TERRORISM

studies
analyses
prevention

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

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

Translation Sylwia Kłobuszewska

Cover design Aleksandra Bednarczyk

ISSN 2720-4383
e-ISSN 2720-6351

Material posted in the Articles section and review articles posted in the Review Articles/Reviews section are subject to 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. Nadwiślańczyków 2, 05-462 Wiązowna, Poland

Contact
phone (+48) 22 58 58 695
e-mail: wydawnictwo@abw.gov.pl
www.abw.gov.pl/wyd/

Printed in July 2025.

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

TABLE OF CONTENTS

AWARDED THESES

VARIA

Ladies and Gentlemen!

Over the years that I have had the privilege of taking part in the development of the Polish counter-terrorist system at the strategic, tactical or operational level, I have enjoyed working with the commanders and operators of the country's counter-terrorist units, both civilian and military. As part of my foreign cooperation, I have observed the esteem in which Polish counter-terrorists are held in NATO countries. This approval was not a courtesy result. It has been gained through joint operations on land, sea and air. It is worth knowing that the solutions developed in Poland have been and are being implemented in many partner countries. They were created by people who built the foundations of counter-terrorism in our country and are constantly working on improving it. I am far from being over-enthusiastic about this pillar of the Polish anti-terrorist system, but I can see and appreciate the progress that has been made in this area after 11 September 2001.

In the seventh issue of the journal "Terrorism – Studies, Analyses, Prevention" (T-SAP) we publish material on the elite "GROM" Military Unit No. 2305. In this way we want to honour the 35th anniversary of its establishment and to offer well-deserved congratulations from the partner service. I recommend an article in which you can read about potential directions for the development of cooperation between the "GROM" Military Unit and intelligence and coutreintelligence. I hope that in this way we will trigger discussions on how to improve the anti-terrorist system of the Republic of Poland to make it more efficient, more flexible and more responsive to current challenges and threats.

In an article discussing the data in the annual Europol report (*European Union Terrorism Situation and Trend Report 2024*), the most authoritative source of knowledge about the terrorism in Member States, you can find out how the level of these risks is currently shaping up in the European Union. It is the subject of evaluation by all European law enforcement authorities. We asked Polish terrorism experts to analyse it.

A big influence on the scale of the terrorist threat in Europe is what happens in Africa. The migration phenomenon on the eastern NATO's flank and the EU border, artificially induced by Russia and Belarus, would not have reached such a scale were it not for, among other things, the difficult situation in the Sahel region. Political instability in the countries of this part of Africa, humanitarian crises, the growing influence of terrorist groups and mercenary actions increase the risk of destabilisation of the southern flank of the Alliance. In the following expert analysis appearing in this issue you can find out how much of impact this region has on terrorist activity in the EU. The question of whether there will be a revision of the strategy of action regarding this region and direction after this year's NATO Summit in The Hague, remains open.

One of the pillars of the fight against terrorists is blocking the propaganda they disseminate on the internet. Creating the illusion of belonging to a virtual community of fighters for a common cause is an effective way of attracting the next generation of young people. In Poland, the amended Act on anti-terrorist activities implementing the provisions of the *Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online* came into force. According to it, the leading service in this area is the Internal Security Agency (ABW). We are publishing a legal commentary on the provisions of this law concerning orders to remove terrorist content and special measures, i.e. the procedure for issuing decisions on hosting service providers exposed to this type of content. This is the most comprehensive study on this subject in Poland.

The events of the recent years allow us to risk a statement that threat scenarios, which have so far been classified by the services as unlikely, should not be underestimated. One of these is the use of biological agents for hybrid activities. I encourage you to read the article that provides an introduction to the issue of biosecurity. It includes a review and analysis of security and protection of biological agents as well as related technologies that could be used as a weapon or terrorist agent.

I would like to conclude by highlighting the first in-depth analysis in years on the state of the protection of persons and property sector in Poland. Those who operate within the private security sector are a key partner of the services and institutions creating a national anti-terrorist community. Not only public order but also the security of strategic facilities, including critical infrastructure, depend on the strength of these alliances. This is not the first time that the problems and challenges facing the security sector in Poland appear on the pages of T-SAP. The authors of the report, the results of which we present, identify our journal as a valuable source for the industry. Thank you for appreciating our work.

The magazine published by the ABW is becoming an important voice not only in building internal security of the Republic of Poland. We are increasingly effective in promoting the Polish point of view on EU anti-terrorist policy in the EU institutions and agencies. On this occasion, I offer for your consideration the special issue of T-SAP entitled *Terrorist and sabotage threats to critical infrastructure*, prepared in cooperation with the Internal Security Agency and the Government Centre for Security (RCB). This issue, in line with priorities of the Polish Presidency of the Council of the EU, is available online in two languages: Polish and English on our website. We prepared it to support national and EU initiatives to increase resilience of CI to hybrid threats.

https://abw.gov.pl/pub/terrorism-studies-analyses-pre/15,Intro.html

Editor-in-Chief
Damian Szlachter, PhD

ARTICLES

Terrorism – Studies, Analyses, Prevention, 2025, no. 7: 307–326

https://doi.org/10.4467/27204383TER.25.035.21812

Article

The new face of terrorist threat in the European Union. Analysis of the EU Terrorism Situation and Trend Report 2024 (TE-SAT) and other sources

SEBASTIAN WOJCIECHOWSKI https://orcid.org/0000-0002-7972-6618

Adam Mickiewicz University in Poznań
Institute for Western Affairs in Poznań

ARTUR WEJKSZNER https://orcid.org/0000-0002-7638-9708

Adam Mickiewicz University in Poznań

Abstract

This article focuses on the issue of the terrorist threat in the European Union in 2023. The starting point for the analysis is Europol's latest report entitled *TE-SAT. European Union Terrorism Situation and Trend Report 2024*, and other sources. The analysis covers both the substantive aspect of the threat (from ethno-national and separatist, far-left and anarchist, jihadists and far-right groups) and the quantitative aspect (indicating the number of terrorist incidents and the number of people involved in particular types of terrorist activity). In 2023, as many as 120 terrorist attacks were reported in the EU, including 98 completed, 9 failed and 13 foiled. This compares with 18 attacks in 2021 and 28 in 2022. In 2023 there was over a fourfold increase in the number of attacks compared to the previous year. The attacks occurred in 7 EU countries: France – 80, Italy – 30, Germany and Spain – 3 each, Belgium – 2, Greece and Luxembourg – 1 each. In 2023, a total of 426 people were arrested for terrorism and in 2022 – 380. The highest number of arrests in 2023 was in Spain, France, Belgium, and Germany – over 50 in each of them. It means that terrorism poses a serious threat to the security of the EU in a vertical dimension (concerning

the number of attacks and accused of terrorism), a horizontal dimension (relating to the diverse tactics and strategies of the perpetrators), and a behavioral dimension (analysing different motivations and profiles of terrorists).

Keywords

terrorism, European Union, security, Europol

Introduction

The re-escalation of the terrorist threat, which is occurring in the 2020s in various parts of the world, and the accompanying phenomena are unfortunately not always recognised and countermeasures are not adequately implemented. This is illustrated by the results of a report on threats to the modern world, which was published ahead of the World Economic Forum (WEF) in Davos (20–24 January 2025). This cyclically published survey shows that the vast majority of the more than 900 respondents (business, political and scientific leaders) believe that terrorism[1] is not a significant threat in the next 12 months, the next 2 years or the next decade[2]. State-based armed conflict ranked first among responses regarding threats in 2025 with 23%. This choice was explained by respondents, among other things, by the highest level of global polarisation since the end of the Cold War[3]. They further stressed that the number of wars has increased over the past decade. This is also pointed out by the Stockholm International Peace Research Institute (SIPRI), according to whose findings as many as 52 countries experienced armed conflict

[1] On defining the concept of terrorism, see, for example: S. Wojciechowski, *The Hybridity of Terrorism: Understanding Contemporary Terrorism*, Berlin 2013; *The Routledge Companion to Terrorism Studies. New Perspectives and Topics*, M. Abrahms (ed.), London 2024; K. Maniszewska, *Towards a New Definition of Terrorism: Challenges and Perspectives in a Shifting Paradigm*, series: Contributions to Security and Defence Studies, Cham 2024. https://doi.org/10.1007/978-3-031-58719-1.

[2] *The Global Risks Report 2025. 20th Edition. Insight Report*, World Economic Forum, https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf [accessed: 6 II 2025].

[3] Ibid., pp. 7–8.

in 2023[4]. This was followed by extreme weather events (14% of responses) and geoeconomic confrontation (8%). In addition, misinformation and disinformation (7%) and societal polarisation (6%) were mentioned in the top five. Disinformation, extreme weather events, escalation of hostilities, polarisation of societies and cyber warfare were identified as the biggest threats in the next two years. The responses regarding perceptions of dangers over the decade were slightly different. Here, the first 4 of the 5 dominant categories related to various environmental issues, while the last one related to misrepresentation and disinformation. Unlike some earlier reports[5], nowhere was terrorism indicated. This is all the more surprising given that it has been escalating to varying degrees in different parts of the world[6], including Africa, the Middle East and the European Union, as will be discussed later in this article.

Furthermore, according to the Bertelsmann Foundation 2024 survey of more than 26 000 respondents in the 27 EU Member States and the UK, terrorist attacks are the second (21% of indications) biggest threat to peace in Europe, after the lack of effective border protection (25%). This was followed by major cyber attacks (19%), attack by a foreign power (18%) and organised crime (17%)[7].

The starting point of the analysis carried out in this article is the hypothesis that terrorism poses a serious threat to the security of EU Member States and their populations both vertically (concerning the number of attacks and people accused of terrorism), horizontally

[4] R. Gowan, *Overview, 2. Trends in armed conflicts,* in: *SIPRI Yearbook 2024*, Stockholm International Peace Research Institute, https://www.sipri.org/yearbook/2024/02 [accessed: 5 II 2025].

[5] See, e.g.: *The Global Risks Report 2021. 16th Edition. Insight Report*, World Economic Forum, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf [accessed: 7 II 2025]; *The Global Risks Report 2022. 17th Edition. Insight Report,* World Economic Forum, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf [accessed: 12 V 2025].

[6] See, e.g.: R. Gunaratna, *Global Terrorism Threat Forecast 2025*, "RSIS Commentary" 2025, no. 002; *Security Council debates growing terrorism threat in Africa*, United Nations, 21 I 2025, https://news.un.org/en/story/2025/01/1159246 [accessed: 8 II 2025].

[7] I. Hoffmann, C.E. De Vries, *Old Habits Die Hard – Member States Report. Part II: Remaking the Transatlantic Partnership: Public Opinion in the EU and seven Member States*, Eupinions, 20 XI 2024, https://eupinions.eu/de/text/old-habits-die-hard-member-states-report [accessed: 15 III 2025].

(referring to the varying tactics and strategies of the perpetrators) and behaviourally (analysing the motivation and profile of terrorists)[8].

Terrorist threat in the context of the situation in Africa, the Middle East and the war in Ukraine

Europol's *TE-SAT. European Union Terrorism Situation and Trend Report 2024*[9] not only presented the extent and nature of the threat in the EU, but also the related broader context, including the war in Ukraine, the situation in the Middle East or the escalation of terrorism in Africa. The latter aspect was also highlighted in the United States Africa Command (AFRICOM) report[10]. It indicated that in the first half of 2024 alone, the Islamic State of Iraq and Syria (ISIS) and its affiliated groups carried out 788 attacks worldwide, of which as many as 536 occurred in Africa. This is alluded to in information provided to the United Nations Security Council by the African Union Commissioner for Political Affairs, Peace and Security (PAPS) Bankole Adeoye. They show that Africa is currently the area most threatened by terrorism. In 2024, there were more than 3400 terrorist attacks there, with almost 14 000 deaths. This is particularly true in sub-Saharan Africa, where 59% of the world's terrorist deaths occurred. The spread of Al-Qaeda and ISIS from Mali, Niger and Burkina Faso to West African coastal states such as Nigeria, Benin, Togo, Ghana, Côte d'Ivoire has resulted in a 250% increase in attacks relative to 2022–2024. UN Security Council Deputy Secretary-General Amina Mohammed commented: *Africa tragically remains the epicentre of global terrorism*[11]. Deteriorating economic, social and political conditions there, resulting in, among other things, mass migration or armed conflicts, are factors that contribute to

[8] On the causes of terrorism, see in more detail: S. Wojciechowski, *Reasons of Contemporary Terrorism. An Analysis of Main Determinants*, in: *Radicalism and Terrorism in the 21st Century. Implications for Security*, A. Sroka, F. Castro-Rial Garrone, R.D. Torres Kumbrián (eds.), Frankfurt am Main 2017.

[9] Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2024*, https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf [accessed: 9 II 2025].

[10] *U.S. Africa Command Civilian Casualty Assessment Report; 2nd Quarter, FY2024*, https://www.africom.mil/what-we-do/airstrikes/civilian-harm-report/us-africa-command-civilian-casualty-assessment-report-2nd-quarter-fy2024 [accessed: 14 IV 2025].

[11] *Security Council debates growing terrorism…*

the growing terrorist threat in Africa. All this destabilises the situation not only in the region, but also outside, including in the EU[12].

The apparent resurgence of ISIS and the accompanying operational-propaganda offensive was commented on by the Head of the United Nations Office of Counter-Terrorism (UNOCT), Vladimir Voronkov. He stressed that ISIS and its affiliates have also started to operate outside of Africa – in Syria, Iraq or Afghanistan[13], which has resulted in a significant increase in the number of attacks and their victims, mainly among civilians[14]. This is due in part to the spectacular success of the opposition in Syria, including its Islamist strands also represented by ISIS. Both this and the earlier successes of ISIS in Syria or Iraq and of the Taliban in Afghanistan are being propagandised by fundamentalists.

In Europe, on the other hand, jihadist activity quadrupled between October 2023 and early 2025, as Peter Neumann, a terrorism expert from King's College London, points out[15]. In Spain, for example, 81 suspected jihadists were arrested in 2024, including 25 in Catalonia. The number of people arrested on suspicion of jihadist activity increased in the country for the second year in a row and reached levels not seen since the terrorist attacks in Madrid in March 2004.

EU countries with a higher terrorist risk include those already frequently attacked, such as France, Italy, Spain or Germany, as well as others, such as Poland. Although the Europol report indicated no attempted attacks in Poland and only 1 arrest due to terrorist activity, this case is important, inter alia due to Poland's involvement in Ukraine. The increased level of this risk is also largely influenced by the accumulation of threats from both state terrorism inspired, for example, by Russia, Belarus or Iran, and non-state terrorism, which takes different forms: ethno-nationalist

[12] See e.g.: S. Wojciechowski, P. Osiewicz, *Zrozumieć współczesny terroryzm* (Eng. Understanding contemporary terrorism), Warszawa 2017.

[13] S. Wojciechowski, *History Repeats Itself. The Issue of Terrorism and Afghanistan on the Twentieth Anniversary of the 9/11 Attacks*, "Przegląd Strategiczny" 2021, no. 14, pp. 9–22. https://doi.org/10.14746/ps.2021.1.1.

[14] *Nineteenth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat*, United Nations Security Council, 31 VII 2024, https://docs.un.org/en/S/2024/583 [accessed: 6 II 2025].

[15] M. Auermann, F. Piatov, *Der IS-Terror ist zurück!*, Bild, 3 I 2025, https://www.bild.de/politik/ausland-und-internationales/top-experte-warnt-in-bild-der-is-terror-ist-zurueck-677687610195b908c1898f69 [accessed: 13 IV 2025].

and separatist, extreme left-wing and anarchist, Islamist, extreme right-wing. The increase in the terrorist threat in selected EU countries is also indicated by the *Global Terrorism Index 2025* published by the Institute for Economics & Peace. It shows that in 2024, the number of terrorist incidents in Europe doubled from the figures in the previous report – there were 67 incidents. These mainly affected 6 countries: Sweden, Finland, the Netherlands, Denmark, Switzerland and Germany. For some EU Member States, the terrorist threat score (Global Terrorism Index) also increased. The highest ranking – 27th – was for Germany, up 13 places from the previous report. This is followed by Greece in 36th place (down 1 place), the Czech Republic in 39th place (down 6 places), France in 40th place (down 2 places), Poland in 47th place (up 33 places) and Sweden in 50th place (up 22 places)[16].

Terrorist threat in the European Union in 2023 – analysis of the TE-SAT report

For the EU, one of the most important sources of information on the terrorist threat is Europol's annual *TE-SAT European Union Situation and Trend Report*. Its analysed version, published in December 2024, deals with data for 2023 and was prepared in cooperation with EU Member States and other partners involved in counter-terrorism. The report, with an introduction by Europol's Executive Director Catherine De Bolle, analyses the key trends currently affecting the phenomenon of terrorism. It provides information on, inter alia, attacks carried out, failed and foiled, the number of people arrested for terrorist activities, and ongoing legal proceedings. Different types of terrorism are covered, such as ethno-nationalist and separatist, left-wing and anarchist, jihadist and right-wing.

In 2023, as many as 120 terrorist attacks were recorded in the EU, including 98 carried out, 9 failed and 13 foiled. This compares to 18 attacks in 2021 and 28 in 2022, so there was a more than fourfold increase in 2023 compared to the previous year. These figures show that terrorism is an increasingly serious security threat to EU Member States.

[16] *Global Terrorism Index 2025*, Institute for Economics & Peace, https://www.economicsandpeace.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf [accessed: 4 V 2025].

Noteworthy is the large disproportion between the number of attacks carried out and foiled in 2023. This year, attacks involved 7 EU countries: France – 80, Italy – 30, Germany and Spain – 3 each, Belgium – 2, Greece and Luxembourg – 1 each. More than 90% of the cases therefore involved two countries – France and Italy. They also registered the highest number of attacks carried out, 72 and 23 respectively, with the remainder occurring in Belgium, Germany and Spain – 1 each. Unsuccessful attacks occurred in Italy – 7 and Greece and Spain – 1 each. In contrast, 8 attacks were foiled on French territory, 2 in Germany and 1 each in Belgium, Luxembourg and Spain. Most terrorist acts targeted critical infrastructure – 15 incidents, with the remainder targeting, among others, private companies – 7, civilians – 4 and police officers – 3. The most common form of attack was arson – 20, the others indicated: bombings – 8, destruction of property – 6, knife attacks – 6 and firearms – 5.

The phenomenon of terrorism in Europol reports is also considered in terms of the rate of people arrested on account of terrorist activities or prosecutions in this regard. For example, in 2023, law enforcement authorities in EU Member States arrested 426 people accused of terrorism-related offences. This compares to 380 in 2022 (Figure 1). The highest number of such cases was in 2023 in Spain, France, Belgium and Germany – more than 50 in each of these countries. However, there was a decrease in the number of court convictions, reported by Eurojust, with 358 convictions in 2023 compared to 427 in 2022. Court proceedings concluded in 2023 led to 290 convictions and 68 acquittals in 14 EU countries[17].

Terrorist attacks have long been carried out using a variety of means, from the use of a knife or a car through the use of firearms, explosives and even the so-called dirty bomb, to drone or cyber attacks. A significant increase has also been observed in the online acquisition of training materials, instructions on tactics and strategies for carrying out attacks, information on the manufacture of 3D-printed weapons, the military use of drones, the acquisition of firearms or explosives, and even the possibility of possessing chemical weapons. This includes people with different peeps and ideological affiliations that are difficult to attribute to a single trend, such as Islamist or far-right. Added to this is the issue of the use of artificial intelligence by terrorists or their sympathisers. The internet and cyber technologies, which are readily used by young people, remain an important

[17] Europol, *TE-SAT. European Union Terrorism Situation...*, p. 15.

tool used, for example, for propaganda, recruitment or fundraising purposes. They are also used to influence radicalisation and promote hate speech. This generates serious consequences, including the carrying out of attacks by increasingly younger attackers. During Christmas 2024, for example, German police arrested a 15-year-old terrorist who was planning an attack on a church in Berlin. The increasingly strong links within the triad: terrorist/terrorists – criminal groups – secret services of countries hostile to the EU should also be highlighted.

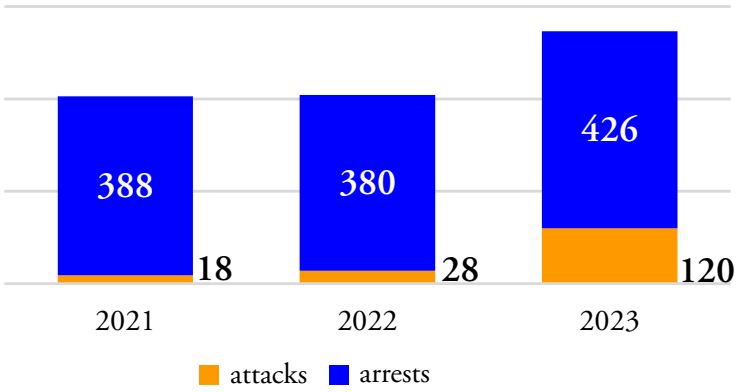


Figure 1. Number of terrorist attacks carried out, failed or foiled and persons arrested for terrorist activities in the European Union between 2021 and 2023.

Source: Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2024*, https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf, p. 11 [accessed: 9 II 2025].

The statistics confirm that terrorism remains a complex threat, encompassing different ideologies, forms or methods of action. The Europol report underlines that the phenomenon of terrorism in the EU stems from a variety of premises and does not have, as is still quite often erroneously believed, only an Islamist background (Table 1).

Table 1. Number of terrorist attacks carried out, failed or foiled in the EU in 2023 by motivation of the attackers.

COUNTRY/ terrorism type	JIHADIST	RIGHT-WING	LEFT-WING AND ANARCHIST	ETHNO-NATIONALIST AND SEPARATIST	OTHER	TOTAL
Belgium	2					2
France	8	1		70	1	80
Germany	3					3
Greece			1			1
Italy			30			30
Luxembourg		1				1
Spain	1		1		1	3
TOLAL	14	2	32	70	2	120

Source: Europol, *TE-SAT. European Union Terrorism Situation and Trend Report 2024*, https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%20 2024.pdf, p. 62 [accessed: 9 II 2025]. Changes have been made in the form of translation and graphic design – editor's note.

The report also mentions 2 incidents where the motivation of the assassins was not indicated. One of these was the shooting of a Spanish politician in Madrid on 9 November 2023 by an unidentified perpetrator. The reasons for his act are also unknown[18]. This act should be considered purely criminal, as recognising something as an act of terrorism requires knowing the real motives of the perpetrator.

Ethno-nationalist and separatist terrorism

By far the greatest terrorist activity was undertaken in 2023 by terrorists motivated by ethno-nationalist and separatist ideology[19]. During this period, 70 terrorist attacks of this nature were reported, all carried out in Corsica, France. Thirty-four, or almost half, occurred on the night of 8–9 October. The affiliation of those arrested in connection with terrorism motivated by ethno-nationalist and separatist ideology included the following terrorist organisations: the Corsican Fronte di Liberazione Naziunale Corsu (FLNC) and Ghjuventù clandestina Corsa (GcC), the Irish Dissident Republican, the Kurdish Partiya Karkerên Kurdistanê (PKK) and the Basque Euskadi ta Askatasuna (ETA). Detentions and arrests of those suspected of terrorist activity have also occurred in Italy, Sweden, Germany and Greece. Among the charges brought against those arrested were participation in terrorist plots, possession of weapons, financing of terrorism and recruitment as well as promotion of terrorist activity[20].

Extreme left-wing and anarchist terrorism

Extreme left-wing[21] and anarchist groups were significantly more active in the EU in 2023 compared to jihadist and far-right groups.

[18] Ibid., p. 55.

[19] The Europol report's characterisation of ethno-nationalist and separatist terrorist groups indicates that these groups appeal to nationalism or ethnic or religious affiliation as part of a political agenda. The aim of these groups is to create their own territory by separating from an already existing state or annexing the separated territory to another state. See: ibid., p. 51.

[20] Ibid., pp. 51–52.

[21] In the Europol report, terrorism by extreme left-wing groups (left-wing terrorism) is understood as the use of violence to provoke a violent Marxist-Leninist revolution against the democratic state with the aim of establishing socialism, communism or a classless society. Anarchist terrorism, on the other hand, aims to destroy the current model of political power and replace it with an anti-discriminatory and anti-capitalist model that promotes equality, freedom and social justice. See: ibid., p. 43.

Their members were responsible for 32 terrorist incidents, 23 of which resulted in the carrying out of terrorist attacks. All of them were carried out in Italy. It was also mainly in this country that the attacks were foiled – 7, and in Greece and Spain – 1 each. According to figures published by the anarchists themselves, most of the attacks were carried out as a gesture of solidarity with the Informal Anarchist Federation/ International Revolutionary Front (IAF/FAI) members imprisoned by the Italian authorities. The anarchist attack in Spain was also in support of those imprisoned in Italy. The modus operandi of the attackers did not differ from that of previous years and included the use of improvised explosive devices (IED), which were detonated near mobile phone masts or other infrastructure of telecommunications and energy companies, as well as arson or physical destruction of mainly real estate. The attacks were justified with anti-capitalist slogans (criticism of the increasingly powerful role of corporations in the Italian economy), anti-state and anti-war (including opposition to NATO)[22], criticism of the growing techno-industrial domination of modern powers (state and non-state), the worsening economic situation (including rising inflation), the rise in popularity of neo-fascist groups, disrespect for worker' and migrants' rights as well as the climate crisis and increasing repression by state structures. In view of this, it is not surprising that state officials, including police officers and members of the judiciary, were also targets of attacks. The Italian authorities only managed to arrest 10 people from this very active terrorist group. The others were arrested in Spain – 1, Germany – 1 and Greece – 2. They were mostly men between the ages of 27 and 75. There was also 1 woman arrested[23]. Some of those detained were affiliated with the Turkish DHKP-C (The Revolutionary People's Liberation Party/ Front, Turkish: Devrimci Halk Kurtulus Partisi-Cephesi)[24]. Terrorists associated with leftist and anarchist ideology obtained funds for their activities in a manner similar to the previously discussed groups, i.e. using both legal and illegal sources.

[22] Ibid., p. 46.

[23] Ibid., pp. 45–48.

[24] Ibid., pp. 47–48.

