to cover good practices in preventing, detecting and responding to the first phase of a terrorist attack, but not necessarily the organised response and intervention usually carried out by a government when deploying priority resources in response to a terrorist attack.

The presidency of the EU-HRSN allows the country holding the chairmanship to use not only the resources provided by the European Commission, but also the national resources allocated to the above-mentioned objectives. The first presidency was held by the Dutch Koninklijke Marechaussee through the Hoog Risico Beveiliging Brigade (HRB) and with the support of Spain, which took on the role of vice-presidency. On 1 July 2021, the Spanish Guardia Civil took over the presidency for a further 24 months, in accordance with the EU-HRSN Charter, through the Grupo de Acción Rápida (GAR).

Grupo de Acción Rápida was born in 1978 as "Unidad Antiterrorista Rural" (UAR), with the specific target of fighting against ETA, Spanish national-socialist terrorist band with more than 850 killed in 42 years. This Unit, has in its backpack more than 40 years of CT fight experience, and has been internationally deployed to Kosovo, Bosnia, Afghanistan, Iraq, Haiti, Central African Rep. and Lebanon, inter alia, under the NATO and UN umbrellas.

[1] EU Action Plan "Union for Security: Protection of Public Spaces", October, 2017.

Figure 2. Grupo de Acción Rápida logo.

Source: Grupo de Acción Rápida's own materials.

Due to the COVID-19 outbreak, some EU-HRSN activities were halted or delayed by ten months. This led to a six-month extension of the presidencies held first by the Dutch HRB and then by the Spanish GAR. The latter will end on 1 January 2024. The development of the EU-HRSN idea was negatively affected by the death of Colonel Jesús Gayoso Rey, head of the GAR and co-founder of the EU-HRSN, who died of a coronavirus infection. He was one of the main animators of both this and other EU initiatives. Let us hope that the next presidency, which will be held by Portugal's Guarda Nacional Republicana (GNR), through the Grupo de Intervenção de Ordem Pública (GIOP), will not have to face these kinds of problems. Unforeseen challenges are the domain of the members of the EU-HRSN, and when people of the same mindset work together, there are no insurmountable obstacles.

EU-HRSN aims

The main objectives of the network are:

1. Sharing best practices, conducting cross-training, sharing knowledge of procedures and other operational details, and building collaborative structures at the tactical command and control level to improve resilience to acts of serious violence or terrorism targeting civilian critical infrastructure, soft targets and transport hubs in EU Member States.

2. Increasing the knowledge base of all members by undertaking activities whereby knowledge of TTP, standard operating protocols (SOPs), risk assessment and (predictive) profiling is shared through cross-training.
3. Advising EU organisations responsible for security issues taking into account lessons learnt from the exchange of experience between EU-HRSN Member States.
4. Sharing lessons learned through specific communication channels with other organisations cooperating on security in the EU. This does not refer to working on common standards or practices, but includes - where appropriate and compatible with national law - adapting best practices and tactics and bringing together the techniques developed as a common doctrine to make them most effective. The aim is to achieve synergies, and this is to be achieved by meeting on national crisis response procedures and drawing on different solutions.

EU-HRSN membership

Members of the EU-HRSN are uniformed high-risk special operations formations (civilian and military) that are part of law enforcement agencies or units performing tasks in support of operational or protective activities to ensure the protection of public places, soft targets and critical infrastructure from acts of a terrorist nature and the detection and prosecution of their perpetrators.

Membership of the EU-HRSN is possible upon submission of a written application to the Chair. This application is subject to approval by a two-thirds majority of the Network's Member States. One of the conditions for admission is the acceptance and signature of the EU-HRSN Charter.

Associated membership is an alternative option. It gives interested parties the possibility to participate in the EU-HRSN without fulfilling all the requirements for EU-HRSN members. However, the cost of such membership is not covered by the EU budget.