Jihadist terrorism

In the EU, terrorist activity undertaken by jihadists increased in 2023 compared to the previous year[25]. On the territory of France, Belgium, Germany and Spain, terrorists with such links carried out or attempted to carry out 14 attacks. As a result, 6 people were killed and 12 injured in them. The modus operandi of the perpetrators included the activity of so-called lone wolves loosely linked to existing terrorist groups[26]. The perpetrators of the attacks were exclusively men, who killed their victims most often by stabbing. Only once, in the case of an attack in Brussels, firearms were used. The attacks took place in urban areas. The figure also includes 9 terrorist plots that were detected in advance: most in France – 6, as well as in Germany – 2 and Belgium – 1[27]. An interesting phenomenon is the lack of clear links between the perpetrators and existing terrorist groups. Police services were only able to confirm the link between the bombers and ISIS in 4 cases, and only for 1 did ISIS take full responsibility[28]. The existence of an extensive jihadist terrorist network within the EU[29] can be evidenced by the arrest of 334 people by law enforcement authorities. This number is up 68 from 266 in the previous year. Of those arrested, 133 did not have the nationality of an EU country. The vast majority

[25] In the Europol report, jihadism is defined as a radical strand of Salafism (a Sunni Muslim revivalist movement) whose adherents reject modern democracy, arguing that man-made legislation contradicts God's status as the sole lawgiver. Jihadists aim to create an Islamic state governed exclusively by Islamic law (sharia). Unlike other Salafist currents, jihadists legitimise the use of violence by referring to Islamic doctrines of jihad (this term literally means 'striving' or 'effort', but jihadists interpret it as religiously sanctioned war). All those who oppose jihadist interpretations of Islamic law are considered enemies of Islam and therefore become legitimate targets for attack. Some jihadists include Shiites and other Muslims among their enemies. See: Europol, *TE-SAT. European Union Terrorism Situation…*, p. 20. The issue of jihadist terrorism is described in more detail in this article than other types of terrorism in the EU due to the particular impact of such terrorist incidents on law enforcement tasks in recent years.

[26] On the subject of lone wolves, see in more detail: A. Wejkszner, *Samotne wilki kalifatu? Państwo Islamskie i indywidualny terroryzm dżihadystyczny w Europie Zachodniej* (Eng. Lone wolves of the caliphate? The Islamic State and individual jihadist terrorism in Western Europe), Warszawa 2018, pp. 27–47.

[27] Europol, *TE-SAT. European Union Terrorism Situation…*, p. 20.

[28] Ibid.

[29] On this subject, see in more detail: A. Wejkszner, *Europejska armia kalifatu. Tom 1. Centrum supersieci* (Eng. The European Army of the Caliphate. Volume 1. The centre of the supernetwork), Warszawa 2020, pp. 30–48.

of those arrested (276 people) were men. Those arrested were charged with belonging to a terrorist organisation – 30%, planning or carrying out an attack – 14%, financing terrorist activities – 12%[30]. Court proceedings in 208 cases resulted in convictions. Most of those convicted came from Belgium, France, Germany and Austria. Their terrorist affiliations, if confirmed, included the networks of the 2 largest and competing jihadist terrorist organisations operating on EU territory, i.e. ISIS and Al-Qaeda. Despite the loss of influence by both groups in the Middle East, they were able to increase their presence in Europe. In this case, it is not the expansion of organisational structures, but the popularisation of jihadist ideology that has resulted in the terrorist radicalisation of many young people. Moreover, this process has been shortened and intensified, and its participants are prepared to use violence against civilians[31]. This means the persistence of the threat from individual jihadist terrorism[32]. Additional threats in the form of jihadist radicalisation in prisons, the low effectiveness of the deradicalisation process and the return of so-called foreign fighters (or foreign terrorist fighters) to EU territory (often using false identity documents) have also not been avoided[33]. These processes were reinforced by jihadist propaganda undertaken primarily in the dark web[34]. Among the most common narrative threads there were the growing oppression of Muslims in Europe, the lack of response to insulting the Quran in Sweden, Denmark or the Netherlands, the glorification of Hamas terrorist activity, especially after the 7 October 2023 attack on Israel, and support for the growing polarisation in the Middle East and the anticipated religious war between Muslims and Jews or representatives of other religious groups. There have been open calls to attack symbolic targets, such as places of worship.

[30] Europol, *TE-SAT. European Union Terrorism Situation...*, p. 23.

[31] Ibid., p. 25.

[32] See: I.J. Sandboe, M. Obaidi, *Imagined Extremist Communities: The Paradox of the Community-Driven Lone-Actor Terrorist*, "Perspectives on Terrorism" 2023, vol. 17, no. 4, pp. 19–41. https://doi.org/10.19165/CAQH8148.

[33] See: A. Wejkszner, *Państwo Islamskie. Narodziny nowego kalifatu?* (Eng. Islamic State. The birth of a new caliphate?), Warszawa 2016, pp. 164–169.

[34] Europol, *TE-SAT. European Union Terrorism Situation...*, pp. 27–28.

Extreme right-wing terrorism

Terrorism by far-right groups[35] in the EU posed the least threat in 2023, far less than jihadist terrorism. During this period, there was attempted violence motivated by far-right ideology once in France and once in Luxembourg. Such motivation was mainly characterised by individual terrorists not belonging to any known terrorist organisation. A total of 26 people were arrested accused of involvement in terrorist activities motivated by far-right ideology, including 5 in the Netherlands and 4 each in France and Belgium. They were exclusively men, almost always citizens of the country in which they were arrested. Their targets were minorities of all kinds (religious or sexual). Their main weapons of choice were firearms, most of them legally acquired – which was unusual for terrorists motivated by other ideologies – as well as white weapons and IEDs. Police reports indicated that the way to obtain firearms, such as the FGC-9 semi-automatic carbine[36], was through the use of modern technologies such as 3D printers[37]. The popularity of terrorism motivated by far-right ideology can also be seen in the number of people convicted – 35, which increased compared to the previous year. The radicalisation of the views of those with far-right views was influenced by neo-fascist, eco-fascist, racist, anti-Semitic or accelerationist slogans promoted both online and offline. Slogans with a misogynist or incel background were slightly less frequent. It was also characteristic to reinforce the narrative through the use of many

[35] The authors of the Europol report understand the term 'right-wing terrorism' as the use of violence to transform the contemporary political, social and economic system into an authoritarian model in which democratic values and institutions would be rejected. Right-wing ideologies referring to this model use a violent narrative focused on nationalism, racism, xenophobia or other expressions of intolerance. The basic concept of right-wing extremism is the supremacy of the nation or race. In practice, this means that some element characterising a particular group causes these individuals to consider themselves superior to others and thus have a natural right to dominate the rest of the population. Right-wing extremist ideologies also popularise ideas such as misogyny, hostility towards the LGBTQ+ community and anti-immigration attitudes that oppose the diversity of society and the equal rights of minorities. See: Europol, *TE-SAT. European Union Terrorism Situation…*, p. 34.

[36] A weapon designed by a German of Kurdish origin nicknamed JStark. The abbreviation FGC-9 comes from the words "Fuck Gun Control 9 millimeter". The carbine is powered by 9x19 mm ammunition. See more: P. Juraszek, *Broń z drukarki 3D w Birmie. Zaprojektował ją Niemiec* (Eng. A weapon from a 3D printer in Burma. It was designed by a German), WP Tech, 18 XII 2021, https://tech.wp.pl/bron-z-drukarki-3d-w-birmie-zaprojektowal-ja-niemiec,6716336908528512a [accessed: 25 III 2025].

[37] Europol, *TE-SAT. European Union Terrorism Situation…*, p. 37.

conspiracy theories, especially the Jewish conspiracy thread[38]. Participation in terrorist action was intended as a way for right-wing extremists to gain notoriety. Both private and public property was targeted, specific individuals, electoral commissions, opposition party headquarters were attacked, and refugee centres were also set on fire. The far-right terrorists raised funds for their activities by organising weapons training and by accepting contributions, including in cryptocurrencies. Many of them had a criminal past, which made it easier for them to raise funds from illegal sources such as drug and firearms trafficking[39].

Summary

1. According to Europol reports, the number of terrorist attacks increased from 18 to 120 incidents between 2021 and 2023.
2. The 2024 Europol report points out that the phenomenon of terrorism in the EU stems from a variety of reasons and is not only Islamist in origin. The different types of terrorist threats cover only a subset of EU Member States. The country where terrorist attacks appeared to be most diverse in terms of the motivation of the attackers was France.
3. Terrorist threats on EU territory in 2023 had a negative impact on both individual and national security in at least 7 Member States. In two of these, France and Italy, this threat was particularly high.
4. The operational and propaganda offensive accompanying the resurgence of ISIS will gradually intensify in different parts of the world. This is due to a number of determinants, including the success of the opposition in Syria, including its Islamist strands. One of the regions at greater risk from Islamist terrorism is the EU. Countries at higher risk include those that have been frequently attacked so far, as well as others, such as Poland.
5. Although this Europol report does not indicate any attempted attacks and only one case of arrest due to terrorist activity

[38] Ibid., pp. 38–39.

[39] Ibid., p. 41. On the evolution of various forms of modern terrorism, see: M. Ingelevič-Citak, Z. Przyszlak, *Jihadist, Far Right and Far Left Terrorism in Cyberspace. Same Threat and Same Countermeasures?*, "International Comparative Jurisprudence" 2020, vol. 6, no. 2, pp. 154–177. https://doi.org/10.13165/j.icj.2020.12.005.

in Poland, the case of Poland is important due to the accumulation of threats from both state terrorism (inspired, for example, by Russia, Belarus or Iran) and non-state terrorism, taking different forms.

6. An analysis of the political motivation of the terrorist attack perpetrators in the EU indicates that most of them are related to the demands of extremist organisations. Separatist views predominate in this respect, e.g. within the long-standing socio-political conflicts in Corsica or the Basque Country.
7. An interesting issue is the modus operandi of the perpetrators which is similar for most terrorist attacks. This includes the use of the most common tools and techniques, including firearms, knives, explosives or arson.
8. The European Union needs a new approach to perceiving terrorism and combating it effectively. This is important because of the escalation and evolution of this threat, which includes the possibility for perpetrators to use, inter alia, firearms smuggled en masse from the Balkans or Ukraine, as well as modern solutions such as drones, firearms manufactured in 3D technology, artificial intelligence, etc. Also of concern are the increasingly strong links within the triad: terrorist/terrorists – criminal groups – special services of countries hostile to the EU.
9. Effective countering of the terrorist threat must be achieved not only through in-depth cooperation (intelligence, logistics, legal, political, etc.) between all EU Member States, but also through extended cooperation with NATO and other allies in different parts of the world. The aim is to build multi-faceted resilience in external and internal dimensions. This requires effective prevention of other challenges as well, as identified e.g. in the reports by Mario Draghi[40] or Sauli Niinistö[41].

[40] M. Draghi, *The future of European competitiveness*, European Commission, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf [accessed: 4 II 2025].

[41] S. Niinistö, *Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness*, European Union, 26 XI 2024, https://civil-protection-knowledge-network.europa.eu/media/safer-together-strengthening-europes-civilian-and-military-preparedness-and-readiness [accessed: 8 II 2025].

10. Effective implementation of counter-terrorism plans may be threatened by the vested interests of individual EU Member States, the ongoing political crisis in some of them, the rift in transatlantic relations, the lack of financial resources or the increasingly announced economic meltdown.

Bibliography

Gunaratna R., *Global Terrorism Threat Forecast 2025*, "RSIS Commentary" 2025, no. 002.

Ingelevič-Citak M., Przyszlak Z., *Jihadist, Far Right and Far Left Terrorism in Cyberspace. Same Threat and Same Countermeasures?*, "International Comparative Jurisprudence" 2020, vol. 6, no. 2, pp. 154–177. https://doi.org/10.13165/j.icj.2020.12.005.

Maniszewska K., *Towards a New Definition of Terrorism: Challenges and Perspectives in a Shifting Paradigm*, series: Contributions to Security and Defence Studies, Cham 2024. https://doi.org/10.1007/978-3-031-58719-1.

Sandboe I.J., Obaidi M., *Imagined Extremist Communities: The Paradox of the Community-Driven Lone-Actor Terrorist*, "Perspectives on Terrorism" 2023, vol. 17, no. 4, pp. 19–41. https://doi.org/10.19165/CAQH8148.

The Routledge Companion to Terrorism Studies. New Perspectives and Topics, M. Abrahms (ed.), London 2024.

Wejkszner A., *Europejska armia kalifatu. Tom 1. Centrum supersieci* (Eng. The European army of the caliphate. Vol. 1. The centre of the super-network) Warszawa 2020.

Wejkszner A., *Państwo Islamskie. Narodziny nowego kalifatu?* (Eng. Islamic State. The birth of a new caliphate?), Warszawa 2016.

Wejkszner A., *Samotne wilki kalifatu? Państwo Islamskie i indywidualny terroryzm dżihadystyczny w Europie Zachodniej* (Eng. Lone wolves of the caliphate? The Islamic State and individual jihadist terrorism in Western Europe), Warszawa 2018.

Wojciechowski S., *History Repeats Itself. The Issue of Terrorism and Afghanistan on the Twentieth Anniversary of the 9/11 Attacks*, "Przegląd Strategiczny" 2021, no. 14, pp. 7–21. https://doi.org/10.14746/ps.2021.1.1.

Wojciechowski S., *Reasons of Contemporary Terrorism. An Analysis of Main Determinants*, in: *Radicalism and Terrorism in the 21st Century. Implications for Security*, A. Sroka, F. Castro-Rial Garrone, R.D. Torres Kumbrián (eds.), Frankfurt am Main 2017.

Wojciechowski S., *The Hybridity of Terrorism: Understanding Contemporary Terrorism*, Berlin 2013.

Wojciechowski S., Osiewicz P., *Zrozumieć współczesny terroryzm* (Eng. Understanding contemporary terrorism), Warszawa 2017.

Internet sources

Auermann M., Piatov F., *Der IS-Terror ist zurück!*, Bild, 3 I 2025, https://www.bild.de/politik/ausland-und-internationales/top-experte-warnt-in-bild-der-is-terror-ist-zurueck-677687610195b908c1898f69 [accessed: 13 IV 2025].

Global Terrorism Index 2025, Institute for Economics & Peace, https://www.economicsandpeace.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf [accessed: 4 V 2025].

Gowan R., *Overview, 2. Trends in armed conflicts*, in: *SIPRI Yearbook 2024*, Stockholm International Peace Research Institute, https://www.sipri.org/yearbook/2024/02 [accessed: 5 II 2025].

Hoffmann I., De Vries C.E., *Old Habits Die Hard – Member States Report. Part II: Remaking the Transatlantic Partnership: Public Opinion in the EU and seven Member States*, Eupinions, 20 XI 2024, https://eupinions.eu/de/text/old-habits-die-hard-member-states-report [accessed: 15 III 2025].

Juraszek P., *Broń z drukarki 3D w Birmie. Zaprojektował ją Niemiec* (Eng. A weapon from a 3D printer in Burma. It was designed by a German), WP Tech, 18 XII 2021, https://tech.wp.pl/bron-z-drukarki-3d-w-birmie-zaprojektowal-ja-niemiec,6716336908528512a [accessed: 25 III 2025].

Security Council debates growing terrorism threat in Africa, United Nations, 21 I 2025, https://news.un.org/en/story/2025/01/1159246 [accessed: 8 II 2025].

U.S. Africa Command Civilian Casualty Assessment Report; 2nd Quarter, FY2024, https://www.africom.mil/what-we-do/airstrikes/civilian-harm-report/us-africa-command-civilian-casualty-assessment-report-2nd-quarter-fy2024 [accessed: 14 IV 2025].

Other documents

Draghi M., *The future of European competitiveness*, European Commission, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf [accessed: 4 II 2025].

Europol, *TE-SAT. European Union Terrorism Situation and Trend. Report 2024*, https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf [accessed: 9 II 2025].

Niinistö S., *Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness*, European Union, 26 XI 2024, https://civil-protection-knowledge-network.europa.eu/media/safer-together-strengthening-europes-civilian-and-military-preparedness-and-readiness [accessed: 8 II 2025].

Nineteenth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat, United Nations Security Council, 31 VII 2024, https://docs.un.org/en/S/2024/583 [accessed: 6 II 2025].

The Global Risks Report 2021. 16th Edition. Insight Report, World Economic Forum, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf [accessed: 7 II 2025].

The Global Risks Report 2022. 17th Edition. Insight Report, World Economic Forum, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf [accessed: 12 V 2025].

The Global Risks Report 2025. 20th Edition. Insight Report, World Economic Forum, https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf [accessed: 6 II 2025].

Sebastian Wojciechowski, Professor

Head of the Department of Strategic Studies and International Security at the Faculty of Political Science and Journalism of Adam Mickiewicz University in Poznań. Chief analyst at the Institute for Western Affairs in Poznań. Expert on security issues, including

terrorism, of the Organization for Security and Cooperation in Europe. Editor-in chief of "Przegląd Strategiczny". Recipient of two scholarships from the Foundation for Polish Science and the US State Department. Winner of the scientific award of the Prime Minister of the Republic of Poland and the scientific award funded by the European Union. Member of, among others: the Commission on Balkan Studies of the Polish Academy of Sciences, the Scientific Board of the Terrorism Research Center at Collegium Civitas. Author of many expert opinions and analyses prepared for Polish and foreign institutions, as well as publications in the field of international relations and internal and international security. He is also NATO DEEP eAcademy security expert.

Contact: sebastian.wojciechowski@amu.edu.pl

Assoc. Prof. Artur Wejkszner, Professor at the Adam Mickiewicz University

Political scientist, professor in the Department of Strategic Studies and International Security at the Faculty of Political Science and Journalism of Adam Mickiewicz University in Poznań. Author of dozens of publications on contemporary international relations and the issues of international terrorism and Islamic radicalism, including a two-volume monograph entitled *Europejska armia kalifatu* (Eng. The European Army of the Caliphate).

Contact: artur.wejkszner@amu.edu.pl

Terrorism – Studies, Analyses, Prevention, 2025, no. 7: 327–380

https://doi.org/10.4467/27204383TER.25.036.21813

Article

Commentary on the amendment of the Act on anti-terrorist activities in relation to countering the dissemination of terrorist content on the internet

MARIUSZ CICHOMSKI

https://orcid.org/0000-0003-3707-7856

Ministry of the Interior and Administration
Republic of Poland

Abstract

The article is a commentary on the *Act of 10 June 2016 on anti-terrorist activities* in terms of the provisions introduced to this regulation by the *Act of 18 October 2024 amending the Act on anti-terrorist activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency*. The purpose of the introduced provisions is to ensure the application in the Polish legal order of the *Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online*. The author recalled previous amendments to the Act on anti-terrorist activities and discussed the basic solutions contained in Regulation 2021/784 concerning hosting providers – orders to remove terrorist content and special measures, i.e. issuing decisions on hosting providers exposed to terrorist content.

Keywords

terrorism, internet content blocking, the act on anti-terrorist activities, terrorist content, hosting provider, content provider

Introduction. Amendments to the Act on anti-terrorist activities to date

By the *Act of 18 October 2024 amending the Act on anti-terrorist activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency*, the application of the *Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online* (hereinafter: Regulation 2021/784), was ensured in the Polish legal order, which was implemented through the amendment of the *Act of 10 June 2016 on anti-terrorist activities* (hereinafter: AT Act). By the Regulation of 18 October 2024, the *Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency* (hereinafter: the Act on the ABW and the AW) was also amended, complementing the implementation of the *Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA* (hereinafter: Directive 2017/541).

This was the first such significant change to the AT Act since its enactment in 2016, i.e. after nearly nine years in force. This change consisted both in broadening the scope of the regulation's normative subject matter and extending it to new categories of addressees. The previous amendments, although their number (12) may seem relatively high were of an adjusting, correcting or streamlining nature from the perspective of the mechanisms implemented earlier, and did not introduce new legal institutions significantly changing the scope of its application.

In five cases the changes concerned the inclusion of an entity that came into being as a result of the transformation of another entity after the entry into force of the original version of the AT Act. These were: the establishment of the National Revenue Administration in place of the fragmented structures of the Ministry of Finance, in particular the Customs Service, fiscal control, tax intelligence and tax administration[1], transformation of the Government Protection Bureau into the State Protection Service[2], change of the status of the Marshal Guard into a state uniformed service with the adjustment of its tasks[3], inclusion

[1] *Act of 16 November 2016 – Provisions introducing the Act on the National Revenue Administration*. The article presents the legal status as of 23 II 2025.

[2] *Act of 8 December 2017 on the State Protection Service*.

[3] *Act of 26 January 2018 – Provisions introducing the Act on the Marshal' s Guard*.

of the General Inspector of Financial Information[4], previously omitted as a result of the changed status, or statutory assignment to the National Prosecutor the tasks hitherto belonging to the Prosecutor General[5].

The next group of amendments consists of three cases of changes related to the coherence with other emerging or changing laws, in order to maintain the legislative compatibility of references or terminological correctness. In this way, the amendments introduced by the *Act of 6 March 2018 – Entrepreneurs Law*, the *Act of 21 January 2021 on foreign service* and the *Act of 11 March 2022 on defence of the homeland* should be read.

The last group of changes consists of four amendments which, although of substantive importance, remained fragmentary in nature and were intended to streamline or correct the existing provisions from the perspective of the practice of law application. Thus, by the *Act of 12 March 2022 on assistance to Ukrainian citizens in connection with the armed conflict on the territory of the country*, Art. 13 of the AT Act, which regulates issues related to the establishment of temporary radio communication installations and the construction, reconstruction or installation of cable infrastructure and other equipment or infrastructure to the extent necessary for the launch and proper operation of such installations, was made more precise. In addition, Art. 13a was added to the AT Act, according to which the Prime Minister, taking into account the possibility of a terrorist incident or a threat to public safety and order, may, by order, restrict public access to lists, registers, databases and ICT systems containing location data of technical infrastructure.

By the *Act of 7 July 2023 on amending the Act on the protection of shipping and seaports and certain other acts* a correction regarding the scope was made to Art. 24 of the AT Act by including the Polish exclusive economic zone as an area in which anti-terrorist activities may be carried out. According to the new wording of the provision, anti-terrorist activities under the principles set out in this Act may be carried out outside the borders of the Republic of Poland, in waters within the Polish SAR (search and rescue) area of responsibility, in accordance with the *International Convention on Maritime Search and Rescue, drawn up at Hamburg on 27 April 1979* and in the Polish exclusive economic zone. Similarly, the emergency services may carry out operations to deal with the consequences of a terrorist incident and, in this

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

[5] *Act of 7 July 2023 amending the Civil Procedure Code, the Law on the System of Common Courts, the Criminal Procedure Code and certain other acts.*

respect, shall cooperate with each other and with the services carrying out anti-terrorist activities in the aforementioned areas. In its original version, this provision limited the area of operation to the SAR area of responsibility.

Another amendment was introduced by the *Act of 17 August 2023 amending the Act – Criminal Code and certain other acts* and it concerned, in the author's opinion, the two provisions of the AT Act that were the most controversial from a constitutional perspective. The first amendment modified Art. 9 of the Act, which provides the basis for the Head of the Internal Security Agency (hereinafter: Head of the ABW) to carry out operational control in relation to foreigners for the purpose of identifying, preventing, combating and detecting terrorist offences and prosecuting their perpetrators. This provision was expanded to include an additional premise, i.e. the offence of espionage[6]. The second change concerned Art. 26(2) – the maximum period of pre-trial detention under this law was extended to 30 days. It should be emphasised that the changes introduced assumed an increase in the possibility of practical application of the aforementioned provisions. However, their aim was not to make changes that could minimise constitutional doubts[7].

A slightly larger range of changes was made to the AT Act by the *Act of 26 July 2024 on amending certain acts to improve the activities of the Armed Forces of the Republic of Poland, the Police and the Border Guard in the event of a threat to state security*. However, these changes did not create new legal institutions. Instead, their aim was to improve the functionality of the previous solutions by introducing the possibility of communicating an opinion on the appropriateness of introducing, abolishing or changing the alert level also orally, by telephone, or by means of electronic

[6] In this context, it is worth recalling, first of all, the Judgement of the European Court of Human Rights (ECHR) in the case Pietrzak v. Poland and Bychawska-Siniarska and Others v. Poland, in which the ECHR held that there had been a violation of Art. 8 of the *Convention for the Protection of Human Rights and Fundamental Freedoms* in connection with the way the system of operational control was shaped in Poland. The ECHR noted that, with regard to operational control under the AT Act, neither the introduction of covert surveillance nor its application during the initial three-month period is subject to any control by an independent body external to the officers of the Internal Security Agency (ABW) carrying out this surveillance. See: Judgement of the European Court of Human Rights in the case Pietrzak v. Poland and Bychawska-Siniarska and Others v. Poland, https://arch-bip.ms.gov.pl/pl/prawa-czlowieka/europejski-trybunal-praw-czlowieka/orzecznictwo-europejskiego-trybunalu--praw-czlowieka/listByYear,2.html?ComplainantYear=2024 [accessed: 18 V 2025].

[7] See in more detail: M. Gabriel-Węglowski, *Działania antyterrorystyczne. Komentarz* (Eng. Anti-terrorist activities. Commentary), Warszawa 2018, pp. 36, 76–116, 213–214, 224–229.

communication (Art. 16 of the AT Act)[8]. An analogous solution has also been adopted for the transmission of a request to mobilise assistance to the Police from the Polish Armed Forces (Art. 22 of the AT Act). The provisions have also been aligned with the *Act of 6 April 1990 on the Police* by indicating that soldiers of branches and subdivisions of the Special Forces used to assist branches and subdivisions of the Police are entitled, to the extent necessary for the performance of their tasks, to the rights of the Police officers, and the exercise of these rights takes place on the principles and in the manner specified for Police officers (also Art. 22 of the AT Act).

The need to provide a Polish framework for the application of Regulation 2021/784

To begin with, it is worth asking whether ensuring the application of Regulation 2021/784 required amendments at the statutory level and, if so, whether this could have been done on the basis of regulations other than the AT Act. The limited framework of the study does not allow for a comprehensive commentary on the individual provisions of Regulation 2021/784, and therefore, for the purposes of this article, only a synthetic discussion of the main legal instruments introduced by this regulation to prevent the dissemination of terrorist content on the internet has been made. The commentary to the individual provisions discusses the basic regulations of Regulation 2021/784 in relation to Polish solutions, as well as the issue of the choice, on national grounds, of the authority competent to fulfil obligations under Regulation 2021/784, taking into account institutional solutions adopted in other EU states. Furthermore, the procedures for issuing and challenging orders under the aforementioned regulation are described.

As mentioned in the introduction, the Act amending the AT Act and the Act on the ABW and the AW also completed the earlier implementation of Directive 2017/541. It should be emphasised, that while the application of Regulation 2021/784 was ensured by the amendment of the AT Act, the transposition of Directive 2017/541 was ensured by the amendment of the Act on the ABW and the AW. Combining in a single legislative interference the implementation of these two pieces of EU law should

[8] This issue as a de lege ferenda postulate was pointed out in: M. Cichomski, I. Idzikowska-Ślęzak, *Alert levels – practical and legal dimensions of their use*, "Terrorism – Studies, Analyses, Prevention" no. 2, pp. 251–252. https://doi.org/10.4467/27204383TER.22.025.16345.

be assessed as an optimal solution, although the two regulations, despite the convergence of the areas they cover related to the removal and blocking of online content, have a different scope of application and do not overlap.

Regulation 2021/784 came into force on 7 June 2021 and Member States had to adapt their regulations to it within one year. This is the first comprehensive piece of direct-application legislation at EU level to regulate against the dissemination of terrorist content online. However, it was preceded by other initiatives. For instance, a framework for voluntary cooperation between Member States and hosting providers was introduced in 2015. At its meeting on 22–23 June 2017, the European Council, in response to the terrorist attacks that have taken place in EU countries and the associated propaganda spread on the internet, stated that it:

> "expects industry to [...] develop new technology and tools to improve the automatic detection and removal of content that incites to terrorist acts". In its Resolution of 15 June 2017 the European Parliament called on these online platforms "to strengthen measures to combat illegal and harmful content". The call for companies to take a more proactive approach when it comes to protecting their users from terrorist content was echoed by Member State ministers at the EU Internet Forum[9].

On 28 September 2017 the European Commission (EC) adopted a Communication providing guidance on the obligations of online service providers with regard to illegal content on the internet[10]. It then issued a *Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online*, which set out specific recommendations on terrorist content in Chapter 3. The Recommendation followed the European Parliament's call to strengthen measures against illegal and harmful content on the internet, in line with the horizontal framework established by *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, and in

[9] Recital 5 of *Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online*.

[10] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms*, Brussels, 28 IX 2017, COM(2017) 555 final.

response to calls from the European Council to improve the detection and removal of content on the internet that incites terrorist acts.

The next step was the adoption of Regulation 2021/784. According to the EC it is worth to notice that: *The regulatory framework to address illegal content online was further strengthened with the entry into force of the Digital Services Act on 16 November 2022. The Digital Services Act regulates the obligations of digital services that act as intermediaries in their role of connecting consumers with content, services and goods, thereby better protecting users online and contributing to a safer online environment*[11]. Under this act, the EC has gained supervisory and enforcement powers to take action against large online platforms and search engines. Among other things, it can target information requests and investigate companies' content moderation activities, with the possibility of imposing fines.

The primary motive for issuing Regulation 2021/784 was to ensure the smooth functioning of the digital single market in an open and democratic society by countering the use of hosting services for terrorist purposes and contributing to the improvement of public security across the Union[12]. The EU also aimed to improve the functioning of the digital single market by increasing legal certainty for hosting providers and user trust in the online environment, as well as strengthening guarantees on freedom of expression, including the freedom to receive and impart information and ideas in an open and democratic society as well as media freedom and pluralism. The EU legislator has recognised that online hosting providers play a key role in the digital economy by connecting businesses and citizens and facilitating public debate as well as distribution and receipt of information, opinions and ideas, which clearly contributes to innovation, economic growth and job creation in the Union[13]. In this context, it is pointed out that it is not the hosting providers that may pose a threat in terms of spreading terrorist content, but their services that may be used by third parties for this purpose. It is noted, however, that it is the hosting providers, due to their technical

[11] *Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online,* 14 II 2024, COM(2024) 64 final, p. 1.

[12] Recital 1 of the Regulation 2021/784. This issue was also addressed in: the *Government draft of the Act amending the Act on anti-terrorist activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency* – explanatory memorandum, print no. 661, p. 1, https://www.sejm.gov.pl/Sejm10.nsf/druk.xsp?nr=661 [accessed: 24 XII 2024].

[13] Recital 4 of the Regulation 2021/784.

capacity, that have particular obligations towards the public to protect their services from terrorist use and to assist in countering the dissemination of this type of content online[14]. All the more so because: *Of particular concern is the misuse of those services by terrorist groups and their supporters to disseminate terrorist content online in order to spread their message, to radicalise and recruit followers, and to facilitate and direct terrorist activity*[15].

If, however, the rules for preventing and responding to the publication of terrorist content are regulated at the level of an EU regulation, i.e. an act of law directly applicable in all Member States, the question is whether there was a possibility of measures of intervention by public authorities alternative to the enactment of a law, in view of § 1(1) point 3 of the *Regulation of the Prime Minister of 20 June 2002 on "the Principles of Legislative Techniques"* (hereinafter: Principles of legislative techniques). In this case, the answer is simple. Art. 291(1) of the *Treaty on the Functioning of the European Union* requires Member States to take all measures of national law necessary to implement legally binding Union acts. In turn, the second sentence of Art. 4(3) of the *Treaty on European Union* indicates that Member States shall take any general or specific measures appropriate to ensure fulfilment of the obligations arising out of the treaties or resulting from the acts of the EU institutions. Moreover, Regulation 2021/784 itself already obliges states to take specific actions requiring legislative interference. For example, Art. 12 obliges Member States to designate competent authorities for issuing content removal orders or specific preventive measures. On the other hand, from a national perspective, in connection with Art. 7 of the *Constitution of the Republic of Poland of 2 April 1997*, the definition of the competence of the authorities is a statutory norm, and public authorities act on the basis and within the limits of the law (legality principle). Therefore, the need for statutory solutions in this respect is not in doubt.

The second general issue concerning ensuring the application of Regulation 2021/784 in Polish law remains whether it was rightly done by adding provisions to the AT Act and whether there were other possible solutions. In the context of these considerations, it will be helpful to briefly analyse the current state of the law in the area covered by the regulation and, therefore, to fulfil the obligation referred to in

[14] Recital 5 of the Regulation 2021/784.

[15] Recital 4 sentence 3 of the Regulation 2021/784.

§ 1(1) point 2 of the aforementioned Principles of legislative techniques prior to the drafting of the legislative act.

The explanatory memorandum to the Act amending the AT Act and the Act on the ABW and the AW, indicates that the subject matter of Regulation 2021/784 is currently partly covered by national regulation, which does not fully implement Directive 2017/541 in force in this area[16]. Indeed, under its Art. 21, Member States are obliged to put in place measures that will ensure, as a matter of priority, the immediate removal of internet content inciting to commit a terrorist offence hosted on servers in their territory. Under Art. 21(1) of the Directive, states are also to take action to have such content located on servers outside their territory removed. Only if removal of such content is not possible may Member States take measures to block access to it (Art. 21(2) of the Directive). Polish legislation, on the other hand, only provides for content blocking, which, in the EC's view, is not sufficient to consider the implementation correct. There is a lack of a basic mechanism to remove such content from websites in the first place. In fact, there are provisions in the Act on the ABW and the AW, according to which the Head of the ABW, with the approval of the court, may cause a so-called blocking of the availability on the internet of certain data linked to a terrorist event. Pursuant to Art. 32c of this Act, the court may order the blocking of the availability in an ICT system of certain IT data or ICT services that are linked to a terrorist incident or that make the commission of an offence of espionage plausible. It may do so upon the written request of the Head of the ABW made with the written approval of the National Prosecutor. The blocking of the availability of ICT data shall be ordered for a period of no more than 30 days with the possibility of judicial extension for a period of no more than three months. The law also provides for a simplified procedure for urgent cases[17]. In its position, the EC states that:

> Polish law does not provide for measures to ensure the immediate removal of such online content, in particular when such content is hosted on servers within Poland. Although this may vary in some individual cases, there is no reason to believe that removal of content at source would generally be impracticable. Art. 21(2) cannot be understood as a reason for a Member State not to transpose Art. 21(1).

[16] *Government draft of the Act amending the Act...*– explanatory memorandum, p. 4.

[17] Ibid.

> Indeed, under the Directive, Member States are required to transpose both provisions, so that it is possible to remove content under Art. 21(1) as a general rule and to block access under Art. 21(2) if removal is not practicable in individual cases[18].

It should also be noted that the provisions of Directive 2017/541 have not been repealed by Regulation 2021/784, which means that the two acts are complementary and should be applied in parallel. *Regulation 2021/784 imposes obligations to remove terrorist content only on hosting providers not imposing such obligations on other providers of electronic services, including, for example, so-called caching services, which are to be understood as services consisting in the automatic and short-term storage of someone else's data on an intermediary server by creating a copy of it in order to make it available to the end user more quickly*[19].

Furthermore, Directive 2017/541, unlike Regulation 2021/784, does not link terrorist content with the public nature of its dissemination as a prerequisite for being able to issue an order to remove content or block access to it. On the basis of the Directive, it is therefore possible to seek the removal of content, e.g. in restricted internet forums.

As a result, although the indicated provision of the Act on the ABW and the AW addresses the issue of blocking content on the internet, it cannot be equated with the regulatory obligations to ensure the application of Regulation 2021/784. Accordingly, Art. 32c of the Act on the ABW and the AW has been retained, but a modification has been made according to which this provision applies in cases of publication or attempted publication of terrorist content on the internet by entities that are not hosting providers within the meaning of Regulation 2021/784.

However, since the existing regulations were in the Act on the ABW and the AW, it is worth considering whether the new regulations, coinciding thematically, should also be in this Act. In the author's opinion, a positive answer to this question raises significant doubts. Indeed, ensuring the application of Regulation 2021/784 requires the designation of a competent authority on the side of the Member State. If, in the case of Poland, it was decided that it would be the Head of the ABW, this designation could be made in the pragmatic law defining the tasks and powers of this service and its organs,

[18] *European Commission's position on 9 June 2021* (ref. no. INFR(2021)2046, C(2021)3630 final), p. 7; *Government draft of the Act amending the Act…* – explanatory memorandum, p. 15.

[19] *Government draft of the Act amending the Act…* – explanatory memorandum, p. 14.

i.e. the Act on the ABW and the AW. However, the range of matters delegated by the EU legislator to be regulated at national level is much broader. Indeed, Regulation 2021/784 defines not only the sphere of action of the competent authorities, but also the rights, including the right to challenge decisions of state authorities, and the obligations of hosting providers and content providers, as well as the system and level of penalties that may be imposed on them. This is therefore well beyond the sphere that can be normalised in a pragmatic law for a particular formation. Pragmatic laws should not, although this currently happens, regulate the rights and obligations of others. Furthermore, in the author's view, the current positioning of the provisions of Art. 32c of the Act on the ABW and the AW should be regarded as legislatively questionable. These provisions were introduced by amending provisions as part of the original text of the AT Act in 2016, so the legislature could already have included them in the act. Another decision was probably dictated by the fact that the construction of the provisions in the procedural dimension is similar to the legal institution of operational control regulated in Art. 27 of the Act on the ABW and the AW (analogous to the pragmatic laws of other services authorised to conduct it, e.g. in Art. 19 of the Act on the Police). Thus, it is not the provisions ensuring the application of Regulation 2021/784 that should be included in the Act on the ABW and the AW, but conversely, it is the existing provisions related to the blocking of content included in this act that could ultimately be included in the AT Act. As an aside, it is worth noting, that this observation also applies to Art. 32a–32b of the Act on the ABW and the AW concerning the conduct of security assessments of ICT systems of public administration bodies and critical infrastructure operators, as well as warning systems by the Internal Security Agency (ABW).

Another argument confirming the correctness of the approach to the provisions related to Regulation 2021/784 is provided by § 2 of the Principles of legislative techniques, pursuant to which the act should comprehensively regulate a given area of matters and not leave important fragments of this area outside the scope of its regulation. In the context related to the issue of threats of a terrorist nature, the basic regulation is the AT Act and it is the act which, as a rule, should contain the matters related to this issue. This argument is pertinent also with regard to the second potential alternative location of the provisions for the application of Regulation 2021/784, i.e. to regulate this issue in a new separate regulation.

As an aside, it is worth noting that, for analogous reasons, the provisions of the current *Act of 13 April 2016 on the security of trading in explosives*

precursors, which serves to apply *Regulation (EU) No 98/2013 of the European Parliament and of the Council of 15 January 2013 on the marketing and use of explosives precursors,* could be incorporated into the AT Act. The Regulation was issued in the wake of the attacks by Norwegian extremist Anders Breivik on the Norwegian Prime Minister's residence and on participants in the Norwegian Labour Party's youth camp[20].

Basic solutions included in Regulation 2021/784 in relation to countering the dissemination of terrorist content on the internet – removal orders and specific measures

In the context of the commentary to the individual provisions of the AT Act, numerous references to the provisions and recitals of Regulation 2021/784 are necessary, but they serve to interpret the individual provisions of Polish law. However, a synthetic presentation of the basic instruments for preventing the dissemination of terrorist content on the internet introduced by Regulation 2021/784 is necessary. Enabling their application in Poland is the goal of activities at the level of the national legislator.

For the purposes of this study, two basic mechanisms can be distinguished for countering the dissemination of mentioned content on the internet:

- issuing orders requiring hosting providers to remove terrorist content or prevent access to terrorist content in all Member States, in accordance with Art. 3 of Regulation 2021/784 (hereinafter: removal orders);
- issuing decisions on hosting providers exposed to terrorist content, based on Art. 5 of Regulation 2021/784 (hereinafter: specific measures).

These two mentioned instruments are matched by a number of additional powers and procedural rules, as well as mechanisms and

[20] See in more detail: M. Cichomski, P. Marchliński, *Krajowe rozwiązania w zakresie bezpieczeństwa obrotu prekursorami materiałów wybuchowych – po zamachu terrorystycznym w Norwegii 22 lipca 2011 r. w kontekście nowych zadań Policji* (Eng. National security arrangements in the trade in explosives precursors – after the terrorist attack in Norway on 22 July 2011 in the context of new police tasks), in: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (eds.), Szczytno 2016, pp. 591–600.

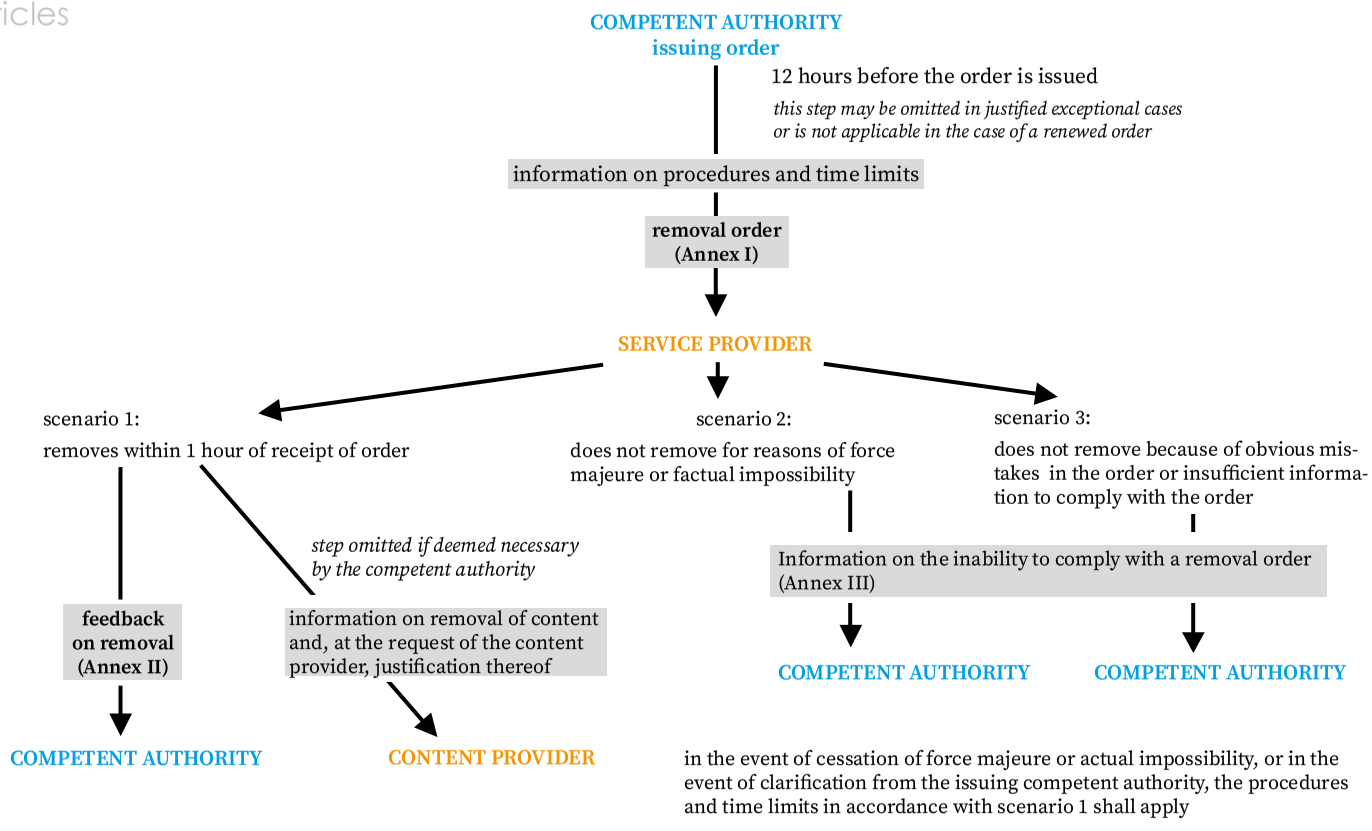
tools for cooperation between EU states, the EC and the European Union Agency for Law Enforcement Cooperation, or Europol, as well as hosting providers (schemes 1 and 2).

The first of the instruments mentioned above – the removal order – implies that the competent authority of each Member State has the power to issue a removal order obliging hosting providers to remove terrorist content or to prevent access to terrorist content in all Member States. Following the order, the hosting providers shall remove or disable access to the content in all Member States as soon as possible, no later than one hour after receipt of the removal order.

The orders are issued on a standardised form and contain such information as: the identification of the competent authority issuing the order, the grounds for the order, the exact standardised format for addressing the resource (URL address) and, if necessary, additional information to identify terrorist content or information on the legal remedies available to the hosting provider and the content provider. The hosting providers shall then inform the competent authority of the execution of the order – indicating in particular the time of removal or disabling access to the content (a model removal order is set out in Annex I to Regulation 2021/784).

If such an order is being issued for the first time in respect of a particular hosting provider, it shall be preceded by the provision of information to that provider on the applicable procedures and time limits at least 12 hours prior to the issuing of the removal order. This obligation may be omitted in particularly justified cases.

If the hosting provider is unable to comply with the order due to force majeure or actual impossibility attributable to it, including technical or operational reasons which can be objectively justified, the hosting provider shall inform the competent authority which issued the order and the one-hour time limit for removing the content or blocking access to it shall start to run as soon as the aforementioned reasons cease to exist. If, on the other hand, the hosting provider is unable to comply with the order because it contains errors or does not contain sufficient information to comply with it, the hosting provider shall inform the competent authority which issued the removal order. In this case, the time limit starts to run as soon as the hosting provider has received the necessary clarifications. The order shall become final either after the expiry of the time limit for lodging an appeal, where it was not lodged in accordance with national law, or as a result of the maintenance of the removal order following an appeal.



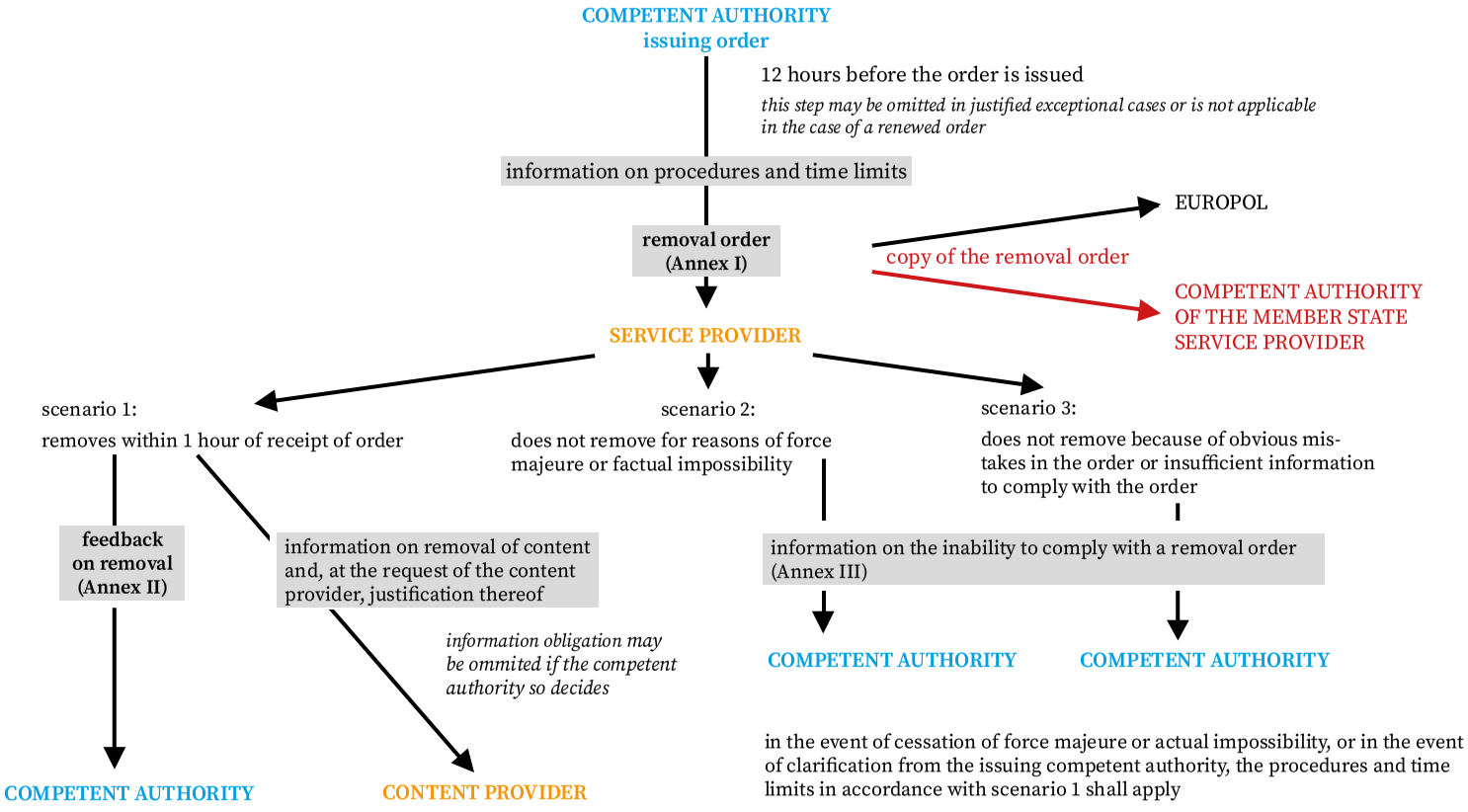
Scheme 1. Procedure for the imposition of a removal order of terrorist content where the main organisational unit or legal representative of the hosting provider is located in the same Member State as the competent authority issuing the order.

Source: study by Aneta Suda, *Mechanisms for blocking terrorist content on the internet in the light of Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online*, presentation by the Ministry of Internal Affairs and Administration prepared for the Interministerial Team for Terrorist Threats.

Mention should be made of the mechanism for verifying removal orders issued by the competent authorities of other Member States and identifying possible infringements in this respect (Art. 4 of Regulation 2021/784). This is the so-called cross-border removal procedure (scheme 3). According to this solution, in the event that the hosting provider does not have a main establishment or a legal representative in the Member State of the competent authority that issued the order, this authority shall transmit a copy of the removal order to the competent authority of the Member State in which the hosting provider has its main establishment or in which its legal representative is resident or established.

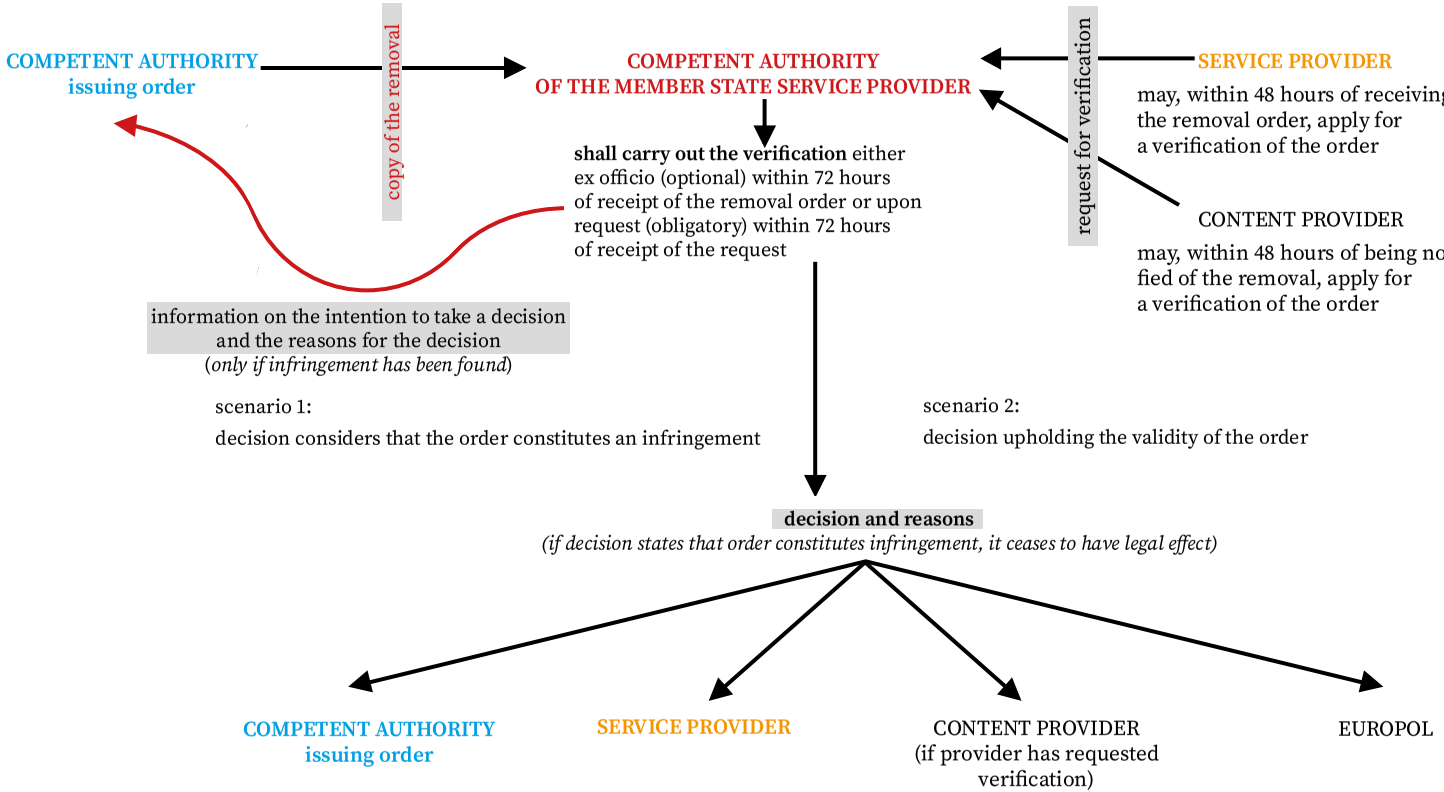
The competent authority of the Member State in which the hosting provider has its main establishment or in which its legal representative is resident or established may, on its own initiative, within 72 hours of receipt of a copy of that order, review it in order to establish that it does not seriously or manifestly infringe the legal grounds for issuing it or fundamental rights and freedoms. If such an infringement is found, it shall take a reasoned decision on the matter within the same time limit.