EU-HRSN organisational structure

The structure of the EU-HRSN includes:

a) leadership in the form of a chair, vice-chair and steering group. The Vice-Chair is elected by a vote among the members of the Steering Group and automatically becomes the next Chair after 24 months. This allows them to gain the knowledge, experience and networking needed to properly lead the EU-HRSN during the presidency. The current Steering Group consists of representatives of the Presidency (Spanish Guardia Civil via the GAR), the Vice-Presidency (Portuguese GNR via GIOP), Belgium (Police Fédérale), Estonia (Kaitsepolitsei), Ireland (Garda Síochána via Special Tactics & Operations Command, STOC), the Netherlands (Koninklijke Marechaussee via HRB) and the D2 Terrorism Unit of DG HOME (Directorate-General of the Directorate-General for Terrorism, DG HOME-D2) as a permanent observer;
b) 25 full members (counter-terrorism units) from 18 Member States;
c) Norway, the United Kingdom and the United States as associate members;
d) ATLAS Network and DG HOME as observers.

EU-HRSN activities

The network is vigorously exchanging information with and receiving organisational and substantive support from other counter-terrorism initiatives of the European Commission. This applies in particular to the experience of the work on so-called Red Teaming tactics[2] within the Policy Group on Public Spaces Protection, the projects carried out within the EU-US security subgroups (e.g. security of special events, explosives seminar) and the Protective Security Advisors (PSA) group, which is a very interesting initiative of DG HOME-D2. This group consists of a number of experts with extensive expertise in public spaces protection (PSP) and counter-terrorism protection at mass events and major VIP events (e.g. CBRN-E, C-IED, UAS/

[2] Red Teaming – types of procedures related to assessing the level of protection against terrorist activity and dealing with measures to increase attack resistance. These are carried out using unmanned systems (editor's note).

C-UAS threats[3], snipers, tactical rescue and response, K2 service dog unit, building resilience to hybrid threats in critical infrastructure)[4]. They can be organised into small teams, advising a particular service or government and supporting a comprehensive security approach.

Image 1. Meeting of the Protective Security Advisors group.

Source: Grupo de Acción Rápida's own materials.

The EU-HRSN also exchanges extensively with other EU networks such as ATLAS and ENLETS (The European Network of Law Enforcement Technology Services). It is also represented in various forums, e.g. Operators and Practitioners, and has close links with EU working groups on issues such as CBRN-E, UAS/C-UAS, EDD[5]. All this serves to disseminate best practice in the protection of major events, public spaces, transport and communication hubs or places of worship. In order to achieve these objectives, five working groups have been set up within the EU-HRSN:

- WG 1 – *Threat and Risk Assessment* – working group on threat and risks assessment for terrorist attacks, coordinated by PSA unit,
- WG 2 – *Tactical use of UAV/C-UAV*[6] – working group on unmanned aerial vehicles, coordinated by Spain (GAR),

[3] CBRN-E - chemical, biological, radiological, nuclear, explosive threats; C-IED - counter improvised explosive device; UAS - unmanned aerial system; C-UAS - counter unmanned aerial system (editor's note).

[4] See In more detail: M. Schieffer, R. Olszewski, B. Zapletal, W. Wojtas, *European Union initiative to support Member States' efforts in the protection of citizens and critical infrastructure from terrorist attacks*, "Terroryzm – studia, analizy, prewencja" 2023, no. 4.

[5] EDD – Explosives Detection Dogs (editor's note).

[6] UAV - unmanned aerial vehicle; C-UAV - counter-unmanned aerial vehicle (editor's note).

– WG 3 – *Tactical Rescue and Response* – working group on tactical rescue and high-risk incident response issues, coordinated by Ireland (STOC),
– WG 4 – *Human Factor* – working group on issues related to the selection of people and their training procedures, coordinated by the Netherlands (national police),
– WG 5 – *Multi-agency Command and Control* – working group responsible for managing high-risk operations, coordinated by the UK (National Counter Terrorism Security Office).

Diagram. EU-HRSN working groups.

Source: Grupo de Acción Rápida's own materials.