Hosting providers and content providers also have the possibility to initiate a verification action – within 48 hours of receiving the order, they can request a verification to the competent authority of the Member State where the hosting provider has its main establishment or where its legal representative is resident or established. This verification shall be carried out within 72 hours of receipt of the request. As a result, the competent authority shall take a decision, the issuing of which shall be preceded by communication to the issuing authority of its intention to do so. When a decision is taken, it shall immediately notify the competent authority which issued the removal order, the hosting provider, the content provider which requested the review and Europol of the decision. Where it is determined that a removal order constitutes an infringement, it shall cease to have legal effect and the hosting provider shall immediately restore the content in question or access to it.



Scheme 2. Procedure for the imposition of an order for the removal of terrorist content where the main organisational unit or legal representative of the hosting provider is not located in the same Member State as the competent authority issuing the order.

Source: Study by Aneta Suda, *Mechanisms for blocking terrorist content on the internet in the light of Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online*, presentation by the Ministry of Internal Affairs and Administration prepared for the Interministerial Team for Terrorist Threats.



Scheme 3. Procedure for the imposition of a cross-border removal order.

Source: Study by Aneta Suda, *Mechanisms for blocking terrorist content on the internet in the light of Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online*, presentation by the Ministry of Internal Affairs and Administration prepared for the Interministerial Team for Terrorist Threats.

The second main mechanism identified for preventing and responding to the dissemination of terrorist content on the internet (specific measures) is the issuing of decisions on hosting providers exposed to terrorist content and the supervision of their implementation of specific measures.

Explaining the *ratio legis* of this solution, the EU legislator pointed out that:

> With a view to reducing the accessibility of terrorist content on their services, hosting service providers exposed to terrorist content should put in place specific measures taking into account the risks and level of exposure to terrorist content as well as the effects on the rights of third parties and the public interest to information. Hosting service providers should determine what appropriate, effective and proportionate specific measure should be put in place to identify and remove terrorist content. Specific measures could include appropriate technical or operational measures or capacities such as staffing or technical means to identify and expeditiously remove or disable access to terrorist content, mechanisms for users to report or flag alleged terrorist content, or any other measures the hosting service provider considers appropriate and effective to address the availability of terrorist content on its services[21].

A hosting provider recognised as a provider exposed to terrorist content shall include in its contractual terms as well as apply provisions to counter the use of its services for the public dissemination of terrorist content and shall take specific measures to this end. These may include, for example:

- technical and operational means or capabilities, such as appropriate personnel or technical means for the purpose of identifying and promptly removing or preventing access to terrorist content;
- easily accessible and user-friendly mechanisms for users to report or flag alleged terrorist content to the hosting provider;
- other mechanisms to raise the awareness of the availability of terrorist content on its services, such as mechanisms to moderate users;
- other measures that the hosting provider considers appropriate to counter the availability of terrorist content on its services.

[21] Recital 22 of the Regulation 2021/784.

The premise is that the specific measures are intended to effectively reduce the level of exposure of the hosting provider's services to terrorist content, to be targeted and proportionate, and to be applied in a careful and non-discriminatory manner, taking into account full respect for the rights and legitimate interests of users.

A hosting provider should be deemed to be exposed to terrorist content where the competent authority of the Member State in which the hosting provider has its main establishment or in which its legal representative is resident or established has decided that the provider is exposed to terrorist content. This decision should be taken on the basis of objective factors, such as the receipt by the provider of at least two final removal orders of such content in the last 12 months.

Upon receipt of the decision, the hosting provider shall, within three months, notify the competent authority of the specific measures it has taken or intends to take to ensure compliance with its obligations. Thereafter, once a year, the hosting provider shall draw up a report on their implementation.

If the competent authority considers that the specific measures taken do not comply with the requirements, it shall address a decision to the hosting provider requiring it to take the necessary measures. The hosting provider may choose which type of specific measures it will take. It may also, at any time, request the competent authority to review and, where appropriate, amend or revoke its decision to designate it as a hosting provider exposed to terrorist content.

To conclude this part of the article, it is worth recalling some statistics on the application of Regulation 2021/784 until 31 December 2023[22]. According to the EC's findings, Member States have issued 349 removal orders of terrorist content. This option was used by the competent authorities of six Member States, i.e. Spain – 62 orders, Romania – 2 orders, France – 26 orders, Germany – 249 orders (all issued after the attack carried out by Hamas on 7 October 2023), Czech Republic – 2 orders, Austria – 8 orders. The orders were addressed to the following entities, among others: Telegram, Meta, JustPaste.it, TikTok, DATA ROOM S.R.L., FlokiNET S.R.L., Archive.org, SoundCloud, X, Jumpshare, KrakenFiles.com, Top4toP and Catbox.

[22] Based on the *Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784...*

Out of 349 removal orders issued, only in 10 cases did the hosting provider fail to remove the terrorist content or block it within the maximum deadline, i.e. within one hour of receiving the order. In only one case did the hosting provider state that it was impossible to comply with the order.

No order was subject to the review in the cross-border removal order procedure. Consequently, there was no case recorded stating that the issued order made such a violation.

To date, no hosting provider has been identified as being exposed to terrorist content and therefore no provider has been required to implement special measures.

Noteworthy, no order issued has been challenged in court to date.

Commentary on specific provisions of the AT Act in relation to the prevention of the dissemination of terrorist content on the internet

Two groups of provisions were introduced into the AT Act by the Act amending the AT Act and the Act on the ABW and the AW. The first is the expansion of the statutory vocabulary contained in Art. 2 of the amended Act to include three definitions, each of which includes a reference to Regulation 2021/784. The second group of provisions is covered by a new unit of statutory systematisation labelled as Chapter 5a – countering the dissemination of terrorist content on the internet. It contains six provisions related to the designation of the competent authority on the national side, procedural provisions and provisions specifying administrative penalties, i.e. legal norms directly ensuring the application of Regulation 2021/784. Moreover, the title of the Act was supplemented with a reference to this regulation.

The next part of the article is a commentary on the individual provisions.

Art. 1. The Act of 10 June 2016 on anti-terrorist activities (Journal of Laws of 2024, item 92 and 1248) is amended as follows:

1) The following reference is added to the title of the Act:

"1) This Act serves to apply the Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Official Journal of the EU L 172 of 17.05.2021, p. 79)".

By supplementing the title of the AT Act with a reference to the application of Regulation 2021/784, the obligation under § 19a(2) of the Principles of legislative techniques was fulfilled. According to it, in the case of a law the enactment of which is linked to the issuance or validity of a directly applicable normative act established by an EU institution, the specification of the subject matter of the law shall be followed by a reference to the title of the law indicating the normative act with which the law is linked, which is expressed in particular by the phrase, "this law serves to apply... [title of the act]".

> 2) In Art. 2 point 7, the full stop shall be replaced by a semicolon and the following points 8–10 shall be added:
> [whenever the Act refers to:]
> "8) hosting service provider – means a service provider of services consisting in storing information provided by and at the request of a content provider, as referred to in Art. 2(1) of the Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Official Journal of the EU L 172 of 17.05.2021, p. 79), hereinafter referred to as "Regulation 2021/784"; (…)

According to Art. 2 point 1 of Regulation 2021/784 'hosting service provider' means a provider of services (as defined in letter (b) of Art. 1 of *Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services)*, storing information provided by and at the request of a content provider. According to the Directive, 'service' means any information society service, that is to say any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. Except that 'at a distance' means that the service is provided without the simultaneous presence of the parties. 'By electronic means' means that the service is sent and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and which is entirely transmitted, conveyed and received by wire, radio waves, optical or other electromagnetic means. 'At the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.

It is worth noting recital 13 of the cited regulation, according to which:

> In order to effectively address the dissemination of terrorist content online, while ensuring respect for the private life of individuals, this Regulation should apply to providers of information society services which store and disseminate to the public information and material provided by a user of the service on request, irrespective of whether the storing and dissemination to the public of such information and material is of a mere technical, automatic and passive nature. The concept of 'storage' should be understood as holding data in the memory of a physical or virtual server. Providers of 'mere conduit' or 'caching' services, as well as of other services provided in other layers of the internet infrastructure, which do not involve storage, such as registries and registrars, as well as providers of DNS (domain name systems), payment or DDoS (distributed 'denial of service' attack) protection services, should therefore fall outside the scope of this Regulation.

Regulation 2021/784 extended its scope to hosting providers offering services in the EU, i.e. enabling natural or legal persons, in one or more Member States, to use services of a hosting provider who has a substantial link with the Member State, either by virtue of having an establishment in the Union or by virtue of specific factual criteria, such as having a significant number of users of its services in one or more Member States or directing its activities towards one or more Member States (Art. 2 points 4 and 5 of the Regulation). This offering of services must be carried out to the extent that the hosting providers disseminate information to the public (Art. 1(2) of the Regulation), regardless of the location of their main organisational unit, i.e. their head office or registered office, where the main financial functions are performed and operational control is exercised (Art. 2 point 9 of the Regulation). However, it should be borne in mind that where access to information requires registration or admission to a group of users – under Art. 2 point 3 and Recital 14 of the Regulation – this information should only be considered publicly disseminated if users seeking access to the information are automatically registered or admitted to a group of users, without the need for a human decision as to whom to grant such access.

In order to ensure a workable application of the Regulation with regard to hosting providers, an obligation has been introduced under Art. 17 of Regulation 2021/784 whereby, if the provider does not have a main establishment in the EU, the provider shall designate in writing

a natural or legal person as its legal representative in the Union for the purpose of receiving, complying with and implementing removal orders and decisions issued by the competent authorities. Furthermore, the provider shall delegate to its legal representative the necessary powers and resources to comply with those removal orders and decisions and to cooperate with the competent authorities. The hosting provider shall notify the appointment of the legal representative to the competent authority of the Member State in which its legal representative is resident or established and shall make information on the legal representative publicly available. The legal representative may be held liable for infringements of this Regulation, without prejudice to the hosting provider's liability and legal action against the hosting provider.

In the author's opinion, the aforementioned issue is of key importance to the efficiency of application of Regulation 2021/784 itself from the perspective of the effectiveness of removal or blocking of terrorist content. Indeed, in contrast to solutions adopted at the level of individual states, including the mechanisms in force in Poland set out in the Act on the ABW and AW, it can be effectively applied to content posted at a hosting provider located outside a given state. An analogous opinion was expressed by the EC:

> While voluntary measures and non-binding recommendations contributed to reduce the availability of terrorist content online, limitations including the small number of hosting service providers adopting voluntary mechanisms[23] as well as the fragmentation of procedural rules across Member States limited the effectiveness and the efficiency of cooperation among Member States and hosting service providers and made it necessary to establish regulatory measures[24]. Therefore, the effective application of the Regulation is key to address the dissemination of terrorist content online. The Commission has proactively supported national competent authorities in this process[25].

[23] *Commission Staff Working Document Impact Assessment. Accompanying the document. Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online*, Brussels, 12 IX 2018, SWD(2018) 408 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN [accessed: 4 V 2023].

[24] Ibid.

[25] *Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784...*, p. 4.

9) in Art. 2 in point 7, the full stop shall be replaced by a semicolon and the following points 8–10 shall be added: […]
[whenever the Act refers to:]
"9) content provider – it shall mean the user referred to in Art. 2 point 2 of the Regulation 2021/784;"

According to Art. 2 point 2 of Regulation 2021/784 a 'content provider' means a user that has provided information that is, or that has been, stored and publicly disseminated by a hosting provider; In turn 'public dissemination' means the making available of information, at the request of a content provider, to a potentially unlimited number of persons (Art. 2 point 3 of Regulation 2021/784).

While the EU legislator clearly emphasises the socially and economically crucial role of hosting providers as connectors between businesses and citizens establishing a space for public debate or exchange of information, and whose activities can be used by third parties to transmit terrorist content, it is explicitly indicated with regard to the content provider that it bears editorial responsibility for its activities.

2) in Art. 2 in point 7, the full stop shall be replaced by a semicolon and the following points 8–10 shall be added: […]
[whenever the Act refers to:]
10) terrorist content – means the materials referred to in the Art. 2 point 7 of the Regulation 2021/784.

According to Art. 2 point 7 of Regulation 2021/784 terrorist content means material that:

- incites the commission of one of the offences referred to in Art. 3(1) letters (a)–(i) of Directive (EU) 2017/541 (indicated below), where such material, directly or indirectly, for instance, by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed;
- induces a person or a group of persons to commit or to contribute to the commission of one of the following offences within the meaning of Directive 2017/541;
- solicits a person or a group of persons to participate in the activities of a terrorist group;

– provides instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques for the purpose of committing or contributing to the commission of one of the following offences within the meaning of Directive 2017/541;
– constitutes a threat of committing one of the following offences within the meaning of Directive 2017/541.

According to Art. 3(1) letters (a)–(j) of Directive 2017/541, terrorist offences are intentional acts, defined under Polish law as offences which, by their nature or context, are capable of causing serious damage to a State or an international organisation and have been committed with a specific purpose. They are:

a) attacks upon a person's life which may cause death;
b) attacks upon the physical integrity of a person;
c) kidnapping or hostage taking;
d) causing extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;
e) seizure of aircraft, ship or other means of public or goods transport;
f) manufacture, possession, acquisition, transport, supply or use of explosives or weapons, including chemical, biological, radiological or nuclear weapons, as well as research into, and development of such weapons;
g) release of dangerous substances, or causing fires, floods or explosions, the effect of which is to endanger human life;
h) interfering with or disrupting the supply of water, power or any other fundamental natural resource, the effect of which is to endanger human life;
i) illegal interference with systems, as referred to in Art. 4 of Directive of the European Parliament and of the Council 2013/40/EU (1), where Art. 9(3) or Art. 9(4) letter (b) or (c) of this Directive applies, and unlawful interference with data, as referred to in Art. 5 of that Directive, in cases where Art. 9(4) letter (c) of that Directive applies[26];

[26] According to Art. 4 and 5 of the *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council*

j) threatening to commit any of the acts listed.

According to Art. 3(2) of Directive 2017/541, the indicated categories of offences are terrorist offences if committed with the aim of:

- serious intimidation the population;
- unlawful compelling a government or an international organisation to take or refrain from taking some action;
- serious destabilisation or destruction of the fundamental political, constitutional, economic or social structures of the state or international organisation concerned.

The cited definition, in principle, corresponds to the definition of a terrorist offence in Art. 115 § 20 of the *Act of 6 June 1997 Criminal Code*, according to which a terrorist offence is a criminal act punishable by imprisonment of at least 5 years, committed with the aim of:

1) seriously intimidating a number of persons,
2) forcing a public authority of the Republic of Poland or of another state or an authority of an international organisation to take or to refrain from taking a specific action,
3) causing serious disturbances in the system or economy of the Republic of Poland, another state or an international organisation,

- as well as a threat to commit such an act.

However, the Polish definition, contrary to the definition in Directive 2017/541, does not specify the types of underlying offences, but only defines them by indicating that their upper limit is at least 5 years. As an aside, it is worth noting that this dissimilarity has been pointed out as a lack of proper implementation of the Directive[27], but on the other hand it provides flexibility in the application of the national regulation.

In the context of the application of Regulation 2021/784 and the safeguarding against possible abuse, it is most important that the disclosure of terrorist content is properly assessed. Recital 11

Framework Decision 2005/222/JHA, unlawful interference with information systems consists of inputting computer data, transmitting, damaging, deleting, deteriorating, altering or suppressing such data or rendering such data inaccessible. Unlawful data interference, on the other hand, is the intentional and unlawful deleting, damaging, deteriorating, altering or suppressing computer data on an information system or rendering such data inaccessible.

[27] This issue was raised, inter alia, during a visit to Poland by the United Nations Counter-Terrorism Committee Executive Directorate (UN CTED), to evaluate Poland's implementation of UN Security Council resolutions on counter-terrorism.

of that Regulation provides guidance in this regard. According to it, in view of the need to counter the most harmful terrorist propaganda on the internet, the definition of terrorist content should include:

> (...) material that incites or solicits someone to commit, or to contribute to the commission of, terrorist offences, solicits someone to participate in activities of a terrorist group, or glorifies terrorist activities including by disseminating material depicting a terrorist attack. The definition should also include material that provides instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, as well as chemical, biological, radiological and nuclear (CBRN) substances, or on other specific methods or techniques, including the selection of targets, for the purpose of committing or contributing to the commission of terrorist offences. Such material includes text, images, sound recordings and videos, as well as live transmissions of terrorist offences, that cause a danger of further such offences being committed.

The remainder of this recital of Regulation 2021/784 indicates that, in assessing whether material constitutes terrorist content, competent authorities and hosting providers should take into account factors such as the nature and content of the communications, the context in which the communications are presented and the extent to which the communications are likely to result in effects detrimental to the safety and security of persons. However, an important limitation is formulated in this recital. According to it, an important factor in this assessment is that the material in question has been produced by a person, group or entity on the EU list of persons, groups and entities involved in terrorist acts and subject to restrictive measures, that it is attributable to such a person, group or entity, or that it is disseminated on behalf of such a person, group or entity. On the one hand, this is intended to ensure freedom of speech and opinion, but on the other hand, when interpreted literally and not purposefully, it constitutes narrowing the content in question to a link to persons, groups or entities on the EU list of persons, groups and entities involved in terrorist acts. Indeed, not every provider of such content can explicitly demonstrate such a link.

By contrast, Art. 1(3) of Regulation 2021/784 explicitly indicates that material publicly disseminated for educational, journalistic, artistic or research purposes, or for the prevention or combating of terrorism, including material intended to express polemical or controversial views in

the context of a public debate, shall not be deemed to be terrorist content. Moreover, it is to be determined by means of an assessment what the actual purpose of the dissemination of the content in question is. It is worth mentioning in this context Recital 12 of Regulation 2021/784. According to it, in determining whether material provided by a content provider constitutes 'terrorist content', particular consideration should be given to the right to freedom of expression and information, including freedom and pluralism of the media, and freedom of the arts and sciences.

From a legislative perspective, it is worth noting the structural consistency of the terminology used in the Criminal Code, the AT Act and Regulation 2021/784. The indicated legal acts use the terms 'terrorist offence', 'terrorist event' and 'terrorist content' respectively. However, not all Polish legal acts include them. For example, the Act on the ABW and the AW refers to the 'crime of terrorism'.

> Art. 26a. The Head of the ABW is the competent authority within the meaning of Regulation 2021/784.

In analysing the scope of the indicated jurisdiction, attention should be drawn at the outset to the previously mentioned Art. 12 of Regulation 2021/784, according to which each Member State shall designate the authority or authorities competent to:

- issue orders requiring hosting providers to remove terrorist content or prevent access to terrorist content in all Member States (removal order),
- verify removal orders issued by the competent authorities of other Member States and to identify possible infringements in this respect (procedure for cross-border removal orders),
- supervise the implementation of specific measures by the hosting provider,
- impose penalties for breaching the provisions of the regulation in question.

The above indication does not exhaust all the obligations and powers imposed on the competent authorities by other provisions of Regulation 2021/784. In this respect, it is possible to point out, inter alia, the following:

- extending the period of retention of terrorist content that has been removed or to which access has been prevented, as a result of a removal order (Art. 6(2) of Regulation 2021/784),

- issuing decisions on hosting providers exposed to terrorist content and to supervise their implementation of specific measures, based on Art. 5 of Regulation 2021/784,
- carrying out cooperation, including the exchange of information, with other competent authorities established by the other Member States, Europol and hosting providers, in accordance with Art. 14 of Regulation 2021/784,
- publication of the report, pursuant to Art. 8 of Regulation 2021/784,
- transmission of annual information to the EC on the basis of Art. 21 of Regulation 2021/784.

In the aforementioned Art. 12 of Regulation 2021/784, the EU legislator provided for the possibility of designating various authorities as the competent authorities for the exercise of the indicated powers and duties. The Polish legislator did not use this possibility and designated the Head of the ABW as the only authority competent on national grounds. This solution seems to be optimal and is in line with the entirety of the national norms in this respect, in connection with which at least four aspects should be noted. Firstly, the Head of the ABW under Art. 3(1) of the AT Act is responsible for the prevention of terrorist incidents[28]. Secondly, on the basis of Art. 5(1) point 1 of the Act on the ABW and the AW, the tasks of this formation include, inter alia, the identification, detection and prevention of terrorist offences, and terrorist content is largely used to carry out terrorist attacks. Thirdly, the Head of the ABW had already been given the authority to block terrorist content under the provisions of the Act on the ABW and the AW. Fourthly, the ABW also has an organisational structure in the form of the Counter-Terrorism Centre of the Internal Security Agency, fully equipped for this purpose, operating on a 24/7 basis.

According to Recital 35 of Regulation 2021/784, Member States should be able to decide on the number of competent authorities to be designated and whether they should be administrative, law enforcement or judicial authorities. These authorities must carry out their tasks in an objective and non-discriminatory manner and should not seek instructions from any other authority in relation to the performance of the tasks assigned to them under this Regulation. Importantly, however, this should not preclude the exercise of supervision in accordance with national constitutional law.

[28] See in more detail: P. Burczaniuk, *Tasks and powers of criminal law enforcement authorities in combating terrorism in Poland – a legal perspective*, "Terrorism – Studies, Analyses, Prevention" 2022, no. 2, pp. 9–30. https://doi.org/10.4467/27204383TER.22.024.16344.

Pursuant to Art. 12(4) of Regulation 2021/784, the EC has set up and keeps up to date an online register containing a list of the competent authorities in each country and their contact points designated or established pursuant to Art. 12(2) of the Regulation, referred to later in the commentary to Art. 26b of the AT Act[29]. According to the register published on the EC website, on the day the Polish Parliament adopted content blocking solutions, 25 out of 27 EU Member States provided such information (notifications were not made by Slovenia and Portugal)[30]. Out of this group, 13 countries designated the competent authority – similarly to Poland – from among services of a police or specialised character, four countries indicated the competence of an organisational unit functioning within the Ministry of Interior and the same number of countries in other central offices, e.g. in the case of Hungary – the National Media and Infocommunications (Nemzeti Média- és Hírközlési Hatóság), in Austria it is the Communications Authority (Kommunikationsbehörde Austria). In two countries it is the prosecuting authority and in one the court has jurisdiction[31].

The decision of the Polish legislator, i.e. to designate the Head of ABW as the competent authority, is in line with EU guidelines and does not deviate from the solutions adopted in other countries, but the practice in this respect differs.

> Art. 26b. 1. The Head of the ABW shall designate a contact point within the ABW as referred to in Art. 12(2) of Regulation 2021/784, operating on a 24/7 basis.
> 2. Information on the seat and contact details of the contact point referred to in paragraph 1, as well as on how to submit requests for clarification and feedback on removal orders obliging hosting providers to remove terrorist content or prevent access to terrorist content, hereinafter referred to as 'removal orders', shall be made available in the Bulletin of Public Information on the webpage of the ABW.

[29] *List of national competent authority (authorities) and contact points,* European Commission, 27 I 2025, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online/list-national-competent-authority-authorities-and-contact-points_en?prefLang=pl [accessed: 15 II 2025].

[30] As of 23 II 2025, the only country that had not made a notification was Portugal.

[31] See in more details: *Government draft of the Act amending the Act…*

Art. 12(2) of Regulation 2021/784 requires Member States to ensure that a contact point is designated or established within the authority competent for issuing removal orders to deal with requests for clarification and feedback on such orders. In Poland, the consequence of the choice of the Head of the ABW as the competent authority was that he designated a contact point within the Agency he heads. Member States were also obliged to ensure that information on the contact point was publicly available.

It is worth noting that the Polish legislator has extended the minimum scope of information to be included on the webpage in line with the requirements under Regulation 2021/784. In addition to information on the contact point, the webpage must also contain information on how to submit requests for clarification and feedback on removal orders. According to the notice on the webpage of the ABW:

> Requests for clarification on removal orders obliging hosting providers to remove terrorist content or to prevent access to terrorist content, submitted using the model set out in Annex III to Regulation 2021/784, may be addressed in hard copy to the postal address of the contact point or in electronic form to the e-mail address of the contact point. Feedback after the removal or disabling of access to terrorist content, submitted using the model set out in Annex II to Regulation 2021/784, will be provided in the same form[32].

It should be noted that the contact point is only for the hosting providers affected by the removal order. The ABW does not operate a general portal for reporting illegal content on the internet.

Art. 26c. 1. The Head of the ABW shall supervise the implementation of the specific measures referred to in Art. 5(1)–(3) of Regulation 2021/784 by:

1) reviewing the specific measures taken by the hosting provider, including their compliance with Art. 5(2) and (3) of Regulation 2021/784;
2) issuing written recommendations to the hosting provider to remedy the anomalies identified and to bring its operations into line with Regulation 2021/784.

2. An authorised officer of the ABW, when carrying out the activities referred to in paragraph 1, has the right to:

[32] *Punkt kontaktowy TCO* (Eng. Contact point TCO), BIP ABW, https://bip.abw.gov.pl/bip/punkt-kontatowy-tco/525,Punkt-kontaktowy-TCO.html [accessed: 13 XII 2024].

1) enter the controlled premises used for the provision of hosting services;
2) demand explanations from the hosting provider and make available the technical and operational documentation resulting from the application of specific measures or to inspect such documentation.

3. The hosting provider exposed to terrorist content shall remedy the breaches of the law and irregularities identified in the supervision by the Head of the ABW within the timeframe specified in the written recommendation.

Allowing a hosting provider to be subject to specific measures by declaring it vulnerable to terrorist content is linked to the obligation of states to ensure effective oversight functions by competent authorities. As indicated earlier, the safeguards implemented by the hosting provider may relate to appropriate technical and operational measures to enable users to report terrorist content, as well as other mechanisms to raise awareness among content viewers. If, on the other hand, the competent authority considers that the specific measures taken are not compliant, it shall address a decision to the hosting provider requiring it to take the necessary complementary or corrective measures.

To ensure the application of these provisions, it was necessary to indicate that the Head of the ABW shall supervise the implementation of the special measures, which will consist of inspecting the special measures applied by the hosting provider, as well as making written recommendations to the provider in the event that irregularities are found in this regard.

In order to ensure that these activities are carried out, an authorised ABW officer has the right to enter the inspected premises used for the provision of hosting services and to request explanations from the hosting provider and to make available the technical and operational documentation resulting from the application of the special measures.

Under the regulations, the hosting provider is obliged to remedy the irregularities found in a timely manner.

The provisions introduced, on the one hand, refer in some elements to the *Act of 22 August 1997 on the protection of persons and property* and, on the other hand, which is extremely important from the perspective of the principles of the activities implementation, do not exclude the application of the Act – Entrepreneurs' Law.

In the context of the Act on the protection of persons and property, it is worth noting the wording of Art. 43(2) points 3–5, which sets out the principles of the supervision of the Commander-in-Chief of the Police over the activity of specialised armed security formations. The supervision indicated therein consists, inter alia, in entering the premises of an entrepreneur conducting business activity and issuing written recommendations aimed at removing identified irregularities and adjusting the activity of such formations to the provisions of the law.

However, the explanatory memorandum to the Government draft of the Act amending the AT Act and the Act on the ABW and the AW states: *It should be emphasised that the provisions of the Act of 6 March 2018 – Entrepreneurs' Law, including Art. 48, Art. 49(1)–(3) and (6)–(9), as well as Art. 51–57*[33].

In the context of Art. 48 of the Act – Entrepreneurs' Law, attention should be drawn, inter alia, to the obligation of the control authority to notify the entrepreneur of its intention to initiate a control. It shall be initiated no earlier than after the lapse of 7 days and no later than before the lapse of 30 days from the date of delivery of the notice of the intention to initiate control. At the request of the entrepreneur, it may be initiated before the lapse of 7 days from the day of delivery of the notice. A protocol shall be drawn up of the control activities performed in the manner connected with the control.

Pursuant to Art. 49 of this regulation, control activities may be performed by employees of the control body upon presentation to the entrepreneur or a person authorised by the entrepreneur of an official ID card authorising them to perform such activities and upon delivery of an authorisation to perform the control. Its scope cannot go beyond that indicated in the authorisation.

Pursuant to Art. 51–57 of this Act, the control shall be carried out, as a rule, at the entrepreneur's seat or place of business activity and during working hours or while the entrepreneur is actually carrying out business activity. The control activities shall be performed as efficiently as possible and in such a way as not to disrupt the entrepreneur's operations. The findings of the control shall be included in a protocol. In the event that the entrepreneur indicates in writing that the activities carried out significantly interfere with the entrepreneur's business activity,

[33] *Government draft of the Act amending the Act...* – explanatory memorandum..., p. 9.

the necessity to take such activities shall be justified in the inspection protocol. Furthermore, the prohibition to undertake and carry out more than one inspection of the entrepreneur's activity applies. The duration of all controls at the entrepreneur in one calendar year depends on the size of the enterprise. The extension of the duration of the inspection is only possible for reasons beyond the control authority's control and requires justification in writing.

The indicated norms resulting from the Act – Entrepreneurs' Law do not exhaust the entire regulation of control, however, on the basis of the solutions referred to, it should be emphasised that the control of the application of special measures is carried out according to the standard rules provided for the control of entrepreneurs and does not contain distinctive solutions.

Art. 26d. 1. A removal order or a declaration of infringement as referred to in Art. 4(3) and (4) of Regulation 2021/784 shall be given by administrative decision. The provisions of Art. 6, Art. 7, Art. 7b, Art. 8, Art. 12, Art. 14, Art. 16, Art. 24, Art. 26 § 1 and 2, Art. 28–30, Art. 32, Art. 33, Art. 35 § 1, Art. 50, Art. 54–56, Art. 63–65, Art. 72, Art. 75 § 1, Art. 77, Art. 97 § 1 point 4 and § 2, Art. 104, Art. 105 § 1, Art. 112, Art. 113 § 1, Art. 156–158, Art. 217 and Art. 268a of the Act of 14 June 1960 – Code of Administrative Procedure (Journal of Laws of 2024, item 572) shall apply to the proceedings in these cases to the extent not regulated by Regulation 2021/784 and this Act.

2. The designation of hosting providers exposed to terrorist content as referred to in Art. 5 of Regulation 2021/784 shall be carried out by means of an administrative decision. The provisions of the Act of 14 June 1960 – Code of Administrative Procedure, referred to in paragraph 1, and Art. 107 of this Act shall apply to the proceedings in these cases.
3. The decisions referred to in paragraphs 1 and 2 shall be final and immediately enforceable.
4. A hosting provider against whom the Head of the ABW has issued a removal order, or a content provider whose content is covered by a removal order, shall have the right to lodge a complaint against that order with an administrative court within 30 days of:
   1) its delivery in the manner referred to in Art. 3(5) of Regulation 2021/784 – in the case of a hosting provider;
   2) receive the information referred to in Art. 11(1) of Regulation 2021/784 – in the case of a content provider.
5. A hosting provider or content provider against whom the Head of the ABW has issued a decision as referred to in Art. 4(4) of Regulation

> 2021/784 shall have the right to lodge a complaint against that decision with an administrative court within 30 days of receiving notification of that decision.
> 6. A hosting provider against whom the Head of the ABW has issued a decision as referred to in Art. 5(4),(6) or (7) of Regulation 2021/784 shall have the right to lodge a complaint against that decision with an administrative court.
> 7. The complaints referred to in paragraphs 4–6 may be investigated under the simplified procedure referred to in Art. 120 of the Act of 30 August 2002 – Law of the Administrative Courts Procedure (Journal of Laws of 2024, item 935) unless a party requests a hearing and the court considers that all the circumstances of the case have been sufficiently explained and a hearing is unnecessary. The provision of Art. 122 of the Act of 30 August 2002 – Law of the Administrative Courts Procedure shall apply.

In the light of the wording of Art. 26d(1) and (2), a removal order or a finding of an infringement in a cross-border removal order procedure, as well as the designation of hosting providers exposed to terrorist content shall be carried out by means of an administrative decision. The procedural norms for issuing decisions are therefore provided not only by Regulation 2021/784 or the amended AT Act, but also by the *Act of 14 June 1960 – Code of Administrative Procedure* (hereinafter: CAP). The scope of application of the latter Act is, however, significantly limited by the enumerative indication of specific provisions.

Whether indeed such a profound exclusion of the CAP makes it feasible to realistically treat a removal order as an administrative decision may be debatable, especially in the context of the inapplicability in these cases of Art. 107 of the CAP defining the necessary elements of a decision. However, as indicated in the explanatory memorandum to the Act:

> The partial application of the regulations of the Code of Administrative Procedure in this case is necessary. This is based on the fact that the procedure described in Regulation 2021/784 for issuing removal orders is intended to provide a coherent and efficient mechanism at EU level (and therefore across borders) for the removal or blocking of any terrorist content on the network. The effectiveness of this mechanism, in turn, is measured by the speed with which it reacts and performs. As a result, the procedure adopted in the EU instrument with regard to both the issuing of removal orders and the finding of infringements referred to in Art. 4(3) and (4) of Regulation

> 2021/784 differs significantly from some solutions adopted under national administrative law. Moreover, most of the elements within the meaning of the administrative procedure are explicitly laid down in the Regulation itself, e.g. the elements of the decision, the timing and the effect of its notification, and it is therefore necessary to exclude national rules in this case[34].

The explanatory Memorandum to the Act also indicates that the catalogue of provisions of the CAP adopted in Art 26d(1) is modelled on Art. 4(1) of the *Act of 13 April 2022 on specific solutions to counteracting support for aggression against Ukraine and to protect national security*. However, necessary additions and adjustments to the procedure mechanism resulting directly from the provisions of Regulation 2021/784 have been made.

It should therefore be noted that the basic principles of the CAP apply to proceedings for injunctions and the designation of hosting providers exposed to terrorist content (special measures), including:

- the rule of law (Art. 6),
- the principle of objective truth (Art. 7),
- the principle of taking into account the public interest and the legitimate interest of citizens (Art. 7),
- the principle of trust in public authority (Art. 8),
- the principle of swift and simple proceedings (Art. 12),
- the principle of written procedures (Art. 14),
- the principle of permanence of administrative decisions (Art. 16).

The aforementioned provisions are of a strictly guarantee nature from the perspective of protecting the interests of a party. In accordance with Art. 24 of the CAP, the objectivity of the proceedings is also safeguarded by the possibility of excluding an employee of the authority concerned from participating in the proceedings in accordance.

From the perspective of the parties, it is also worth mentioning the application of Art. 28 and 29 of the CAP, according to which a party is anyone whose legal interest or duty is affected by the proceedings or who requests an action of the authority by reason of his/her legal interest or duty. The parties may be natural and legal persons, and when it comes to state and self-government organisational units and social organisations – also units without legal personality.

[34] *Government draft of the Act amending the Act*... – explanatory memorandum, pp. 9–10.

In contrast to the above-mentioned pattern from the Act on specific solutions to counteracting support for aggression against Ukraine and to protect national security, the entire Art. 77 of the CAP applies in the cases covered by the analysed regulation. According to it, the authority is obliged to exhaustively collect and consider all evidence, and may at any stage of the proceedings change, supplement or revoke its decision on the taking of evidence. The body carrying out the procedure at the request of the authority competent to deal with the case (Art. 52 of the CAP) may also, of its own motion or at the request of a party, hear new witnesses and experts on the circumstances which are the subject of those proceedings.

By analogy with removal orders and the finding of infringements in the form of an administrative decision, the designation of hosting providers exposed to terrorist content also takes place, pursuant to Art. 5 of Regulation 2021/784. The CAP also applies to these decisions, but to a limited extent. In this case, however, Art. 107 of the CAP, which is the provision defining the elements of a decision, applies, in contrast to the proceedings related to the issuance of a removal order or a finding of infringement referred to in Art. 4 (3) and (4) of Regulation 2021/748. This is due to the fact that the aforementioned Regulation in this case does not specify the form or components of this decision.

At the same time, in all these cases the proceedings are single-instance and the decisions issued are subject to immediate enforceability, which is related to the need to ensure the efficiency and effectiveness of the conduct of such proceedings. In the context of the single-instance nature of administrative proceedings, Art. 78 of the Constitution of the Republic of Poland should be recalled, according to which each party has the right to appeal rulings and decisions issued in the first instance, and exceptions to this principle and the procedure of appealing are determined by law. Thus, the Constitution of the Republic of Poland allows for such a solution, but it constitutes an exception to the principle, which must have its justification. In these circumstances, it must be sought in the constitutional premise of ensuring public safety and order. For, according to Art. 31(3) of the Constitution of the Republic of Poland, limitations on the exercise of constitutional freedoms and rights, in this case the right to appeal against a decision issued at first instance, may be established only by law and only if they are necessary in a democratic state for its security or public order or for the protection of the environment, public health and morals or the freedoms and rights of others. These restrictions must not affect

the essence of freedoms and rights. In this case, the lack of possibility to appeal against the first instance decision does not seem, in the author's opinion, to violate the essence of the rights referred to above, as the legal action remains. A separate issue, however, is to assess whether this solution is necessary in a democratic state for its security or public order. It also seems to meet this constitutional requirement. While it is conceivable that, as a result of a challenge to the decision, the Head of the ABW will process an application for reconsideration, the substance of the matters decided requires immediate enforceability. A removal order cannot wait until it becomes final, because its essence is to immediately prevent the dissemination of terrorist content. The waiting period for the decision to become final would deprive this legal tool of its preventive significance, as the removal order is not a punishment but a preventive instrument. Only on the basis of other legal provisions in separate proceedings, no longer administrative but criminal, it is possible to punish a provider of such content. An analogous view should be taken of the solution according to which an appeal against the decision would take place to the body of second instance, i.e. the body supervising the formation, in this case the Prime Minister.

The hosting provider against which the Head of the ABW has issued a removal order, or the content provider whose content covers removal order, shall be entitled to lodge a complaint with an administrative court within a period of 30 days. In the first case, this period is calculated from delivery of the decision and, in the second case, from the date of receipt of the information. In this respect, Art. 26d of the Act is an implementation of Art. 9 of Regulation 2021/784, which grants the right to appeal against removal orders issued and other decisions issued by the competent authority.

In case of a hosting provider, the competent authority shall address the removal order to its main organisational unit or to its legal representative. The removal order shall be transmitted to the contact point of the hosting provider by electronic means capable of producing a written confirmation under conditions that allow to establish the authenticity of the sender, including the exact date and time of sending and receipt of the order.

A hosting provider or content provider against whom the Head of the ABW has issued a decision in the aforementioned cross-border removal order procedure shall have the right to lodge a complaint against that decision with an administrative court within 30 days of receiving notification of that decision.

Also, a hosting provider that has been recognised as a vulnerable provider for terrorist content (special measures) has the right to file a complaint against this decision with an administrative court.

Complaints filed in all of the above-mentioned cases may be examined under the simplified procedure referred to in Art. 120 of the *Act of 30 August 2002 – Law of the Administrative Courts Procedure*, i.e. in camera session with three judges, unless a party requests a hearing and the court finds that all circumstances of the case have been sufficiently explained and a hearing is unnecessary. As indicated in the explanatory memorandum to the Act, this solution is intended to ensure that the processing of judicial remedies against decisions is carried out efficiently and effectively, with all guarantees of the right to a court[35].

The procedure adopted in the Act is an administrative procedure. According to the explanatory memorandum to the draft:

> In the proceedings referred to above, the administrative court remains competent court, which is due to the fact that these proceedings will concern exclusively legal-administrative issues. It should be noted that the sanctions set out in Regulation 2021/7 84 relate to situations of failure to comply with certain obligations of an administrative nature by the hosting provider and not their [his/her] commission of punishable acts under the provisions of criminal law substantive law. The mere removal of content is not a sanctioning measure, but a restrictive measure. Accordingly, the draft proponent envisages that, in this respect, only the administrative courts will be the competent judicial units to hear complaints against decisions of the Head of the ABW[36].

In the course of the parliamentary work on the law, another solution was considered to streamline the stage of the ongoing court proceedings. According to it, the transfer of the file and the response to the complaint to the administrative court would take place within 15 days of the receipt of the complaint, while the complaint would be examined by the Provincial Administrative Court within 30 days of the receipt of the file and the response to the complaint[37]. This solution was modelled on Art. 21 of the *Act*

[35] *Government draft of the Act amending the Act...*, p. 11.

[36] Ibid.

[37] *Report of the Administration and the Internal Affairs Committee and the Committee of Digital Affairs, Innovation and New Technologies on the government draft amending the Act on anti-terrorist activities and the Act on the Internal Security Agency and the Foreign Intelligence*

of 6 September 2001 on access to public information. The government side, i.e. the draft proponent, reacted negatively to the proposal. It pointed out that it would not guarantee a real acceleration of the processing of possible complaints at the judicial stage, as the deadlines contained therein in relation to the court are instructive in nature.

The governmental side proposed a different solution – consideration by the President of the Republic of Poland of the application of Art. 13 § 3 of the Law of the Administrative Courts Procedure on the basis of which not only the Provincial Administrative Court in Warsaw, but also other Provincial Administrative Courts, e.g. those competent according to the place of residence or seat of the complainant or the place of residence or seat of his/her legal representative, could hear cases concerning complaints against decisions issued by the Head of the ABW. An alternative solution could also be to permanently designate the jurisdiction of Provincial Administrative Court other than the one in Warsaw.

> Art. 26e. A hosting provider, in respect of whom a removal order has been issued, shall communicate to the Head of the ABW data referred to in Art. 21(1) letter (b) and (d) of Regulation 2021/784 by 1 March each year for the preceding year.

The aforementioned Art. 21(1) of Regulation 2021/784 obliges Member States to collect and transmit to the EC, by 31 March each year, the information they have obtained from their competent authorities and hosting providers under their jurisdiction for the previous calendar year. This information , according to Regulation 2021/784 includes:

- the number of removal orders issued and the number of times terrorist content has been removed or access to it has been prevented, and the speed with which removal has taken place or access has been prevented;
- specific measures taken under the Regulation, including the number of times terrorist content has been removed or access to it has been prevented, and the speed with which removal has taken place or access has been prevented;

Agency (print no. 661), print no. 706, https://orka.sejm.gov.pl/Druki10ka.nsf/0/C75A45601BC82E4EC1258BB3003DFB3A/%24File/706.pdf [accessed: 21 XII 2024].

– the number of requests for access made by the competent authorities, in relation to content retained by a hosting provider on the basis of Art. 6 of the Regulation (hosting providers shall retain terrorist content, which have been removed or to which access has been prevented as a result of a removal order or specific measures, which have been removed as a result of the removal of such terrorist content and data which are necessary for: control in administrative or judicial proceedings or for hearing complaints in the event of a decision to remove terrorist content and related data or to disable access to them; or the prevention of terrorist offences, their detection, the conduct of preliminary investigations in their case and prosecution of terrorist offences);
– the number of complaint procedures initiated and actions taken by hosting providers;
– the number of administrative or judicial proceedings initiated and decisions taken by the competent authority in accordance with national law.

Art. 26f. 1. A hosting provider, who fails to comply with the obligation referred to in Art. 3(3) or (6), Art. 4(2) or (7), Art. 5(1–3),(5) or (6), Art. 6, Art. 7, Art. 10, Art. 11, Art. 14(5), Art. 15(1) or Art. 17 of Regulation 2021/784 shall be liable to a fine.

2. The fine referred to in paragraph 1 shall be imposed by the Head of the ABW, by administrative decision, taking into account the conditions and circumstances referred to in Art. 18 of Regulation 2021/784, at a rate of up to 4% of the total turnover of the hosting provider in the preceding turnover year.
3. The decision referred to in paragraph 2 shall be final.
4. The funds from the fines referred to in paragraph 1 shall constitute revenue for the state budget.

Art. 26f contains penalising norms in the form of administrative fines for specific behaviour that constitutes a breach of the obligations set out in Regulation 2021/784. In accordance with Art. 18, Member States shall lay down provisions on penalties applicable in the event of infringements of this legal act by hosting providers and shall take all measures necessary to ensure their enforcement. The enumeration of the articles of Regulation 2021/784, which refer to the obligations of the hosting provider is repeated

after the EU legislator in the described Art. 26f of the Act. A sanction may be applied to a hosting provider in cases where:

- a hosting provider has failed to remove a terrorist content or prevented access to that content in all Member States as soon as possible and, in any event, did so no later than one hour after receiving the removal order (Art. 3(3));
- a hosting provider has failed to inform the competent authority, using the model set out in Annex II to the Regulation, of the removal of terrorist content or the prevention of access to terrorist content in all Member States, indicating in particular the time of that removal or disabling of access (Art. 3(6));
- a hosting provider who has been ordered to remove terrorist content under a cross-border removal order procedure has not taken the measures envisaged for removal orders or has not taken the necessary measures to be able to restore the removed content or access to it (Art. 4(2));
- where the competent authority of the Member State in which the hosting provider has its main organisational unit or where its legal representative is resident or established has issued a decision finding an infringement of the Regulation by an authority of another country which issued a removal order, the hosting provider has not immediately restored the content in question or access to it (Art. 4(7));
- a hosting provider exposed to terrorist content has failed to include in its contractual terms and does not apply provisions to counteract the use of its services for the public dissemination of terrorist content. In doing so, hosting provider shall not act with due diligence, in a proportionate and non-discriminatory manner, taking due account in all circumstances of the fundamental rights of users, in particular freedom of expression and information in an open and democratic society, so as to avoid the removal of material which does not constitute terrorist content (Art. 5(1));
- a hosting provider exposed to terrorist content does not take specific measures to protect its services from the public dissemination of terrorist content (Art. 5(2));
- the specific measures applied by a hosting provider exposed to terrorist content do not meet all of the following requirements:
  - effectively reduce the level of exposure of a hosting provider's services to terrorist content;

  - are targeted and proportionate, taking into account the level of exposure of services to terrorist content;
  - are applied in a manner which fully respects the rights and legitimate interests of users, in particular the fundamental rights of users relating to freedom of expression and information, respect for private life and protection of personal data;
  - are applied in a careful and non-discriminatory manner,
- a hosting provider exposed to terrorist content fails to notify the competent authority of the specific measures he/she has taken and intends to take to comply with its obligations (Art. 5(5));
- a hosting provider exposed to terrorist content has failed to comply with a decision of the competent authority requiring him to take the necessary additional precautionary measures (Art. 5(6));
- a hosting provider has not retained content of a terrorist nature, which have been removed or to which access has been prevented as a result of a removal order or specific measures pursuant to Art. 3 or 5 of the Regulation, as well as the related data which are necessary for the purposes of controlling in administrative or judicial proceedings or the examination of complaints or for the prevention, detection, the conduct of preliminary investigations in their case and prosecution of terrorist offences (Art. 6 of the Regulation);
- a hosting provider has failed to clearly define in its contractual terms its rules against dissemination of terrorist content (Art. 7);
- a hosting provider, who in in the calendar year concerned has taken measures to counter the dissemination of terrorist content or has been required to take action under this Regulation, shall not make a publicly available transparency report on its activities for the year concerned. He shall not publicise the report before 1 March of the following year or the report does not contain the elements provided for in the regulation (Art. 7);
- a hosting provider has failed to establish an effective and accessible mechanism allowing content providers, in case where their content has been removed or access to it has been prevented as a result of specific measures, to submit a complaint against such removal or prevention of access with a request to restore the content or to have access to it (Art. 10);

- a hosting provider fails to process complaints and to restore content or access in a timely manner where their removal or disabling of access was unjustified (Art. 10);
- a hosting provider who has removed terrorist content or has prevented access to it, failed to make available to the content provider of information on such removal or disabling of access or, despite a request from the content provider, failed to inform the content provider of the reasons for the removal or disabling of access and of its rights to challenge the removal order, or failed to provide the content provider with a copy of the removal order (Art. 11);
- a hosting provider, who become aware of terrorist content involving an immediate threat to life did not immediately inform the authority competent for the investigation and prosecution of offences in the Member State or Member States concerned (Art. 14(5));
- a hosting provider has failed to designate or establish a contact point for the receipt of removal orders by electronic means or to ensure that information on the contact point is publicly available (Art. 15(1));
- a hosting provider, which does not have a central organisational unit in the EU, has not appointed a natural or legal person as its legal representative in the EU for the purpose of receiving, complying with and implementing removal orders and decisions issued by competent authorities (Art. 17).

The indicated acts or omissions, despite their large number, do not exhaust the entirety of the behaviour that may be sanctioned on the basis of the catalogue provisions set out in Art. 26f(1) of the Act. However, it is important to emphasise their multidimensionality and the fact that they do not relate solely to the issue of the application of removal orders or specific measures alone, but concern, inter alia, the implementation of obligations relating to the transparency of actions on the part of these suppliers.

The procedure for the imposition of the penalty and its form (by the Head of the ABW by means of administrative decision), as well as the directives for the penalty and its maximum amount has been determined by the legislator in Art. 26f(2). Pursuant to Art. 18 of the Regulation 2021/784 referred to in this provision, the Head of the ABW, when making a decision on the imposition of a penalty and determining its type and amount shall

be obliged to take into account all relevant circumstances of the case, including:

- the nature, severity and duration of the violation;
- the intentionality or negligent nature of the breach;
- the previous infringement committed by the hosting provider;
- the financial condition of the hosting provider;
- the level of cooperation of the hosting provider with competent authorities;
- the nature and the size of the hosting providers, especially whether they are micro, small or medium-sized enterprises;
- the degree of fault of the hosting provider, taking into account the technical and organisational measures taken by him to comply with the requirements of the Regulation.

The maximum administrative penalty adopted in the provision, which may be imposed under the provisions of the Act, also follows directly from Regulation 2021/784. In its Art. 18(3), it is indicated that Member States shall ensure that systematic or persistent failure to comply with the obligations will be subject to fines of up to 4% of the total turnover of the hosting provider in the preceding financial year.

It should further be noted that the Act, as far as the proceedings are concerned, does not exclude or limit the application of the Code of Administrative Procedure. In the result the Head of the ABW will be able to make use of mitigating tools, such as the institution of deferment or payment in instalments. The principle of proportionality is also maintained through the possibility for the authority to apply provisions the authority may waive the fine in favour of a lighter form of punishment, such as a caution, provided that there are legally defined grounds for doing so (Art. 189f of the CAP)[38].

The decisions of the Head of the ABW are of a final nature, therefore also in this non-judicial challenge mechanisms have been excluded.

Funds from fines constitute revenue for the state budget. In this context, it is worth recalling the regulatory impact assessment attached to the draft law, according to which (...) *the draft law provides for the imposition of administrative fines by the Head of the ABW on hosting providers for violations arising from the regulation, which will constitute income to the state budget, revenue to the state budget should be projected from this state budget. However,*

[38] *Government draft of the Act amending the Act...* – explanatory memorandum, p. 13.

it must be assumed that it will be negligible and, moreover, impossible to quantify at this stage[39]. This provision indicates that, in the opinion of the project proponent the actual application of Regulation 2021/784 and the Act itself will be incidental and the level of threat in Poland of dissemination of terrorist content is low. This opinion results from the frequency of application of the solutions from Art. 32c of the Act on the ABW and the AW currently functioning in the Polish legal order.

> Art. 26g.1. In connection with the pending proceedings for the imposing a financial penalty, the hosting provider shall be obliged to provide to the Head of the ABW, at his every request, within 30 days from the date of receipt of the request, the data necessary to determine the basis for the calculation of the financial penalty.
> 2. Where a hosting provider fails to provide data, or where the data provided by that provider makes it impossible to establish the basis of assessment of the financial penalty, the Head of the ABW shall establish the basis of assessment of that penalty on an estimated basis, taking into account publicly available financial data concerning that provider, including criteria referred to in Art. 7(1) points 1–3 of the Act of 6 March 2018 – Entrepreneurs' Law.

Art. 26g obliges the hosting provider to cooperate with the Head of the ABW in relation to pending proceedings for the imposition of financial penalty. Failure to comply with the obligation contained in paragraph 1 or to provide data that makes it impossible to determine the basis for the penalty, shall result in the Head of the ABW determining the basis for the penalty in an estimated manner, taking into account publicly available financial data concerning that supplier, including the criteria referred to in the Entrepreneurs' Law. The criteria mentioned are the size of the company – whether it is a micro-entrepreneur, a small entrepreneur or a medium-sized entrepreneur.

This provision is analogous to the functioning of legal order Art. 101a of the *Act of 10 May 2018 on the protection of personal data*.

[39] *Government draft of the Act amending the Act…* – regulation impact assessment, https://orka.sejm.gov.pl/Druki10ka.nsf/0/5083CA680B1B465AC1258B97003B446F/%24File/661.pdf, p. 8 [accessed: 14 XII 2024].

> Art. 26h. Financial penalty shall be paid within 14 days of the day on which the decision of the Head of the ABW referred to in Art. 26f(2) has become final.

The time limit for payment of the fine shall be 14 days counted from the day on which the administrative decision of the Head of the ABW to impose the fine has become legally binding, and as indicated, it is final.