During the current Spanish Presidency, efforts have been made (together with the Steering Group) to develop a new approach to event protection issues. Indeed, the GAR's experience has shown that there is no better way to exchange knowledge and good practices than to work in the field, facing real challenges and applying different TTPs, developed in different environments and legal frameworks, and confronting hostile TTPs encountered in the work of the services of individual member countries. This way of exchanging knowledge and experience was used for the first time in the history of the EU-HRSN in September 2022 in Templemore (Ireland), to which the Irish police (Garda Síochána) invited more than 60 experts from 12 different countries. These were specialists

in tactical rescue and emergency response, representatives of all those who would be involved in a real situation requiring intervention.

In turn, the Experiences Polygon for Special Forces (UAR/GAR/CoEST)[7] met in November 2022 in Logroño (Spain) to exchange experiences between members of WG 2. This included experts from the US (FBI), Belgium, Spain, Portugal, France and Ireland.

Image 2. WG 2 meeting - exchange of experience on C-UAS.

Source: Grupo de Acción Rápida's own materials.

The work of WG 1 started a few weeks later in Brussels. As they are closely linked to the activities of the EU PSA group and those involved in Red Teaming tactics, the opportunity was taken for those involved in these three EU initiatives to exchange their knowledge.

Image 3. Meeting of WG 1 and persons involved in Red Teaming tactics in the EU PSA.

Source: Grupo de Acción Rápida's own materials.

[7] CoEST – Centre of Excellence for Special Training.

In 2023 in London meeting of WG 5 and Ramming Vehicle Workshop took place. Meeting of WG 4, general conference, steering group meetings and joint training and other forms of knowledge exchange organised to increase resilience to terrorism and create conditions that make it more difficult to undertake various types of terrorist acts are planned for the second half of 2023.

The activities of the EU-HRSN are not limited to the EU area. It also directly or indirectly supports other Union initiatives beyond its borders through projects such as GAR-SI SAHEL (Groupes d'Action Rapide - Surveillance et Intervention au Sahel), covering Mauritania, Burkina Faso, Mali, Niger, Senegal and Chad, the already completed CT MENA (Counter-terrorism in the Middle East and North Africa) concerning the Middle East and North Africa, and CT Public Spaces - in Ghana, Kenya and Senegal.

The EU-HRSN network is needed and that is why this initiative will grow, as terrorist threats will unfortunately continue to exist. Creating a common language in the counter-terrorism community, sharing expertise and building trust is intended to create a strong team to effectively counter terrorist threats. The EU-HRSN may prove to be one of the best tools in the fight against these threats.

Useful links

Action Plan to support the protection of public spaces:
https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52017DC0612

CT Public spaces:
https://www.ctpublicspaces.eu/

EU networks and initiatives:
https://ec.europa.eu/newsroom/pps/items/715174/en

GAR-SI-SAHEL:
https://ec.europa.eu/trustfundforafrica/region/sahel-lake-chad/regional/gar-si-sahel-groupes-daction-rapide-surveillance-et-intervention_en

PSA:
https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en

Contact: Presidency@HRSN.EU

Gregorio Salazar

Field officer, and later instructor. He is specialised in tactical rescue and response, sniping, police self defense, and intervention and shooting drills. In 2014–2018 he was posted as head of security of the Embassy of Spain in the United Kingdom. Strategist of the Spanish presidency of the EU High Security Network. He has served for more than 20 years in the Guardia Civil. He shares knowledge and expertise in the international environment.

https://doi.org/10.4467/27204383TER.23.039.18341

EU Protective Security Advisors

European Union initiative to support Member States' efforts in the protection of citizens and critical infrastructure from terrorist attacks

Radosław Olszewski, Beate Zapletal, Wiktor Wojtas

EU PSA concept

Securing public spaces and critical infrastructures is the primary responsibility of Member States. Like in many other areas of internal security, there is however a role that the European Union could play – facilitating sharing of good practices, encouraging practical exchanges of experience and supporting mutual operational assistance. One of successful examples of such an approach is the EU Protective Security Advisors programme.

While officially announced only in December 2020, with the publication of the EU Counter-Terrorism Agenda[1], the EU PSA programme has its roots in the EU work on protection of public spaces (back then called soft targets) that started in 2012. That year the European Commission

[1] *A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0795 (editor's note).

officials were invited to provide expert support for the security measures around the EURO 2012 football championship. This positive experience led to subsequent invitations from other Member States. The European Commission contributed to protection of high-level political events such as NATO summits or open-air events such as Christmas markets or music festivals such as the Untold festival organised in Cluj-Napoca, Romania.

A major step in the EU policy on protection of public spaces was the Action Plan adopted in October 2017[2]. As part of its implementation, an EU vulnerability assessment tool was developed. This very practical instrument facilitated on-site assessments of high risk events, performed jointly by the Commission and Member States experts. The success of this initiative led to creation of a pool of experts from law enforcement, but also security and intelligence services, that led to establishment of the EU PSA programme. It is worth underlining that the European Commission – whilst having a clear idea on the way forward – benefited from the support and expertise of relevant international partners such as the United States that are having their own EU PSA programme. Moreover, several EU-US joint missions and exchanges of best practices took place in the EU and United States.

EU PSA tasks

The aim of the EU PSA missions is to provide support to Member State requesting it. The missions have several objectives:

- improve understanding and awareness of the vulnerabilities in public spaces and critical infrastructures by providing a common methodology for their assessment;
- share good practices and encourage peer-to-peer learning to address identified vulnerabilities;
- provide advice to Member States in the organisation of high-risk events or facilities;
- create an expert community through common trainings and missions, contributing to the development of a common EU protective security culture.

[2] *Action Plan to support the protection of public spaces*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0612 (editor's note).

The EU PSA pool is composed of roughly 100 experts from the European Commission and Member States (in case of Poland, the experts come from police, Internal Security Agency and State Protection Service). They are all professionals in the security of public facilities, but at the same time have different expertise. When a Member States requests support, it must specify what kind of expertise it is looking for. Each EU PSA team will consist of experts holding different qualifications in areas such as unmanned aerial vehicles (UAV) operations, explosive and CBRN (chemical-biological-radiological-nuclear) threats detection, special intervention and counter terrorism tactics, crisis management and other expertise areas. Depending on the mission and the target of such support, EU support may be limited to either the event security preparatory phase or both preparatory and support during the actual event. The review will be confidential and conducted in close dialogue and partnership with the experts of the host authority. The exchanges will provide a two-way opportunity to exchange good practices and lessons learnt, improve awareness of vulnerabilities and contribute to the gradual development of a common security culture across the EU.

EU PSA missions scope

Whilst – as explained at the beginning – the EU PSA programme was a result of development of the EU-level policy on protection of public spaces, nowadays it covers also protection of critical infrastructures. The list of recent EU PSA missions includes places of worship and other faith-based institutions, cultural events such as large music festivals, VIP events such as EU summits, but also large infrastructures such as a major hub airport (Warsaw) or a major sea port (Constanza, Romania). In this place it is important to underline that the EU PSA programme does not overlap with the EU aviation and maritime security inspections. These instruments have different scope and objectives. Given the recent focus at the EU level on enhancing the resilience of critical entities, most likely the future will bring more assessments of these types of facilities.

EU PSA mission examples

In the recent years there has been a spike in the attacks against the places of worship. It does not come therefore as a surprise that recently they were among priority locations for EU PSA missions. The EU PSA team visited for instance the cathedrals in Ulm and Münster, Germany, where it looked – among others – at the vehicle ramming threat as well as an active shooter scenario.

An event that particularly benefited from the EU PSA support is the Untold music festival organized in Cluj-Napoca, Romania. Hundreds of thousands of music fans come to enjoy the music and have fun. Providing appropriate level of security in such case is a major challenge. This is the reason why the Romanian authorities requested EU PSA support during three subsequent editions of the festival. With each passing year, the security measures were better and better. At the same time, the EU PSA team provided operational support when it comes to unauthorized drone detection. The operator of the largest Polish airport, i.e. Warsaw Chopin Airport, also asked for help. The EU PSA team assessed – among others – the security of fuel and energy supply.