Summary

With the Act on amending the AT Act and the Act on the ABW and the AW, through the amendment of the AT Act, the proper application of the Regulation 2021/784 was ensured. The designation the Head of the ABW as the Polish competent authority within the meaning of the aforementioned Regulation, as well the establishment of a contact point in the formation headed by him, is optimal from the perspective of improving the functioning of the Polish anti-terrorist system and its division of competences. It should also be regarded as fully justified to base Polish procedural rules, subsidiary to the provisions of Regulation 2021/784, on the solutions adopted in the Code of Administrative Procedure, while acknowledging that in certain cases only its selected provisions may be applicable.

Nevertheless, in the author's opinion, all provisions relevant from the perspective of countering the dissemination of terrorist content on the internet should be transferred to the AT Act, thus Art. 32c of the Act on the ABW and the AW. However, this procedure would only have a legislative dimension, as these regulations contain conflict-of-law rules which guarantee consistency in their application.

Ensuring the application of Regulation 2021/784 by amending the AT Act, in the legislative context, should be complemented with the modification of Art. 1 of this Act, according to which it sets out the rules for the conduct of anti-terrorist activities (therefore, public administration activities) and cooperation between authorities competent to conduct these activities. The solutions adopted in the new chapter 5a of this Act aimed at countering the dissemination of terrorist content on the internet, particularly in the context of the resulting rights and obligations of hosting providers and content providers, should be reflected in the provision defining the scope of the regulation.

From the practical perspective, ensuring the application of Regulation 2021/784 can be assessed as a strengthening of the Polish anti-terrorist system. In this context, it is worth noting that the PERCI platform developed by Europol has been in operation since 3 July 2023. It is a cloud-based solution that ensures the security and protection of the data uploaded to it. This platform facilitates the transmission of removal orders, Member State reporting and coordination, as well as conflict resolution, where there is an ongoing investigation into the content against which the removal order is to be sent[40].

In this context, it should be noted that although according to Regulation 2021/784, countries should ensure its application from 7 June 2022, in Poland this did not happen until 3 December 2024. Until then, Poland was deprived of both formal basis for the application of the Regulation and the possibility to use its technical support tools. This issue remains all the more important as, during this period, alert levels related to heightened threats of a terrorist nature were in force on Polish territory[41].

It is worth to recall in the end the recital 2 of the Regulation 2021/784, which indicates that:

> regulatory measures to counter online dissemination of terrorist content should be complemented by Member States' counter-terrorism strategies, including, inter alia, the strengthening of media literacy and critical thinking skills, the presentation of alternative narratives or counter-narratives and other initiatives to reduce the impact of and vulnerability to terrorist content posted online, as well as investment in social work, deradicalisation initiatives and contacts with the communities concerned, in order to develop sustainable prevention of radicalisation in the society[42].

This guideline, although not obligatory in nature, should be borne in mind in the context of a future assessment of the adopted legislation application. If it turns out that orders or special measures will be frequently

[40] *Government draft of the Act amending the Act…*– explanatory memorandum…, p. 5.

[41] *Dotychczas wprowadzane stopnie alarmowe i stopnie alarmowe CRP na terytorium RP* (Eng. Alert levels and CRP alert levels introduced so far on Polish territory), Ministerstwo Spraw Wewnętrznych i Administracji, https://www.gov.pl/web/mswia/dotychczas-wprowadzane-stopnie-alarmowe-i-stopnie-alarmowe-crp-na-terytorium-rp [accessed: 23 XII 2024].

[42] Recital 2 of the Regulation 2021/784.

applied at the national level, it will become justified to take additional preventive measures.

Bibliography

Burczaniuk P., *Tasks and powers of criminal law enforcement authorities in combating terrorism in Poland – a legal perspective*, "Terrorism – Studies, Analyses, Prevention" 2022, no. 2, pp. 197–219. https://doi.org/10.4467/27204383TER.22.024.16344.

Cichomski M., *Between armed conflict and state terrorism – specific individual restrictive measures adopted in Poland in the context of the war in Ukraine and the situation in Belarus. Legal perspective*, "Terrorism – Studies, Analyses, Prevention" 2024, no. 5, pp. 311–350. https://doi.org/10.4467/27204383TER.24.011.19399.

Cichomski M., Idzikowska-Ślęzak I., *Alert levels – practical and legal dimensions of their use*, 2022, "Terrorism – Studies, Analyses, Prevention" no. 2, p. 65, 220–258. https://doi.org/10.4467/27204383TER.22.025.16345.

Cichomski M., Marchliński P., *Krajowe rozwiązania w zakresie bezpieczeństwa obrotu prekursorami materiałów wybuchowych – po zamachu terrorystycznym w Norwegii 22 lipca 2011 r. w kontekście nowych zadań Policji* (Eng. National security arrangements in the trade in explosives precursors – after the terrorist attack in Norway on 22 July 2011 in the context of new police tasks), in: *Polska ustawa Antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (eds.), Szczytno 2016, pp. 591–600.

Gabriel-Węglowski M., *Działania antyterrorystyczne. Komentarz* (Eng. Anti-terrorist activities. Commentary), Warszawa 2018.

Internet sources

Dotychczas wprowadzane stopnie alarmowe i stopnie alarmowe CRP na terytorium RP (Eng. Alert levels and CRP alert levels introduced so far on Polish territory), Ministerstwo Spraw Wewnętrznych i Administracji, https://www.gov.pl/web/mswia/dotychczas-wprowadzane-stopnie-alarmowe-i-stopnie-alarmowe-crp-na-terytorium-rp [accessed: 23 XII 2024].

List of national competent authority (authorities) and contact points, European Commission, 27 I 2025, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online/list-national-competent-authority-authorities-and-contact-points_en?prefLang=pl [accessed: 15 II 2025].

Punkt kontaktowy TCO (Eng. Contact point TCO), BIP ABW https://bip.abw.gov.pl/bip/punkt-kontatowy-tco/525,Punkt-kontaktowy-TCO.html [accessed: 13 XII 2024].

Legal acts

International Convention on maritime search and rescue, concluded at Hamburg on 27 April 1979 (Journal of Laws of 1988, no. 27, item. 184 and 185).

Treaty on the functioning of the European Union (consolidated version) – (Official Journal of the EU C 202/47 of 7 VI 2016).

Treaty on European Union (consolidated version) – (Official Journal of the EU C 202/13 of 7 VI 2016).

Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Official Journal of the EU L 172/79 of 17 V 2021).

Regulation (EU) No 98/2013 of the European Parliament and of the Council of 15 January 2013 on the marketing and use of explosives precursors (Official Journal of the EU L 39/1 of 9 II 2013).

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (Official Journal of the EU L 88/6 of 31 III 2017).

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (Official Journal of the EU L 241/1 of 17 IX 2015).

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (Official Journal of the EU L 218/8 of 14 VIII 2013).

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) – (Official Journal of the EU L 178/1 of 17 VII 2000).

Constitution of the Republic of Poland of 2 April 1997 (consolidated text, Journal of Laws of 1997, no. 78, item 483, as amended).

Act of 18 October 2024 amending the Act on anti-terrorist activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency (Journal of Laws of 2024, item 1684).

Act of 26 July 2024 on amending certain acts to improve the activities of the Armed Forces of the Republic of Poland, the Police and the Border Guard in the event of a threat to state security (Journal of Laws of 2024, item 1248).

Act of 17 August 2023 amending the Act – Criminal Code and certain other acts (Journal of Laws of 2023, item 1834).

Act of 7 July 2023 amending the Act – Civil Procedure Code, the Act – the Law on the System of Common Courts, the Act – the Criminal Procedure Code and certain other acts (Journal of Laws of 2023, item 1860).

Act of 7 July 2023 amending the Act on the protection of shipping and seaports and certain other acts (Journal of Laws of 2023, item 1489).

Act of 13 April 2022 on specific solutions to counteracting support for aggression against Ukraine and to protect national security (consolidated text, Journal of Laws of 2024, item 507).

Act of 12 March 2022 on assistance to Ukrainian citizens in connection with the armed conflict on the territory of the country (Journal of Laws of 2022, item 583).

Act of 11 March 2022 on defence of the homeland (consolidated text, Journal of Laws of 2024, item 248, as amended).

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

Act of 21 January 2021 on foreign service (consolidated text, Journal of Laws of 2024, item 1691, as amended).

Act of 10 May 2018 on the protection of personal data (consolidated text, Journal of Laws of 2019, item 1781).

Act of 6 March 2018 – Entrepreneurs' Law (consolidated text, Journal of Laws of 2024, item 236, as amended).

Act of 6 March 2018 – Provisions introducing the Act – Entrepreneurs' Law and other laws on business activity (Journal of Laws of 2018, item 650).

Act of 26 January 2018 – Provisions introducing the Act on the Marshall' s Guard (Journal of Laws of 2018, item 730).

Act of 8 December 2017 on the State Protection Service (Journal of Laws 2018, item 138).

Act of 16 November 2016 – Provisions introducing the Act on the National Revenue Administration (consolidated text, Journal of Laws of 2016, item 1948, as amended).

Act of 10 June 2016 on anti-terrorist activities (Journal of Laws of 2024, item 92, 1248, 1684).

Act of 13 April 2016 on the security of trading in explosives precursors (consolidated text, Journal of Laws 2019, item 994).

Act of 30 August 2002 – Law of the Administrative Courts Procedure (consolidated text, Journal of Laws of 2024, item 935, as amended).

Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence (consolidated text, Journal of Laws of 2024, item 812, as amended).

Act of 6 September 2001 on access to public information (consolidated text, Journal of Laws of 2022, item 902).

Act of 6 June 1997 – Criminal Code (consolidated text, Journal of Laws of 2024, item 17).

Act of 6 April 1990 on the Police (consolidated text, Journal of Laws of 2024, item 145, as amended).

Act of 14 June 1960 – Code of Administrative Procedure (consolidated text, Journal of Laws of 2024, item 572).

Regulation of the Prime Minister of 20 June 2002 on "the Principles of Legislative Techniques" (consolidated text, Journal of Laws of 2016, item 283).

Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online (Official Journal of the EU L 63/50 of 6 III 2018).

Case law

Judgement of the European Court of Human Rights in the case Pietrzak v. Poland and Bychawska-Siniarska and Others v. Poland, https://arch-bip.ms.gov.pl/pl/prawa-czlowieka/europejski-trybunal-praw-czlowieka/orzecznictwo-europejskiego-trybunalu--praw-czlowieka/listByYear,2.html?ComplainantYear=2024 [accessed: 18 V 2025].

Other documents

Commission Staff Working Document Impact Assessment. Accompanying the document. Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, Brussels, 12 IX 2018, SWD(2018) 408 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN [accessed: 4 V 2023].

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms, Brussels, 28 IX 2017, COM (2017) 555 final.

Mechanisms for blocking terrorist content on the internet in the light of the Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, Presentation by the Ministry of Internal Affairs and Administration, prepared for the Interministerial Team for Terrorist Threats.

Government draft amending the Act on anti-terrorist activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency, print no. 661, https://www.sejm.gov.pl/Sejm10.nsf/druk.xsp?nr=661 [accessed: 24 XII 2024].

Report of the Administration and the Internal Affairs Committee and the Committee of Digital Affairs, Innovation and New Technologies on the government draft law amending the Act on anti-terrorist activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency (print no. 661), print no. 706, https://orka.sejm.gov.pl/Druki10ka.nsf/0/C75A45601BC82E4EC1258BB3003DFB3A/%24File/706.pdf [accessed: 21 XII 2024].

Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online, Brussels, 14 II 2024, COM(2024) 64 final.

The European Commission's position on 9 June 2021 (ref. no. INFR(2021)2046, C(2021)3630 final).

Mariusz Cichomski

Lawyer, sociologist. He works on issues related to terrorism, organised crime, oversight of service activities, security legislation and issues related to the application of restrictive measures. He is the author of more than 30 publications on security, particularly in the legal dimension, and on sociology.

Terrorism – Studies, Analyses, Prevention, 2025, no. 7: 381–424

https://doi.org/10.4467/27204383TER.25.037.21814

Article

Terrorist challenges in the Sahel and NATO's southern flank

ALEKSANDER OLECH
https://orcid.org/0000-0002-3793-5913
Defence24

PAWEŁ WÓJCIK
https://orcid.org/0009-0002-8476-0746
Opportunity Institute for Foregin Affairs

Abstract

The aim of the article is to analyse the growing security threats in the Sahel region and their impact on the stability of the North Atlantic Alliance's (NATO) southern flank. The authors adopt the thesis that the increasing presence of armed groups and the activity of terrorist organisations, primarily the Islamic State and Al-Qaeda, are leading to escalation of violence, political and social crisis, which consequently threatens international security, particularly in Europe and NATO countries. The article is based on the author's analysis of the report, a review of the available literature and complementary sources, including reports from journalists and experts specialising in the Sahel region. A research query was conducted, which formulated four key questions concerning the causes of conflict escalation, the impact of interventions and withdrawals of international forces, the role of external actors (Russia and China among others) and the effectiveness of NATO and European Union actions. The analysis showed that these challenges require a comprehensive, long-term international strategy, combining military actions with political reforms and the region development support, while at the same time taking

into account threats not only in the southern, but also in the eastern NATO's flank.

Keywords

Sahel, terrorism, NATO, Africa, Wagner Group, ISIS, Al-Qaeda, migration

Introduction

The Sahel is a region of strategic importance and an area of international competition[1]. Due to the intensification of jihadist insurgencies[2], political instability exacerbated by coups d'état[3], illegal migration[4], as well as increasing environmental degradation[5] the need for comprehensive international engagement in the region has never been more urgent. The sources of the crisis include military juntas incapable of governing and maintaining peace and security, whose power greatly hinders the development of states. The difficult situation is confirmed by the presence in the Sahel of United Nations (UN) peacekeeping forces, foreign troops, private military companies (PMC) and mercenaries. It seems that leading organisations, primarily the European Union[6] and

1 S. As-Sazid, *Emerging Security Challenges in the Sahel and the Need for an Adaptative Approach towards Peacebuilding*, "International Day of United Nations Peacekeepers Journal" 2023, vol. 9, no. 9, pp. 17–34.

2 D. Lounnas, *Le djihadisme au Sahel apres la chute de Daech*, "Politique etrangere" 2019, no. 2, pp. 105–114.

3 *Military juntas in Africa's 'coup belt' fail to contain extremist violence*, Financial Times, 24 XI 2024, https://www.ft.com/content/d0af5533-ecdd-4be0-bbb8-e5b3e4bb11b4 [accessed: 30 XII 2024].

4 A. Fakhry, *More than borders: effects of EU interventions on migration in the Sahel*, Institute for Security Studies, 16 VIII 2023, https://issafrica.org/research/west-africa-report/morethan-borders-effects-of-eu-interventions-on-migration-in-the-sahel [accessed: 30 XII 2024].

5 *Ecological Threat Report 2024. Analysing ecological threats, resilience & peace*, The Institute for Economics & Peace, https://www.economicsandpeace.org/wp-content/uploads/2024/10/ETR-2024-web.pdf [accessed: 15 XII 2024].

6 R. Marangio, *Sahel reset: time to reshape the EU's engagement*, European Union Institute for Security Studies, 5 II 2024, https://www.iss.europa.eu/publications/briefs/sahel-resettime-reshape-eus-engagement [accessed: 15 XII 2024].

the North Atlantic Alliance (NATO)[7], should re-evaluate their strategies in order to stabilise the region and prevent its further disintegration.

The Sahel countries, which have a complex history of colonialism embedded in their creation, are struggling with the long-term consequences of lack of development, social fragmentation and political exclusion. The challenges of regional development and stability are combined there with threats such as: terrorism, extremism, ethnic tensions and systemic corruption. This state of affairs has a negative impact on both national and international efforts aimed at improving the situation in the Sahel. The instability of the region is compounded by the changing dynamics of external influences. The Russian Federation[8] and the People's Republic of China[9] are increasingly positioning themselves as partners for the Sahel states. They offer financial and military support, but they do not expect changes in human rights or the introduction of democratic principles, which is often one of the conditions imposed by Western countries. This allows the Sahel regimes to maintain a semblance of autonomy without sacrificing their own political independence. African states opt for short-term gains at the expense of long-term stability[10]. The geopolitics of the Sahel is thus shaped by both local problems and the interests of global powers. Foreign competition for political, economic and military influence weakens state structures, deepens social divisions and threatens security not only in Africa, but also outside the continent[11]. It should be emphasised that in Mali, Burkina Faso and Niger, the situation is dynamic

[7] *Independent expert group supporting NATO's comprehensive and deep reflection process on the southern neighbourhood. Final Report. May 2024*, NATO, https://nato.int/nato_static_fl2014/assets/pdf/2024/5/pdf/240507-NATO-South-Report.pdf [accessed: 16 XII 2024].

[8] *Moscow's winning return to Africa*, Le Monde, 21 VIII 2024, https://www.lemonde.fr/en/international/article/2024/08/21/moscow-s-winning-return-to-africa_6719241_4.html [accessed: 7 XII 2024].

[9] S. Bhattacharya, *China's Great Game in the Sahel*, Vivekananda International Foundation, 12 X 2022, https://www.vifindia.org/article/2022/china-s-great-game-in-the-sahel [accessed: 7 XII 2024].

[10] F. Mintoiba, *Footsteps of change: Rising influence of China and Russia in Africa*, Daily Sabah, 3 X 2024, https://www.dailysabah.com/opinion/op-ed/footsteps-of-change-risinginfluence-of-china-and-russia-in-africa [accessed: 7 XII 2024].

[11] A. Olech, B. Wójtowicz, *Rywalizacja o surowce w Sahelu – region konfliktu mocarstw* (Eng. Competition for resources in the Sahel – a region of conflict between powers), Trimarium.pl, 18 XI 2022, https://trimarium.pl/projekt/rywalizacja-o-surowce-w-sahelu-region-konfliktu-mocarstw/ [accessed: 7 XII 2024].

in terms of security level and terrorist activity. The phenomena taking place in the north of the African continent directly threaten the EU and undermine NATO's security not only on its southern flank, but also on its eastern flank[12]. The time has come for a coordinated, action-oriented strategy that addresses not only the problems that have been present for years, but also the new problems of the Sahel.

The article discusses the key factors that fuel the crises in the Sahel. The authors make the case for the development of a new international strategy in which NATO and EU Member States would play the most important role. This strategy should be based on a sustained and coordinated engagement, including support for the local security structures, investment in socio-economic development of the region, efforts to stabilise state institutions and countering radicalisation as well as forced migration. This approach should be prioritised over ad hoc, reactive military interventions. The authors adopted a research thesis: the significant presence of armed groups and the increase in terrorist activity in the Sahel region lead to escalation of violence and political destabilisation, which increases the threat to international security, especially in Europe and NATO countries, as well as intensifies uncontrolled migration. The research query detailed the following research questions:

1. Which factors exacerbate the rise of armed groups and the escalation of conflicts in the Sahel region?
2. How international military interventions and withdrawals of troops have affected security and stability of the Sahel?
3. How the growing influence of external actors, i.e. Russia and China, are changing the political dynamic and security in the Sahel region?
4. Can NATO and EU actions effectively stop the spread of terrorism in the Sahel and illegal migration?

The article is based on the report prepared by the authors[13], an analysis of the available literature and a small amount of material including information provided by journalists and experts dealing with the Sahel.

[12] A. Olech, P. Wójcik, *Wojna o Sahel [Raport]* (Eng. The war for the Sahel [Report]), Defence24, 17 XI 2024, https://defence24.pl/geopolityka/wojna-o-sahel-raport [accessed: 15 XII 2024].

[13] Ibid.

Sahel – characteristics of the region

The Sahel is a semi-arid region of Africa stretching from the Atlantic in the west to the Red Sea in the east, forming a transition zone between the desert Sahara and the fertile savannahs of Sub-Saharan Africa[14]. It includes parts of the following countries: Senegal, Mauritania, Mali, Burkina Faso, Niger, Chad, Sudan, Eritrea, Nigeria and Cameroon. The region is characterised by a harsh climate – with high temperatures and erratic and unpredictable rainfall – which makes farming much more difficult and livelihood of local communities dependent on crops and livestock[15]. The unfavourable environmental conditions have a major impact on the daily lives of the inhabitants of the Sahel, but political factors, including weak state institutions, armed conflicts and competition for influence between global powers, are playing an increasingly important role in destabilising the region.

The countries most commonly recognised as central to the Sahel are Mali, Niger, Burkina Faso, Chad and Mauritania, which form the G5 Sahel grouping. In other depictions, the region also includes parts of Senegal, Sudan and Eritrea, demonstrating the complexity of the geographical and political boundaries of the Sahel (Figure 1). Although the basic understanding of this region as a semi-arid zone between the Sahara and the savannahs remains the same, the perception of its extent may vary depending on the adopted perspective – ecological, climatic, geopolitical, military, religious or cultural. Views of the Sahel from an ecological perspective focus on the characteristics of the natural environment and vegetation typical for the region. These, which main determinants are climatic conditions, primarily take into account factors such as temperature and rainfall distribution. In geopolitical terms, the boundaries of the Sahel are determined according to national divisions and the dynamics of political changes, while sociocultural definitions are based on the community of traditions, language and lifestyle of local communities. The military perspective takes into account the presence of military bases, the level of training of armed forces and the flow of armaments, while the agricultural

[14] *Sahel*, Britannica, https://www.britannica.com/place/Sahel [accessed: 14 XII 2024]; H.O. Ibrahim, *The Sahel – a Land of Opportunity*, United Nations, 10 VI 2019, https://unpartnerships.un.org/news/2019/sahel-land-opportunity [accessed: 14 XII 2024].

[15] T.A. Benjaminsen, H. Svarstad, *Climate Change, Scarcity and Conflicts in the Sahel*, in: T.A. Benjaminsen, H. Svarstad, *Political Ecology. A Critical Engagement with Global Environmental Issues*, n.p. 2021, pp. 183–205. https://doi.org/10.1007/978-3-030-56036-2_8.

perspective takes into account the specificity of cropping systems and the dependence on climatic conditions[16]. The diversity of these approaches underlines how multidimensional the nature of the region is[17].

Figure 1. The Maghreb and the Sahel.

Source: A. Olech, *Grupa Wagnera w Afryce* (Eng. The Wagner Group in Africa), Defence24, p. 27. The report is available on the website: https://defence24.pl/geopolityka/rosyjscy-najemnicy-raport-z--dzialalnosci-w-afryce.

[16] B. Tesfaye, *Climate Change and Conflict in the Sahel*, Council on Foreign Relations, November 2022, https://www.cfr.org/report/climate-change-and-conflict-sahel [accessed: 27 V 2025].

[17] *G5 Sahel Region: Country Climate and Development Report – Annex*, World Bank Group, https://documents.worldbank.org/en/publication/documents-reports/document-detail/099150106302237600/p1773430dc79a10c09f600cf2ac1e0e9f3 [accessed: 27 V 2025].

Approx. 64,5% of the Sahel's population is under the age of 25, making it one of the youngest regions in the world demographically. This age structure creates potential for economic development, provided there is adequate investment in education, vocational training and job creation[18]. Moreover, the Sahel has significant potential for renewable energy, especially solar, which can contribute to its energy transition. Initiatives such as Desert to Power aim to harness this potential by developing renewable energy infrastructure[19]. However, realisation of these opportunities requires overcoming major challenges which are political instability, climate change and food insecurity[20].

Internal conflicts in the Sahel have forced tens of millions of inhabitants to flee their homes. Violence, massive corruption, political instability and extreme climatic events, especially droughts and sudden floods, have led to the numerous humanitarian crises. The lack of adequate food is affecting nearly 40 million people[21]. The situation is exacerbated by limited humanitarian access in important countries in the region – Burkina Faso, Mali, Niger and Chad, as the situation there is unstable and violence persists. In 2025, the US government withdrew humanitarian aid, implemented mainly under the aegis of the United States Agency for International Development, which organised the necessary aid in entire Sub-Saharan Africa[22]. The United Nations alerts that during the summer season (between June and August 2025), as many as 52 million people will be at risk of starvation. The largest food crisis in all of West and Central Africa is in Mali. The United Nations needs more than USD 700 million by

[18] A. Dieng, *The Sahel: Challenges and opportunities*, "International Review of the Red Cross" 2021, vol. 103, no. 918, p. 775, https://international-review.icrc.org/articles/editorial-the-sahel-challenges-opportunities-adama-dieng-918 [accessed: 15 XII 2024]. https://doi.org/10.1017/S1816383122000339.

[19] *Desert to Power initiative*, African Development Bank Group, https://www.afdb.org/en/topics-and-sectors/initiatives-partnerships/desert-power-initiative [accessed: 15 XII 2024].

[20] W. McMakin, *UN food agency says 40 million people are struggling to feed themselves in West and Central Africa*, AP, 20 XII 2024, https://apnews.com/article/africa-food-insecurity-hunger-304b66ef7b9b56262fe1114a4b28c7e6 [accessed: 26 XII 2024].

[21] Ibid.

[22] R. Maclean, S. Jammeh, *Africa Received Billions in U.S. Aid. Here's What It Will Lose*, The New York Times, 8 III 2025, https://www.nytimes.com/2025/03/08/world/africa/africa-usaid-funds.html/ [accessed: 20 IV 2025].

October 2025 to carry out essential humanitarian operations in West Africa and the Sahel[23].

The Sahel has become one of the main centres of activity for armed groups, rebels and jihadist organisations[24] that operate with impunity in vast, poorly supervised areas[25]. The lack of efficient border control – particularly on long and difficult-to-access stretches between countries – facilitates the movement of terrorists and transfer of people and weapons. The presence of extremist factions deepens political destabilisation, threatens to local economies and hinders humanitarian operations. A coordinated response from both regional governments as well as international organisations is essential in order to effectively address these threats. From a security point of view, Mali, Burkina Faso, Niger, Sudan and Chad – countries that are particularly vulnerable to violence from terrorist groups and mercenaries and the influence of military regimes – are the most important for the stability of the Sahel. Although other countries of the region also face serious challenges, their internal situation is not deteriorating as much as in the mentioned countries[26]. The effective response to the security challenges is a prerequisite for a stable and more predictable future of the Sahel[27]. This future is not without significance also for Europe, which is already suffering the consequences of the destabilisation of the region – both in terms of migration and geopolitics[28].

---

[23] *More than 50 million in West and Central Africa at risk of hunger*, United Nations, 9 V 2025, https://news.un.org/en/story/2025/05/1163086 [accessed: 30 V 2025].

[24] L. Raineri, F. Strazzari, *Jihadism in Mali and the Sahel: evolving dynamics and patterns*, European Union Institute for Security Studies, 29 VI 2017, https://www.iss.europa.eu/publications/briefs/jihadism-mali-and-sahel-evolving-dynamics-and-patterns [accessed: 16 XII 2024].