EU PSA future

With the EU PSA programme gaining more and more recognition among Member States authorities and with unstable geopolitical environment, one can expect that the interest in the EU PSA missions will be growing. Member States already indicate intention to invite the European Commission and Member States experts with a view to conduct assessment of some of their critical infrastructures, especially in the context of the recently adopted directive on the resilience of critical entities[3]. From the EU PSA point of view, this opportunity comes with certain challenges. Some of the requests concern very niche sectors. It might be therefore difficult to find experts with the relevant expertise. It has to be born in mind that the EU PSA programme is still a young initiative that will be rapidly developing in the coming years, incl. enlarging the scope of its expertise. Whilst this may

[3] *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC* (OJ EU L 333/164 of 27 December 2022) – (editor's note).

be difficult at times, one thing is sure - at the end of the process, the EU citizens and operators of critical infrastructures in the EU will be better protected from the terrorist threat.

Image. EU PSA team's members (from the left: Radosław Olszewski, Wiktor Wojtas, Krzysztof Sowiński, Damian Szlachter) during the assessment of Warsaw Airport; May 2022.

Source: European Commission's Directorate-General for Migration and Home Affairs' materials.

The authors work in the Counter-Terrorism Unit of the European Commission's Directorate-General for Migration and Home Affairs. The article reflects the state of play as of 1 III 2023 and the views expressed are purely personal and do not represent the official position of the European Commission.

Radosław Olszewski

Expert in the counter-terrorism unit of European Commision's Directorate-General Migration and Home Affairs. Founder and leader of the EU PSA initiative. Seaman and aircraft pilot. Former civil aviation security auditor at the European Commission.

Beate Zapletal

Seconded National Expert in the counter-terrorism unit of European Commision's Directorate-General Migration and Home Affairs since February 2020. She is involved in the EU Protective Security Advisors programme. Previously she worked in Germany in the Federal Ministry of Interior and the Federal Ministry of Transport. Before joining the public service, she had worked in Germany in the financial sector.

Wiktor Wojtas

Policy analyst in the counter-terrorism unit of Directorate-General Migration and Home Affairs of the European Commission since early 2013. Previously he worked in the same Directorate-General as a Programme Manager for the Prevention of and Fight against Crime programme. Before joining the European Commission in 2007, he had worked in Poland in the financial sector. He is involved in the EU Protective Security Advisors programme.

https://doi.org/10.4467/27204383TER.23.040.18342
https://orcid.org/0000-0003-2763-9325

Prevention first

Swedish model of anti-terrorist protection

In January 2023, Sweden took over the presidency of the EU Council. One of the four priorities of this Presidency was security, including protection against terrorist threats. Damian Szlachter talks on anti-terrorist solutions used in Sweden, the role of prevention, education and international cooperation in increasing the level of security and challenges for the local services related to the presidency, with **Daniel Hedman**, an expert of the Stockholm Police on building resilience to terrorist attacks.

Sweden took over the six-month presidency of the EU Council. Will protection against terrorism be one of the priorities of this Presidency?

Daniel Hedman: The Presidency of the EU Council always operates in the so-called trio (the classic Troika consists of the member state holding the presidency, the state that held it previously, and the one that will hold it for the next six months - added by D.Sz.). The Swedish Presidency will continue the program agreed with the other two countries of the three. Building resilience to terrorist threats is, of course, one of the priorities of the Swedish government, and the greatest emphasis will be placed on terrorist prevention. This concerns prevention in the context of radicalization leading to violent extremist activities and reducing vulnerability to dangerous ideologies, as well as the terrorist activity itself, crisis management in the event of a terrorist attack and building resistance to such attacks among potential targets. Prevention is the pillar of the fight against terrorism. This approach is particularly close to the Swedish society.

How is the level of terrorist threat in Sweden assessed? Which institution plays a leading role in this regard?