[25] Center for Preventive Action, *Violent Extremism in the Sahel*, Council on Foreign Relations, 23 X 2024, https://www.cfr.org/global-conflict-tracker/conflict/violent-extremism-sahel [accessed: 16 XII 2024].

[26] *Defining a New Approach to the Sahel's Military-led States*, International Crisis Group, 22 V 2025, https://www.crisisgroup.org/africa/sahel/burkina-faso-mali-niger/defining-new-approach-sahels-military-led-states [accessed: 27 V 2025].

[27] L.V. del Portillo, *Challenges in the Sahel: Opportunities for Europe*, Eurodefense Network, 21 II 2021, https://eurodefense.eu/2021/02/21/challenges-in-the-sahel-opportunities-for-europe/ [accessed: 18 XII 2024].

[28] J. Borrell, *Together for the security, stability and development of the Sahel*, European Union External Action, 8 V 2020, https://www.eeas.europa.eu/eeas/together-security-stability-and-development-sahel_en [accessed: 27 V 2025].

Great rivalry in the region

The Sahel constitutes a complex geopolitical area, in which groups with diverse ideologies, aims and structures coexist – from tribal communities, to religious organisations and local institutions. Many of them have been there for years, such as Tuaregs, who have lived in Azawad for centuries and claim these lands. Over the past decade, the structure of this community has undergone radical changes. There has been an increase in the importance of jihadist-terrorist groups that have not only dominated the pre-existing armed organisations, but have also taken control of parts of the territory and significantly destabilised the situation in the region. Following the coup in Niger in 2023, Mali, Burkina Faso and Niger formed the Alliance of Sahel States (Alliance des États du Sahel, AES) as a mutual defence pact and an alternative to the pro-Western trend in the region[29].

Mali

There are three main parties of the conflict in Mali. They are currently represented by dozens of factions and rebellions (their number changes every month). The first camp is the pro-state stream, whose narrative is shaped and implemented by the Malian Armed Forces (Forces Armées Maliennes, FAMa). This formation uses the support of three main allied structures, that vary in scope and character of operation:

1) ethnic militia – above all, representatives of the Dogon ethnic group, actively supported by the authorities in Bamako and the military junta of General Assimi Goïta. These militias are involved in ongoing ethnic conflict with the Fulani, some of whom – deprived of state protection – are seeking security within the structures of organisations such as Al-Qaeda or the Islamic State (IS); the Islamic State of Iraq and Syria (ISIS)[30];

[29] J. Czerep, *Konsekwencje powołania Konfederacji Państw Sahelu* (Eng. The consequences of establishment of the Confederation of Sahel States), Polski Instytut Spraw Międzynarodowych, 14 VIII 2024, https://www.pism.pl/publikacje/konsekwencje-powolania-konfederacji-panstw-sahelu [accessed: 15 I 2025].

[30] A. Hauchard, *In Violence-shattered Central Mali, Victims Recount Their Lives*, Barron's, 9 II 2022, https://www.barrons.com/news/in-violence-shattered-central-mali-victims-recount-their-lives-01644458408 [accessed: 5 I 2025].

2) the Africa Corps – Russian paramilitary formation previously known as the Wagner Group, currently functioning as an official mission of support to Mali's authorities[31];
3) pro-government Tuareg groups – including former members of the organisation Groupe d'Autodéfense Tuareg Imghad et Alliés (GATIA), who currently operate, among others, in the tri-state border area of Mali, Niger and Burkina Faso, where they carry out patrol and security tasks[32].

The second camp is made up of anti-government groups, the most important of which is associated to Al-Qaeda Islam and Muslims' Support Group (Jama'at Nusrat al-Islam wal-Muslimin, JNIM), coalition Cadre stratégique pour la défense du peuple de l'Azawad (CSP-DPA) and newly established Azawad Liberation Front, gathering Tuaregs and other ethnic minorities. Although formally separate structures, they share a hostile attitude towards the authorities in Bamako, as well as family ties and personal relationships between leaders, which enable them to maintain a fragile agreement[33]. The leaders of JNIM and CSP-DPA were active participants in the conflict of 2012–2013, that ended with the French military intervention. Memories of the betrayal committed by Al-Qaeda against the Tuaregs during this period remain vivid and affect current relationships within this camp[34].

The third camp is the most cruel participant of the current conflict – the Islamic State Sahel Province (IS Sahel, ISSP). The group took control of a large part of the border area between Mali and Niger[35]. Unlike other

[31] D. Ehl, *How the Russian Wagner Group is entrenching itself in Africa*, Deutsche Welle, 27 X 2024, https://www.dw.com/en/russia-kremlin-wagner-group-influence-in-central-african-republic-sudan-mali/a-70599853 [accessed: 5 I 2025].

[32] H. Nsaibia, C. Weiss, *The End of the Sahelian Anomaly: How the Global Conflict between the Islamic State and al-Qa`ida Finally Came to West Africa*, "CTC Sentinel" 2020, vol. 13, no. 7, https://ctc.westpoint.edu/wp-content/uploads/2020/07/CTC-SENTINEL-072020.pdf [accessed: 5 I 2025].

[33] C. Weiss, *Tuareg rebels, JNIM each claim victory over Russia's Wagner Group in Mali*, Foundation for Defense of Democracies, 29 VII 2024, https://www.fdd.org/analysis/op_eds/2024/07/29/tuareg-rebels-jnim-each-claim-victory-over-russias-wagner-group-in-mali/ [accessed: 5 I 2025].

[34] *Tuareg rebels driven out of Timbuktu*, Al Jazeera, 29 VI 2012, https://www.aljazeera.com/news/2012/6/29/tuareg-rebels-driven-out-of-timbuktu [accessed: 5 I 2025].

[35] A.Y. Zelin, S. Cahn, *Exploiting a "Vast jihad Arena": The Islamic State Takes Territory in Mali*, The Washington Institute for Near East Policy, 26 IX 2023, https://www.washingtoninstitute.

actors, ISSP does not maintain alliances with either Bamako authorities or other armed groups in Mali, making it an isolated but threatening force in the region. The rapid expansion of ISSP is of concern in the context of the growing number of terrorist groups active in the Sahel.

Burkina Faso

In 2014, the situation of security forces in the country was deteriorated by removal of president Blaise Compaoré from office as well as the army's conflict with special services and military police. In 2020, president Roch Marc Christian Kaboré established a militia known as Volunteers for the Defense of the Homeland (Les Volontaires pour la défense de la Patrie, VDP), whose aim was to involve the civilian population in the fight against the growing jihadist threat and to organise a social line of defence against violent attacks by the terrorist groups[36]. Over time, however, the formation proved operationally inefficient and incapable of effectively countering the violence. The deteriorating security situation and expansion of JNIM structures resulted in the state authorities losing control of much of the territory. Currently, according to available data, the military junta commanded by Capt. Ibrahim Traoré, exercises effective authority over less than 60% of the Burkina Faso territory[37].

This junta significantly increased the number of VDP and expanded its involvement in actions against jihadist groups. However, the increase in the number of members of this formation has coincided with accusations of serious abuses. Between 2023 and 2024 international organisations and the media revealed cases of indiscriminate crimes committed by VDP against civilians, including killings, kidnappings and looting[38]. Currently, VDP is estimated to have approx. 100 000 volunteers supporting Burkina Faso's regular army, but there are serious concerns about the quality

org/policy-analysis/exploiting-vast-jihad-arena-islamic-state-takes-territory-mali [accessed: 5 I 2025].

[36] H. Nsaibia, *Actor Profile: Volunteers for the Defense of the Homeland (VDP)*, Armed Conflict Location & Event Data, 26 III 2024, https://acleddata.com/2024/03/26/actor-profile-volunteers-for-the-defense-of-the-homeland-vdp/ [accessed: 5 I 2025].

[37] *Crisis in Burkina Faso: What you need to know and how you can help*, International Rescue Committee, 14 II 2024, https://www.rescue.org/article/crisis-burkina-faso-what-you-need-know-and-how-you-can-help [accessed: 5 I 2025].

[38] *Burkina Faso: Unlawful Killings, 'Disappearances' by the Army*, Human Rights Watch, 29 VI 2023, https://www.hrw.org/news/2023/06/29/burkina-faso-unlawful-killings-disappearances-army [accessed: 5 I 2025].

of their training, the lack of effective oversight, as well as the exclusion of some communities from the recruitment process and the failure to include parts of the regions in operational planning. Due to growing concerns about the brutalisation of the conflict, Ouagadougou government should urgently strengthen mechanisms to control and monitor the VDP's activities, to prevent further escalation of violence and a deepening crisis of social confidence.

Niger

After the 2023 overthrow of president Mohamed Bazoum by the military junta, a number of pro-government organisations supporting the idea of his return to power began to emerge in Niger. Some of these came from backgrounds previously involved in Tuareg rebellions, in both Niger and Mali territory. One of the most recognisable figures associated with this trend is Rhissa Ag Boula, the former leader of Tuareg armed movements, who set up the Council of Resistance for the Republic (Conseil de la Résistance pour la République, CRR). Its aim was to organise political and military support for the ousted president Bazoum[39]. However, in September 2024, CRR was dissolved due to internal divisions and disagreements over strategy and vision for the future. In response to the disintegration of the organisation, Rhissa Ag Boula announced a new formation – the Free Armed Forces (Forces armées libres, FAL)[40].

One of the main groups supporting ousted president Bazoum is Patriotic Liberation Front (PLF) – gaining in importance armed formation, increasingly active on the Nigerian political scene and in the military sphere. In June 2023, PLF carried out an attack on a Chinese oil pipeline linking Niger and Benin. The justification was an allegation of betraying the interests of the ousted government by the junta's support of foreign, mainly Chinese, influence[41]. In August 2024, the leader of the organisation

[39] P. Kum, *Niger: L'ancien rebelle nigérien, Rhissa Ag Boula, annonce son intention de reprendre les armes pour chasser les putschistes*, Alwihda Info, 21 VIII 2023, https://www.alwihdainfo.com/Niger-L-ancien-rebelle-nigerien-Rhissa-Ag-Boula-annonce-son-intention-de-reprendre-les-armes-pour-chasser-les_a125857.html [accessed: 5 I 2025].

[40] J. le Bihan, *Former Niger minister launches movement to overthrow junta*, The Africa Report, 27 IX 2024, https://www.theafricareport.com/363047/former-niger-minister-launches-movement-to-overthrow-junta/ [accessed: 5 I 2025].

[41] L. Fleming, T.I. Issoufou, *Niger confirms anti-junta rebels behind oil attack*, BBC, 22 VI 2024, https://www.bbc.com/news/articles/c511n4edl7lo [accessed: 5 I 2025].

met in Tinzaouaten, in the north of Mali, with a representative of Tuareg leadership. The meeting took place just a month after the battle between the forces of the Russian-backed Mali government and the Tuareg and Al-Qaeda coalition. This event is indicative of the progressive coordination between PLF and Tuareg rebel groups[42].

Niger is one of the states in the Sahel region, on whose territory three ISIS-affiliated groups operate at the same time. The presence of these factions, which include both cross-border structures and local cells, makes the country particularly vulnerable to escalating violence and poses a serious challenge to maintain internal stability and security in the region. Currently, these factions are: the Islamic State in the Greater Sahara (ISGS), which operates mainly in Mali, Burkina Faso and Niger border region, where it carries out attacks on government forces and civilians; the Islamic State West Africa Province (ISWAP) – active in North-Eastern Nigeria, but also in South-Eastern Niger, in Chad and Cameroon, where it attacks the army and infrastructure, and the Islamic State in Libya (IS Libya), that has its main structures in Libya, but its militants also infiltrated the north of Niger. The ISIS leaders are working to consolidate power, facilitated by the lack of threat from the US and French air force, whose military bases have been closed in May 2024[43]. The armed groups of terrorists systematically used sieges, threats and kidnappings as well as planted explosives and landmines to control supply routes and expand their influence in Mali, Burkina Faso and Niger. Islamic groups impose forced taxes, destroy and plunder civilian infrastructure such as places of worship, health centres, food stores, bridges[44] and schools. They also threaten, kidnap and kill teachers.

[42] *Mali and Niger rebels met to 'strengthen' ties amid political turmoil*, Al Arabiya News, 2 IX 2024, https://english.alarabiya.net/News/world/2024/09/02/mali-and-niger-rebels-met-to-strengthen-ties-amid-political-turmoil [accessed: 5 I 2025].

[43] *US military says withdrawal from Niger is complete*, France24, 16 IX 2024, https://www.france24.com/en/live-news/20240916-us-military-says-withdrawal-from-niger-is-complete [accessed: 5 I 2025].

[44] E. Pertier, *After Military Took Power, Terrorist Attacks Only Got Worse*, The New York Times, 22 XII 2024, https://www.nytimes.com/2024/12/22/world/africa/niger-war-coup.html [accessed: 5 I 2025].

Division of terrorist groups in the Sahel

A number of terrorist organisations are active in the Sahel (Figure 2). The most important of them can be divided on the basis of their relationship with global network of Al-Qaeda and ISIS:

1) Al-Qaeda in the Islamic Maghreb (AQIM) originates from jihadist groups fighting in the civil war in Algeria, since 2007 under the aegis of Al-Qaeda the organisation has been fighting in the North and West Africa. One of several groups forming Shura Council of terrorists assists local structures in the Sahel in the fight against military rebellions and democratic rule;
2) JNIM was established in 2017 as a coalition of loyal groups, well-disposed to Al-Qaeda, that decided to reorganise their operations in the face of pressure from French troops and ISIS. After eight years, it is successfully operating in Mali, Burkina Faso as well as Niger and extends its influence throughout West Africa. In 2025, JNIM also has conducted its operations in North West Nigeria and Benin;
3) ISIS divided into three main operational provinces:
   a) ISSP covering Mali, Burkina Faso and Niger,
   b) ISWAP in Nigeria and neighbouring countries,
   c) IS Libya on the Libya and Niger borderland.

Since 2024, all of these units have a single overarching structure that coordinates operations with both the central command in Syria and the structures in Eastern and South Africa, which strengthens the presence of ISIS along major smuggling routes and in strategic regions of the Sahel.

The number of fundamentalist, extremist and terrorist groups in the Sahel region has grown steadily since the beginning of the 21st century. Since 2019, these organisations have extended their activities to the coastal states of West Africa – Benin, Cote d'Ivoire and Togo[45]. Since 2022, there has been a sharp increase in the number of attacks and they have been extremely violent. In 2024, approx. 11 200 deaths from terrorist activities were recorded in the Sahel – three times more than in 2021. Burkina Faso

[45] M. Jeannin, *Ghana worries about rise of terrorist threat in Gulf of Guinea*, Le Monde, 7 VI 2022, https://www.lemonde.fr/en/le-monde-africa/article/2022/06/07/ghana-concerned-about-extension-of-terrorist-threat-to-coastal-states-of-gulf-of-guinea_5985936_124.html [accessed: 5 I 2025].

remains the most vulnerable country, accounting for 48% of all attacks and 62% of those killed in the region[46].

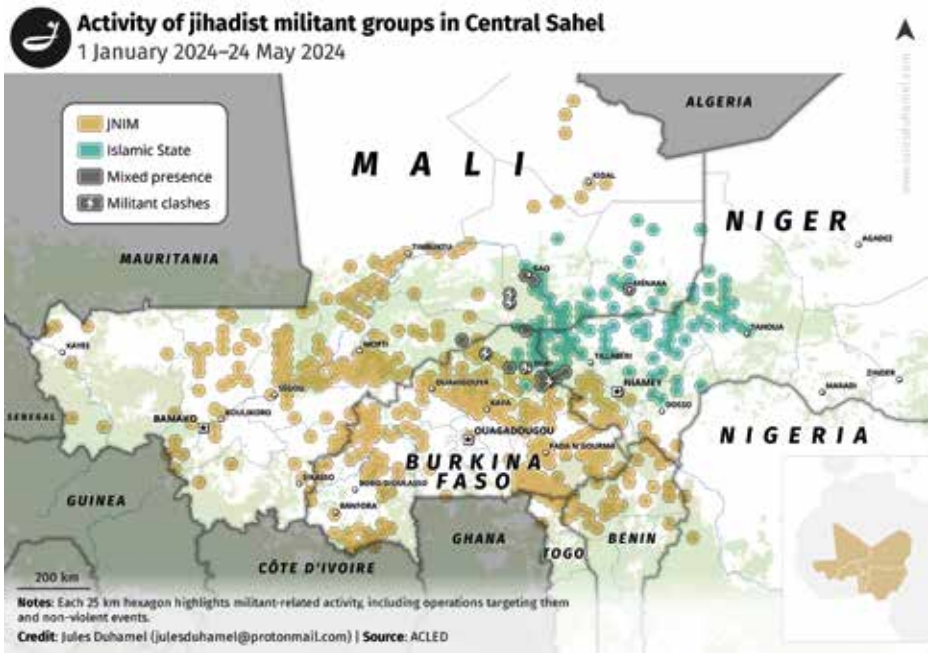


Figure 2. Activities of jihadist groups in the Central Sahel.

Source: ACLED. Quoted after: J. Duhamel, *Central Sahel – Map of jihadist militant groups activity (Jan–May 2024)*, Jules Duhamel, 21 VI 2024, https://www.julesduhamel.com/central-sahel-map-of-jihadist-militant-groups-activity-jan-may-2024/ [accessed: 15 I 2025].

Before the French intervention in the Sahel, there were a number of groups affiliated with Al-Qaeda. Their weakening and the expansion of ISIS have resulted in further fragmentation of jihadism in the region. In response, in 2017, Tuareg Iyad Ag Ghali, together with representatives of AQIM and other groups, led them to unite in JNIM[47]. The aim was both to counter French and UN counter-terrorist efforts and to limit

[46] *Global Terrorism Index 2025*, Institute for Economics & Peace, https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf [accessed: 27 V 2025].

[47] T. Joscelyn, *Analysis: Al Qaeda groups reorganize in West Africa*, FDD's Long War Journal, 13 III 2017, https://www.longwarjournal.org/archives/2017/03/analysis-al-qaeda-groups-reorganize-in-west-africa.php [accessed: 5 I 2025].

the recruitment of fighters by ISIS, and above all to stop the fragmentation of jihadist groups and to keep the organisation united in the Sahel.

Strategic operational plans of JNIM initially focused on three countries in the region: Mali, Burkina Faso and Niger. The formation of the coalition was intended to strengthen the effectiveness of recruitment efforts and to build a centre of power alternative to local governments perceived as allies of "western crusaders"[48]. In the longer term, JNIM envisaged expanding to more countries, including the Gulf of Guinea coastal states. In spite of these ambitions, the high command of this group – Majlis al-Shura – struggles with internal problems typical of decentralised terrorist organisations. These include loyalty conflicts between the organisational structure and clan ties, the ambitions of individual leaders and weak governance at all levels of the hierarchy.

One of the most important elements of *AQIM Playbook*[49] was the principle of avoiding the repetition of mistakes previously made by other jihadist groups. Abdelmalek Droukdel, long-serving emir of AQIM, killed in 2020 by French forces, warned against actions that could trigger foreign intervention and thus damage the long-term interests of the movement. He foresaw the potential consequences of expanding too quickly – particularly in the context of the events of 2013, when the spread of jihadist insurgency to the south of Mali prompted France to launch the "Serval" operation[50]. Droukdel warned commanders against a rapid march to Bamako, as he decided that such action could provoke international intervention. This cautious strategy, however, became a source of tension within AQIM and between AQIM and some allied groups that favoured a more aggressive operational approach.

From the perspective of AQIM, one of the main mistakes made by earlier jihadist movements was to impose harsh Shariah-based punishments too quickly and to prematurely implement quasi-state structures based on

[48] C. Weiss, *AQIM's Imperial Playbook. Understanding al-Qa'ida in the Islamic Maghreb's Expansion into West Africa*, n.p., April 2022, https://ctc.westpoint.edu/wp-content/uploads/2022/04/AQIMs-Imperial-Playbook.pdf [accessed: 5 I 2025].

[49] *AQIM Playbook* – a term used to describe strategies, tactics and methods of operation used by AQIM. It refers to the group's operational, propaganda and recruitment schemes, developed on the basis of its experience in Northern Africa and the Sahel. Abdelmalek Droukdel played an important role in the creation and implementation of *AQIM Playbook*. As the emir of Al-Qaeda in the Islamic Maghreb from 2004 until his death in 2020, he was the organisation's chief strategist and ideologue.

[50] T. Joscelyn, *Analysis: Al Qaeda groups…*

Islamic emirate principles. This approach, according to this organisation, led to the loss of popular support and the collapse of the jihadist state project. After starting the French Operation Barkhane in 2014, AQIM adopted a more cautious strategy and focused on winning the support of local communities. These measures have brought tangible results, particularly in areas lacking effective state management. The withdrawal of French troops from Mali (2022), Burkina Faso and Niger (2023) has reinforced the belief among AQIM supporters that their long-term strategy is bearing fruit and that the idea of creating an Islamic emirate in the region is once again viable[51].

In recent years, Burkina Faso has become a major area of JNIM activity and expansion. This process began in 2016, when Katiba Macina, a unit of AQIM trained by Al-Qaeda, supported by its recruits, finances and command, quickly gained influence in this country. This was fostered by the lack of a coherent political vision among the state elite, the inability of the military to fight the uprisings effectively and the apparent reluctance of the French forces to engage directly. After a series of coups in Burkina Faso and after the forced withdrawal of France, jihadists greatly expanded their territorial gains at the request of the new junta[52]. Terrorists have surrounded the capital, Ouagadougou, seized the country's main roads and cut off access to cities. The situation in Burkina Faso has implications for other countries in the region who feel threatened by terrorism[53].

Al-Qaeda is able to carry out attacks to the north and south, such as in Togo and Benin, and infiltrate the W-Arly-Pendjari National Park complex, which includes the Gulf of Guinea and West African countries. The number of terrorist attacks has steadily increased since 2022, especially in the countries bordering the Gulf of Guinea[54]. An increase in the intensity

[51] H. Nsaibia, *Actor Profile: Jama'at Nusrat al-Islam wal-Muslimin (JNIM)*, Armed Conflict Location & Event Data, 13 XI 2023, https://acleddata.com/2023/11/13/actor-profile-jamaat-nusrat-al-islam-wal-muslimin-jnim/ [accessed: 5 I 2025].

[52] *Deaths Linked to Militant Islamist Violence in Africa Continue to Spiral*, Africa Center for Strategic Studies, 29 I 2024, https://africacenter.org/spotlight/mig2024-deaths-militant-islamist-violence-africa-rise/ [accessed: 5 I 2025].

[53] S. Douce, *Burkina Faso's Djibo city struggles under jihadist siege*, La Croix International, 7 XI 2024, https://international.la-croix.com/world/burkina-fasos-djibo-city-struggles-under-jihadist-siege [accessed: 5 I 2025].

[54] J. Zenn, *Brief: JNIM Attacks in Benin Represented Group's Growing Operational Strength in Periphery*, The Jamestown Foundation, 11 XII 2024, https://jamestown.org/program/brief-jnim-attacks-in-benin-represented-groups-growing-operational-strength-in-periphery/ [accessed: 5 I 2025].

of attacks and success in securing roads and key communication points in the south-east of Burkina Faso in 2024 meant that in 2025 the Al-Qaeda was confidently entering northern Benin and strenghtening its position in the country. According to Critical Threats, more than 157 people were killed in attacks there in the first four months of 2025, this is 50 more than in 2024, and statistics indicate that by the end of 2025 the number of victims could increase up to fivefold[55]. Due to dynamically changing situation and fragility of the state structures in Togo and Benin, further empowerment of jihadists and the establishment of operational bases by them will have direct consequences for states of the Sahel. This region, already struggling to cope with the increasingly dense network of supply routes used by the terrorist group, may not be able to effectively counter their further expansion.

Niger is heavily influenced by groups operating in Mali and Libya borderlands and the Lake Chad basin. The poor, strategically located country has been home to French and US forces for years and has served as a key Western partner in counter-terrorism operations in the region of the Sahel. The US drone base in Agadez was the largest of its kind in the region[56]. It was set up to monitor terrorist groups and support Niger in its fight against them. In recent years, this has mainly been ISIS.

The presence of ISIS in the Sahel has been controversial from the outset among the jihadists. The conflict for dominance between Al-Qaeda and ISIS in the Sahel initially took a unique form. Despite their growing importance of ISIS, particularly in Mali, the two organisations, i.e. JNIM (related to Al-Qaeda) and the local ISIS factions, avoided an open clash for a long time. This state of affairs has come to be known as Sahelian exceptionalism[57]. This term, denoting the coexistence of two competing organisations in one

[55] L. Karr, *Africa File, April 24, 2025: JNIM's Growing Pressure on Benin; Turkey to Somalia; Salafi-Jihadi Cells Continue to Grow Across Nigeria*, Critical Threats, 24 IV 2025, https://www.understandingwar.org/backgrounder/africa-file-april-24-2025-jnim%E2%80%99s-growing-pressure-benin-turkey-somalia-salafi-jihadi/ [accessed: 20 V 2025].

[56] M. Banchereau, *US hands over its last military base in Niger to the ruling junta*, The Associated Press, 7 VIII 2024, https://apnews.com/article/niger-united-states-troops-army-military-bases-junta-sahel-coup-1ae5334bc68eb6b45e1e2d612bfb2b6f [accessed: 5 I 2025]; *US troops pull out of Niger's Air Base 101*, Reuters, 8 VII 2024, https://www.reuters.com/world/africa/us-troops-pull-out-nigers-air-base-101-2024-07-07/ [accessed: 5 I 2025].

[57] W. Nasr, *ISIS in Africa: The End of the "Sahel Exception"*, New Lines Institute, 2 VI 2020, https://newlinesinstitute.org/nonstate-actors/isis-in-africa-the-end-of-the-sahel-exception [accessed: 10 I 2025].

region, which is unusual for global jihadism, was coined by the French journalist Wassim Nasr.

By the end of 2019 JNIM and Malian ISIS cells (mainly ISGS) avoided direct confrontation, and one could even see the signs of local cooperation in selected areas[58]. However, in 2020 JNIM, which saw the growing strength of ISGS and the exodus of fighters to this faction, decided to clash openly and forged closer ties with the global Al-Qaeda structure. Since then, the conflict between JNIM and ISGS has developed into a regular war, interrupted only by occasional ceasefires and ad hoc agreements of a tactical nature[59].

Between 2022 and 2023 both the army of Mali with the support of the French, and Al-Qaeda made attempts to defeat ISGS[60]. Although these forces are hostile to each other, they were united by the goal of reducing ISGS's influence in the region. The Islamic State is known for a more brutal and restrictive government than Al-Qaeda, which is due in part to the more rigorous approach to the *takfir* doctrine. The Muslims, who deviate from the true faith, as interpreted by ISIS, are considered infidels by them. This interpretation allows them to justify violence not only against ideological opponents, but also against local populations who do not accept ISIS authority[61].