D.H.: In Sweden, the terrorist threat level classification system is very similar to the solutions in force in most EU countries. Currently, this level is 3 (increased threat, no evidence of planning - added by D.Sz.) on a 5-point scale (5 - imminent attack, evidence of planning - added by D.Sz.). The body assessing the level of this threat is the National Center for Terrorist Threat Assessment (NCT, Nationellt centrum för terrorhotbedömning). NCT is a permanent working group within the Swedish Counter-Terrorism Cooperation Council (Samverkansrådet mot terrorism) in the Swedish Security Service (Säkerhetspolisen, SÄPO), but not its formal part. NCT is staffed by personnel from the National Defense Radio Establishment (Försvarets radioanstalt, FRA), the Military Intelligence and Security Directorate (Militära underrättelse- och säkerhetstjänsten, MUST) and the Swedish

Security services. Terrorist threat ratings are also given to 14 government agencies that are part of the Counter-Terrorism Cooperation Council. NCT produces analyses, including strategic analyses, but does not investigate crime. It only formulates an assessment of the degree of risk. The final decision on the level is made by the head of the Swedish Security Service.

Stockholm ranks high on the list of European cities that have experienced various types of terrorist attacks in the last few decades. How the resilience against these attacks in the Swedish capital has been building? What is the emphasis on?

D.H.: At the moment, two issues are the most important - continuing cooperation in the field of preventive actions aimed at preventing radicalization leading to terrorism and building resilience to kinetic attacks. Building this resilience is closely related to the country's civil defense and the state's defense strategy, and due to the geopolitical consequences of the war in Ukraine, it is embedded in the area of integration with NATO. In Sweden, we have a holistic approach to protecting the country from modern hybrid threats. Great importance is given to building resistance in society against various types of threats, and more precisely to shaping social mentality.

We have some systemic gaps in the field of legislation, for example in the assessment of what is critical infrastructure (CI) and what is not, as well as who in the government administration is responsible for protecting facilities other than CI. It is worth bearing in mind that historical and statistical data always describes the past, but it does not allow to clearly predict the future (it should also be remembered that the classification of specific incidents related to terrorism changes over the years. For example, a year earlier an event could have been classified as an extremist incident, and after legal changes as a terrorist attack - added by D.Sz.). Unfortunately, Stockholm is a city particularly affected by terrorist incidents. Several of them took place in the center of this metropolis (five in 22 years - added by D.Sz.). This part

of the city is very vulnerable to attack, as it is home to facilities such as shopping and business centers, government buildings, parliamentary offices, symbolic buildings belonging to the Swedish monarchy, strategic hubs for public transport. A lot of VIPs appear there, as well as a huge number of tourists. This attracts the interest of extremists glorifying violence as a tool of political action and terrorists.

What kind of facilities receive state support in the field of anti-terrorist prevention in Sweden?

D.H.: In 2014-2015, the Swedish Police began to support the Stockholm authorities in the first anti-terrorist initiatives aimed at strengthening the physical security of selected facilities that are highly vulnerable to terrorist attacks. These activities were intensified after the attack on the Norwegian island of Utøya, which was a huge shock for all Nordic countries and a moment of awakening. At the beginning of the prevention projects, we focused on increasing the capacity of the Swedish police to deal with the consequences of terrorist attacks, on preventing radicalization leading to terrorism (cooperation between local authorities and communities at risk of radicalization was deepened - added by D.Sz.), developing an advisory program for increasing the resistance of soft targets to kinetic attacks. The leader in this area was the police, which at the initial stage of work was supported by the government's Agency for Crisis Management/Business Continuity (Swedish Civil Contingency Agency, Myndigheten för samhällsskydd och beredskap, MSB).

Since 2016, we have been creating a legal framework from scratch, selecting field leaders, developing a methodology for assessing facilities, procedures and standards standardizing system solutions for protection against terrorism. Specialist guides have been prepared, also in English, in order to reduce vulnerability to attack, devoted to, among others, security of mass events, responding to an active shooter or protection of public spaces. They are considered exemplary and used not only in Sweden, but also at the EU level (the next four are translated into English - added by D. Sz.), e.g. in expertise

published by the EU Joint Research Center of the European Commission in the area of anti-terrorism.

We currently have regulations binding government agencies and 9 out of 12 government sectors that are classified as critical infrastructure systems. However, it has not been clearly defined what is this infrastructure and what is not. For example, Stockholm Central Station is not an CI until an event causing a major disruption to this strategic transport route is classified as critical. In other words, the support of this particular facility by the Swedish secret services takes place only when there is an incident that is critical for ensuring the continuity of rail transport in the city. Nearly 90% of state institutions and related bodies (basic services - added by D.Sz.) belong to the Swedish critical infrastructure and therefore may be covered by programs dedicated to building resistance to terrorist attacks.

Today, it can be said that Sweden has systemic solutions under which local authorities, representatives of social organizations or businesses can ask the police or MSB for support in building comprehensive resistance to terrorist attacks. Until five years ago, people were virtually unaware of the existence of physical anti-terrorist barriers to stop a car attack. Currently, Sweden has a system of protection against a terrorist attack and its consequences, in which dialogue of all parties plays an important role. Let me repeat once again, these are systemic solutions built from scratch.

From the perspective of your experience, what has a real impact on increasing the object's resistance to terrorist attacks? What solutions should be prioritized, for example, in the case of government offices or transport facilities constituting critical infrastructure?

D.H.: The most important issue is designing a detection system that uses a system of sensors, video cameras, gates detecting metal objects or access control points. Increasing the chance of detection is of great importance in preventing terrorist or sabotage threats. The basic condition for creating an effective

detection system is the implementation of a security zone outside the protected facility, at a distance of 10 to 100 meters from its outline. The visibility of each security system is also important. It's an expensive solution, but it's not worth saving on security. This is how we build resistance to terrorist threats at Stockholm Central Station, which I mentioned earlier. In a few months we will know the first data on whether the new protection model for this facility works. It is also worth ensuring that this detection system is designed in the simplest possible way and respecting civil liberties. Sweden is an example of a country that proves that this balance is achievable and acceptable to local communities.

Sweden is very active in the EU in the field of terrorist prevention and undertakes numerous educational initiatives in the field of security. Which of them have a European dimension and could be successfully implemented in other countries?

D.H.: With regard to scientific activities, it is worth highlighting the achievements of Swedish researchers dealing with terrorist threats and social radicalization processes, who co-lead the work of the EU Radicalization Awareness Network (RAN). In particular, I have two professors in mind – Magnus Ranstorp and Hans Brun. When it comes to the issues of physical protection against terrorist attacks, it is certainly worth mentioning the creation of inter-institutional anti-terrorist consulting teams (a kind of experience and knowledge exchange center - added by D.Sz.) for local communities. This initiative is worth taking in other EU Member States and in EU structures. For example, create anti-terrorist advisory teams or centers for improving skills in the field of combating terrorism, consisting of representatives of all organizational units (directorates general) of the European Commission. Currently, each EU body creates its own recommendations and handbooks on protection against terrorist threats, limiting itself only to its area of competence. It is worth going towards the „one for all" principle.

What was the biggest challenge during the Swedish Presidency of the EU in the area of protection against terrorism?[1]

D.H.: The biggest challenge was the large number of meetings and the fact that they were held in several different places – in the north and south of Sweden. Some of our police units at the regional level are inexperienced in handling this type of encounter, partly lacking the operational skills needed to deal with such a challenge. This forced large movements of human and equipment resources in a short time. The organization of security for meetings was difficult due to the need to constantly modify the current threat analysis in various places of event organization, which had to be based on the strategic level of assessing the terrorist threat in the country. This was especially true of the meetings where people with VIP status appeared in an unscheduled way. Given that adverse events could seriously damage Sweden's image, it was necessary to increase efforts beyond the norm to ensure comprehensive protection against several different types of threats, including intelligence gathering and monitoring of terrorist offenses in a crisis situation.

He was talking: Damian Szlachter

Daniel Hedman

Superintendent, officer of the Swedish Police Authority for plus 30 years. He is employed in Public order and Public security unit, with responsibilities in relation to the handling of major events, building of protect capabilities within the Swedish society and executing protective security advisory on national and EU level. He has wide experience in the field of operational command and control over special police operations and multi-agency cooperation. He has worked, among others, at the National Counter Terrorism Council as responsible for increasing Swedish police authority capabilities combatting. He has also worked within the Swedish Defense Forces.

[1] The interview was conducted in February 2023. The last question was asked during the authorization - in July 2023, after the end of the Presidency of the EU Council by Sweden (ed.).