A new phase in the activities of ISIS may be evidenced by the armed drone attack carried out in Nigeria in December 2024. This was the first action of its kind on such a large scale[62]. In 2025, ISIS will probably try to extend its influence in the Sahel and directly in Nigeria, where the largest branch of ISWAP organisation at the moment is located, which has made no secret of its ambitions for Nigeria, Chad, Niger and Cameroon territory and is trying to restore power over areas lost under Abu Bakar Shekau the leader of organisation Boko Haram.

---

58 H. Nsaibia, C. Weiss, *The End of the Sahelian Anomaly*...

59 Ibid.

60 *Islamic State group nearly doubled its Mali territory in under a year, UN says*, France 24, 26 VIII 2023, https://www.france24.com/en/africa/20230826-islamic-state-group-doubled-controlled-territory-in-mali-in-under-a-year-un-experts-say [accessed: 5 I 2025].

61 J. Kadivar, *Exploring Takfir, Its Origins and Contemporary Use: The Case of Takfiri Approach in Daesh's Media*, "Sage Journals" 2020, vol. 7, no. 3, https://journals.sagepub.com/doi/full/10.1177/2347798920921706 [accessed: 5 I 2025]. https://doi.org/10.1177/2347798920921706.

62 T. David, *Troops Foil Boko Haram, ISWAP Drone Attack In Buni Gari*, Leadership, https://leadership.ng/troops-foil-boko-haram-iswap-drone-attack-in-buni-gari/ [accessed: 5 I 2025].

There has been a marked increase in ISGS activity in Morocco, Algeria and Spain over the past two years. ISGS, like other ISIS factions, is developing and testing various operational strategies and aims to become an independently operating structure capable of conducting promotional and recruitment activities, as well as coordinating international fighters. The aim of these activities is to gradually shift the axis of jihad towards Europe.

Cells established in North Africa are to target Mali, where ISGS has its territory[63]. In January 2025, the Moroccan services foiled an attempted ISGS operation on its territory. Terrorists preparing for attacks who were in contact with jihadists of the Islamic State in Mali were arrested[64]. In February 2025, the Moroccans again dismantled the ISGS network, carrying out an operation in nine cities. New ISGS plans came to light, coordinated from Mali by foreign fighters of Arab origin, who formed a special committee to establish contacts abroad and enlist recruits[65]. Through a network of cross-border links, ISGS smuggled weapons hidden in special caches into Morocco. It was supposed to have been picked up – by providing GPS coordinates – by the jihadists planning large-scale attacks[66]. This is an example of one of the many terrorist operations Spaniards and Moroccans broke up together in 2023–2025[67].

In 2024, the Islamic State – Khorasan Province (ISKP) attracted the most attention from the international community, mainly due to its growing ability to influence various groups and diasporas, and its effectiveness in infiltrating Europe by sending there agents and supporters[68].

---

[63] A.Y. Zelin, *The Islamic State on the March in Africa*, The Washington Institute for Near East Policy, 1 III 2024, https://www.washingtoninstitute.org/policy-analysis/islamic-state-march-africa [accessed: 5 I 2025].

[64] S. Kasroui, *Morocco's BCIJ Foils Terrorist Plot, Arrests 4 ISIS-Affiliated Suspects Near Casablanca*, Marocco World News, 26 I 2025, https://www.moroccoworldnews.com/2025/01/367913/morocco-s-bcij-foils-terrorist-plot-arrests-4-isis-affiliated-suspects-near-casablanca [accessed: 20 V 2025].

[65] *Morocco: ISIS-instigated plot foiled, 12 suspects arrested*, The North Africa Post, 19 II 2025, https://northafricapost.com/84516-morocco-isis-instigated-terror-plot-foiled-12-suspects-arrested.html [accessed: 20 V 2025].

[66] I. Toutate, *BCIJ Links 'Highly Dangerous' Foiled Terror Plot to Sahel Terrorist Groups*, Morocco World News, 24 II 2025, https://www.moroccoworldnews.com/2025/02/174948/bcij-links-highly-dangerous-foiled-terror-plot-to-sahel-terrorist-groups/ [accessed: 20 V 2025].

[67] A. Zelin, *The Islamic State on the March*...

[68] A. Jadoon et al., *From Tajikistan to Moscow and Iran: Mapping the Local and Transnational Threat of Islamic State Khorasan*, "CTC Sentinel" 2024, vol. 17, no. 5, https://ctc.westpoint.

A new campaign by jihadists in 2025 poses the threat to tourists in Maghreb and the Sahel, and thus to the lucrative tourism business. The kidnappings of Europeans in Algeria, Chad and Niger are a warning sign[69]. Based on what has happened so far, it can be assumed that in 2026 there is a likelihood that one of the terrorist groups will seize a major city in Mali or Burkina Faso. It appears that in the first half of 2025 Al-Qaeda is preparing the ground for lasting rule. An example of this is the city of Djibo, under siege for three years and exhausted by heavy attacks[70]. The consequence will be an escalation of the conflict, unseen for a decade, and the creation of a new terrorist "state", markedly different from the rule of Hayat Tahrir al-Sham in Syria or Taliban in Afghanistan by its expansive nature.

If Al-Qaeda or ISIS jihadists manage to bring down the authorities in any of the countries that make up AES Alliance, there is a serious risk of a domino effect destabilising the other members of the agreement. The most alarming situation is currently in Burkina Faso, where the spread of terrorist groups poses a direct threat to neighbouring countries in the region as well[71].

Even the newly elected President of Senegal, Bassirou Diomaye Faye, who was initially seen as an adversary of the West because of his stance towards international economic and political institutions, called for European support in 2024, which clearly shows the scale of the threat. In order to prevent further escalation, a coordinated and long-term stabilisation initiative is needed, with the participation of the largest countries in the Economic Community of West African States (ECOWAS), particularly Nigeria. It should include security measures, institutional support and integration of political and economic activities for development of the region. It is also worth considering the possibility of the EU

edu/from-tajikistan-to-moscow-and-iran-mapping-the-local-and-transnational-threat-of-islamic-state-khorasan/ [accessed: 5 I 2025].

[69] P. Wójcik, entry on the portal X, 19 I 2025, https://x.com/SaladinAlDronni/status/1881013944443363547 [accessed: 24 I 2025].

[70] *Al Qaeda affiliate says 200 soldiers killed in Burkina Faso attack*, Reuters, 16 V 2025, https://www.reuters.com/world/africa/al-qaeda-affiliate-says-200-soldiers-killed-attack-burkina-military-site-reports-2025-05-15/ [accessed: 16 V 2025].

[71] J. Wójcik, *Sahel pogrąża się w terrorystycznej rebelii* (Eng. The Sahel plunges in a terrorist rebellion), Defence24, 30 IX 2023, https://defence24.pl/geopolityka/sahel-pograza-sie-w-terrorystycznej-rebelii [accessed: 12 XII 2024].

organising a training mission, which will prepare African countries to counter terrorism primarily at the political level, but will also include specialised training for counter-terrorism groups.

The presence in the Sahel of countries outside the region

Since 2013, France has played the most important role in counter-terrorism and stabilisation in the Sahel for more than a decade, mainly through Operation Barkhane and Mission Takuba. This involvement included Mali, Niger, Chad and Burkina Faso, where the French trained local forces and supported their fight against the jihadists. However, diplomatic tensions, especially after the military coups d'état in Mali in 2020 and 2021, led to the withdrawal of French troops in 2022[72]. France is now re-evaluating its strategy with an emphasis on European partnerships and a limited military presence in Africa.

Germany's efforts to stabilise the situation in the Sahel focus on UN peacekeeping missions and diplomatic initiatives such as the Sahel Plus. Germany is cooperating with neighbouring countries of the region, including Senegal, Ghana and Togo, to reduce migration and promote peace. Berlin is considering further military involvement, although his priority is EU coordination[73]. Germany is betting on dialogue and negotiation, which can help maintain stability in the region.

Spain, through EUTM Mali mission, played a significant role in the training of Mali armed forces. The Spaniards deployed there more than 8300 soldiers and supported counter-terrorist operations[74]. Although Madrid has extensive military and diplomatic experience in the region, and cooperates with Maghreb countries, e.g. on the former colony in Western Sahara, contested today by Morocco and the Polisario Front organisation, is now focused on securing the Mediterranean Sea and maintaining its

[72] A. Olech, *French Operation Barkhane in Africa – success or failure?*, Stosunki Międzynarodowe – International Relations, 18 XII 2023, https://internationalrelations-publishing.org/articles/3-17 [accessed: 3 XII 2024]. https://doi.org/10.12688/stomiedintrelat.17737.1.

[73] *The Federal Government realigns its Sahel policy*, Federal Foreign Office, 3 V 2023, https://www.auswaertiges-amt.de/en/newsroom/news/2595298-2595298 [accessed: 4 XII 2024].

[74] L.M. Sanjuan, *Los soldados más temidos del mundo: hay una unidad española*, AS, 24 X 2024, https://as.com/actualidad/politica/los-soldados-mas-temidos-del-mundo-n [accessed: 4 XII 2024].

economic influence in Africa. The lack of a clear strategy to return to the Sahel suggests that Spanish involvement in the region will decrease.

Italy gradually increased its presence in Africa by opening new embassies and intensifying diplomatic visits. In 2023, in the face of political instability, Italy reduced their forces in Niger, but remains there and represents the EU and tries to maintain influence in the country despite its aggressive attitude towards the West. Italy also remains in Chad and is involved in training local units and working with European partners. Its strategy includes reducing illegal migration and strengthening relations with Maghreb countries[75]. Italy combines humanitarian aid with diplomacy, which is conducive to their positive perception in the region.

Turkey is increasing its influence in the Sahel. It is supplying drones and helping in the fight against terrorism, by which it supports the efforts of NATO [76]. At the same time a private military company Sadat sends mercenaries to regions of conflict and protects critical infrastructure, for instance in Niger. Ankara focuses on economic development, invests in infrastructure projects and expands embassy network[77]. Its strategy, which is less dependent on the resolution of human rights issues by states in the Sahel, makes it an attractive partner for African governments seeking an alternative to the partnership of the West.

The United Arab Emirates (UAE) strengthen cooperation with Chad, to which they supply military equipment and where their troops are stationed. The role of the UAE as a new partner in providing security in the region is important, especially for local leaders who need to replace the traditional alliance with France. The Emirates can become a model for other Arab states, for instance Saudi Arabia. They can also fill the gap left by the withdrawal of France.

Estonia sent its troops to Mali, as part of the Operation Barkhane, to support counter-terrorism efforts in cooperation with international

[75] J. Renoult, *L'Italie, dernier partenaire occidental du Niger*, Le Monde, 23 VII 2024, https://www.lemonde.fr/afrique/article/2024/07/23/l-italie-ultime-partenaire-occidental-du-niger_6256111_3212.html [accessed: 6 XII 2024].

[76] *Sahel Showdown: How Türkiye Can Help NATO With Russian and Chinese Advances*, TRT World Research Centre, 29 VII 2024, https://researchcentre.trtworld.com/featured/perspectives/sahel-showdown-how-turkiye-can-help-nato-with-russian-and-chinese-advances/ [accessed: 10 XII 2024].

[77] B. Roger, T. Eydoux, *Drones turcs, avions russes… au Sahel, la guerre des airs est déclarée*, Le Monde, 20 XI 2024, lemonde.fr/afrique/article/2024/11/20/drones-turcs-avions-russes-au-sahel-la-guerre-des-airs-est-declaree_6405083_3212.html [accessed: 7 XII 2024].

partners. The country's engagement in Africa also includes digitalisation and e-governance initiatives as part of Estonia's broader foreign policy strategy for 2020–2030[78]. Despite the withdrawal of the military contingent, Tallinn remains open to future military missions and the development of cooperation with the African Union – with a particular focus on innovative partnerships in the areas of digital technology, sustainable development and energy transition.

The US focused on countering terrorism. They built an air base in Agadez and invest millions of dollars in training local forces. The coup in Niger in 2023 led to the withdrawal of the US troops, which has weakened the influence of the US in the region[79]. Russia took advantage of the situation. Through military cooperation and the location of private military companies in former French colonies, usually ruled by authoritarian governments, it seeks to challenge the dominance of the US in Africa.

France and the US, despite their common goal of fighting terrorism, often acted independently, which undermined their effectiveness. The lack of coordination has left the region unstable, despite huge investments in security. The two countries should step up their cooperation to respond more effectively to threats in the Sahel region, especially with the growing influence of Russia and China[80].

The Chinese have become the main weapon supplier for Burkina Faso[81]. It usually ends up in the hands of Al-Qaeda, which means that this group has more resources to implement its plans. The EU countries should therefore consider various forms of support for the Gulf of Guinea

[78] *Estonia's strategy for Africa*, Republic of Estonia Ministry of Foreign Affairs, 7 V 2021, https://vm.ee/en/estonias-strategy-africa [accessed: 11 XII 2024].

[79] M.M. Phillips, B. Faucon, *U.S. Forces Try to Regroup as al Qaeda, Islamic State Sow Terror in West Africa*, The Wall Street Journal, 11 IX 2024, https://www.wsj.com/world/africa/u-s-moves-aircraft-commandos-into-west-africa-in-fight-against-islamist-militants-0b15c41b [accessed: 11 XII 2024].

[80] A. Olech, *Francja i USA będą ponownie wojskowo współpracować w Afryce* (Eng. France and the US will again cooperate militarily in Africa), Defence24, 20 II 2024, https://defence24.pl/geopolityka/francja-i-usa-beda-ponownie-wojskowo-wspolpracowac-w-afryce [accessed: 11 XII 2024].

[81] G. Martin, *Burkina Faso receives huge batch of Chinese military equipment*, Defence Web, 27 VI 2024, https://www.defenceweb.co.za/land/land-land/burkina-faso-receives-huge-batch-of-chinese-military-equipment [accessed: 12 XII 2024].

countries, in the worst case scenario re-establishing relations with the juntas in power there.

Russia and Iran have expressed an interest in developing closer relations with Niger, having the world's largest uranium deposits. The potential that the Sahel countries could use for their own development could be seized by foreign states hostile to the West.

The role of NATO in the Sahel

The Sahel region remains one of the most undervalued and marginalised areas in EU[82] and NATO[83] security policies. The dynamics of changes that have taken place there since 2021, combined with the geopolitical proximity of the Maghreb, should make Europe rethink its engagement and step up its efforts in the region. Between 2021 and 2023, most EU and international initiatives concerning the Sahel have been suspended, despite security, migration and radicalisation challenges are steadily increasing. This situation calls not only for an in-depth analysis of potential threats, but also for the development of a long-term, coherent security strategy, adapted to the realities of the region.

Both the negative experience of the NATO intervention in Libya and the failure of French military mission in the Sahel have contributed to the current reticence of Western states. The EU and NATO countries are reluctant to engage in another long-running operation that would require a coordinated response to a complex challenges in the region.

Numerous national, regional and international actors, including the armed forces of the countries of the Sahel, the African Union, ECOWAS, the UN, the EU and partners outside the continent are involved in the region, but the problem is the lack of coordination. Inconsistent approaches, competing interests and limited cooperation mechanisms make stabilisation efforts fragmented and often ineffective. Although some of NATO Member States, particularly these maintaining historic ties

[82] European Parliament, *New EU strategic priorities for the Sahel. Addressing regional challenges through better governance*, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/696161/EPRS_BRI%282021%29696161_EN.pdf [accessed: 14 XII 2024].

[83] NATO, *Strategic foresight analysis. Regional perspectives report on North Africa and the Sahel*, https://www.act.nato.int/wp-content/uploads/2023/05/NU_SFA_Report_North_Africa_and_the_Sahel_SACT_approved_final_edited_version.pdf [accessed: 14 XII 2024].

to the region, have over the years invested in the security and development of the Sahel, end of Operation Barkhane created a serious gap in the military space that remains unfilled to this day[84].

In recent years, the NATO's security efforts have mainly focused on threats occurring in the Mediterranean Sea. The Alliance has implemented training campaigns within Member States, as well as strengthening cooperation with partners from North Africa[85]. Meanwhile, the steadily increasing number of terrorist incidents in the Sahel should prompt NATO to reassess its strategy priorities and pay more attention to this volatile region. The growth of the Islamic State in Niger, Burkina Faso and Mali is of particular concern. It should be a wake-up call for policymakers and analysts dealing with trans-regional security[86].

The character of ISIS's operations makes its presence a threat not only to the countries in which it has direct structures, but also to the countries of Southern Europe, mainly those with large Moroccan, Algerian and Tunisian diasporas. There have been recent reports suggesting that ISIS is not only actively recruiting among these communities, but is also monitoring the activities of potential perpetrators of terrorist attacks on the territory of Spain[87].

The Sahel as an extension of NATO's southern flank. Implications for the Alliance

In its future strategy, NATO should treat the southern and eastern flank as areas that are interlinked. Adopting this perspective requires minimising internal disputes and promoting deeper political integration on the twin

[84] C. Doxsee, J. Thompson, M. Harris, *The End of Operation Barkhane and the Future of Counterterrorism in Mali*, Center for Strategic & International Studies, 2 III 2022, https://www.csis.org/analysis/end-operation-barkhane-and-future-counterterrorism-mali [accessed: 19 XII 2024].

[85] A. Olech, *Cooperation of the Maghreb countries with NATO for security in the region*, Instytut Nowej Europy, 12 X 2021, https://ine.org.pl/en/cooperation-of-the-maghreb-countries-with-nato-for-security-in-the-region/ [accessed: 19 XII 2024].

[86] R. Grammer, *Top counterterrorism official warns of ISIS' rapid rise in Africa*, Politico, 25 XI 2024, https://www.politico.com/news/2024/11/25/top-counterterrorism-official-warns-of-isiss-rapid-rise-in-africa-00191571 [accessed: 20 XII 2024].

[87] L. Breton, *Terrorisme: l'État islamique avait des projets d'attentats visant les Jeux olympiques de Paris et l'Euro de football*, La Depeche, 17 VI 2024, https://www.ladepeche.fr/2024/06/17/terrorisme-letat-islamique-avait-des-projets-dattentats-visant-les-jeux-olympiques-de-paris-et-leuro-de-football-12022418.php [accessed: 21 XI 2024].

tracks. The war in Ukraine has revitalised the structures of NATO, as evidenced by the accession of Finland and Sweden to the Alliance. The reason was that these countries were concerned about potential aggression from Russia[88].

This situation should prompt discussion on developing NATO strategy towards the south. The effectiveness of the new conception will depend on Alliance's ability to take action on the Sahel before there is a significant proliferation of terrorist organisations there[89]. During the NATO Summit in Vilnius in 2023, where the most important issue was the war in Ukraine, a separate document on Southern Europe was published and two of the most important threats to the Alliance – Russia and terrorist organisations were identified[90].

In the past, the activity of NATO on the southern flank was dominated by developments on the eastern flank. Member States presented different approaches to defence capacity building from Africa side, and the war in Ukraine has focused even more attention on the east. However, this should not diminish engagement and strategy development in the south. The war in Ukraine has consequences for the Mediterranean Sea, the Middle East and Africa. Russian's geopolitical inclinations and increasing competition from China have brought to light the security issues common to East and South over the past decade[91].

[88] Y. Atalan, *The Future of NATO's Southern Flank*, Center for Strategic & International Studies, 10 VII 2024, https://www.csis.org/analysis/future-natos-southern-flank [accessed: 23 XII 2024]; J. Davidson, *Four steps that NATO's southern flank strategy needs to succeed*, Atlantic Council, 25 VI 2024, https://www.atlanticcouncil.org/blogs/new-atlanticist/four-steps-that-natos-southern-flank-strategy-needs-to-succeed/ [accessed: 23 XII 2024]; A. Polyakova et al., *A New Vision for the Transatlantic Alliance: The Future of European Security, the United States, and the World Order after Russia's War in Ukrain*e, Center for European Policy Analysis, 30 XI 2023, https://cepa.org/comprehensive-reports/a-new-vision-for-the-transatlantic-alliance-the-future-of-european-security-the-united-states-and-the-world-order-after-russias-war-in-ukraine/ [accessed: 23 XII 2024].

[89] S. Colombo, I. Fakir, *NATO, North Africa, and the Sahel: Squaring the triangle of insecurity*, Middle East Institute, 5 VII 2024, https://www.mei.edu/publications/nato-north-africa-and-sahel-squaring-triangle-insecurity [accessed: 23 XII 2024].

[90] *Vilnius Summit Communiqué*, NATO, 11 VII 2023, https://www.nato.int/cps/en/natohq/official_texts_217320.htm [accessed: 23 XII 2024].

[91] Y. Atalan, *The Future of NATO's Southern Flank*...

Current priorities and challenges to NATO

Geopolitical stability of the southern flank of NATO is very important for the security of Member States: France, the US, Italy, Spain, Turkey and Greece. Its maintenance requires increased coordination and interoperability between allies operating in the region, especially in relation to the most volatile areas such as Maghreb – with a clear focus on the situation in Libya – and the Sahel. Increasing influence of Russia and China in the Middle East and Africa, as well as the growth of terrorist organisations and criminal networks point to the urgent need for NATO to adopt long-term, integrated strategy towards these regions. Counter-terrorism efforts and effective migration management should be at the centre of such an approach. This is one of the most significant challenges for the countries of the Alliance's southern flank.

The effectiveness of NATO's operations on this flank may be undermined by tensions in Greek-Turkish relations, as well as by divergences between France, Spain and Italy over involvement in further military missions in Africa. Lack of political cohesion and limited willingness to cooperate may make it difficult to develop a coordinated response to security challenges in the region.

The countries of West Africa, among others, Senegal, Cote d'Ivoire, Ghana, Togo and Benin, recognise the growing threat from terrorist organisations and are increasingly calling for urgent support from the international community. In this context, the priority for NATO and EU should be to build sustainable political and economic ties with countries on the periphery of the Sahel and to ensure security in the region. Such an approach would not only reduce their dependence on strategic investments made by China, but would also hinder the activities of Russian mercenaries and counter the information war waged by third countries. More broadly, these measures would contribute to the real strengthening of local communities and increase the resilience of the entire region.

Despite efforts over the past ten years, NATO's activities as a security guarantor in the Sahel region remain inconsistent and have limited impact. This is primarily due to the diffuse and difficult-to-define nature of the threats, which encompass not only the activities of multiple terrorist groups, but also deep-seated political, social and economic problems. Additional challenges include the Alliance's unclear ambitions for the region, the lack of internal consensus among its members and the relatively limited use of military resources.

NATO's relations with partners from North Africa and the Sahel, including Algeria, Egypt, Mauritania, Morocco and Tunisia, focused mainly on combating transnational crime and strengthening regional military capabilities. Although this cooperation has contributed to a partial reduction in the activities of terrorist groups in the Mediterranean area, it has also had the unintended consequence of shifting militant activity to the centre of the continent and strengthening terrorist structures in the Central Sahel.

The situation is complicated by the unclear and unspecified policies of West European countries, which complicate NATO's efforts through lack of consultation when taking political action. For instance, France and Spain are pursuing different policies towards Morocco and Algeria, confronting each other over the Western Sahara and hindering contact that could be used to stabilise the situation in the Sahel.

In the coming years, NATO will need to develop a coherent, realistic strategy towards the Sahel region, based on cooperation with legitimate governments, selected private military companies acting on their behalf (this may seem dangerous, but these are viable military structures) and local communities. Only such an approach can lead to the formulation of an effective strategic vision which takes into account the complexity of challenges specific to this region[92]. The Alliance is now at a turning point in terms of shaping overseas missions, following the end of its involvement in Afghanistan and Iraq, and with a limited presence in Libya, Syria and the Sahel. There is a need to reconsider the role of NATO in fragile areas and to develop new models of action that are not simply a duplication of previous interventions, but a viable response to 21st century threats.

The countries of the Sahel, facing a growing threat from terrorist organisations, are now in a situation where they have to make strategic choices: either they confront the West and the NATO structures, or they face alone a rising wave of jihadist violence that neither Russia nor China, despite their growing presence in the region, can effectively stem. This situation provides a real opportunity for Western states to rebuild influence and increase their credibility as a security partner. In the face of a changing threat architecture, NATO should consider reorganising its mission in

[92] S. D'Amato, E. Baldaro, *Does the Sahel need NATO?,* ICCT, 26 VIII 2024, https://icct.nl/publication/does-sahel-need-nato-0 [accessed: 24 XII 2024].

the region, expanding the scope of its operations and engaging more forcefully militarily in countries facing long-lasting jihadist insurgencies.

Migration

Africa is experiencing an unprecedented demographic transition as the region with the fastest population growth in the world. By 2050, the continent's population will grow from the current 1.2 billion to approx. 2.5 billion people[93]. Between 10 million and 12 million young Africans enter the labour market each year. This creates both huge development opportunities and serious challenges for the economic and education systems. More than 60% of Africa's population is under the age of 25 and these young societies have to contend with many difficulties, such as terrorism, repressive power and extreme poverty. The continent's unique demographic profile makes Africa very much at the centre of the global debate on the future of employment, education and mobility for young people. Due to the lack of prospects in the region, an increasing number of them are seeking better living conditions outside the continent and they choose mainly Europe.

One of the main factors in the migration crisis has become the threat of jihadism. These are exacerbated by the war waged by the AES Alliance against Al-Qaeda and ISIS. Following the rupture of agreements with the EU by the military governments of Mali, Niger and Burkina Faso, migration routes leading to Maghreb and the southern borders of Europe have been reactivated. Although Tunisian and Algerian administrations, supported financially by the EU, are taking steps to turn back migrants, new routes of transit are constantly developing. The fact that those moving towards Europe also include fighters linked to terrorist organisations is of great concern. This poses a serious threat to the internal security of European countries.

As climate change intensifies, the situation in Africa, especially in the Sahel region, is getting worse. Desertification and droughts are forcing millions of people from their homes, further weakening an already fragile socio-political structure. This ecological catastrophe is creating ideal

[93] *Forecast of the total population of Africa from 2020 to 2050*, Statista, 22 III 2024, https://www.statista.com/statistics/1224205/forecast-of-the-total-population-of-africa [accessed: 27 XII 2024].

conditions for extremist groups to recruit new members among displaced, desperate communities. Terrorist groups are transforming vast areas of the Sahel into their own territories, taking advantage of the ineptitude of the military juntas that have forcibly taken over governance. These areas have become impossible for the authorities to control. Europe, which is already struggling to cope with the challenges of migration, faces a double threat – a humanitarian crisis and a growing terrorism that is increasingly affecting it.

The route via Maghreb and the Mediterranean Sea to Spain, Italy and France is the most heavily trafficked migration road[94]. Due to increasing pressure on this route, migrant are increasingly using alternative corridors. One of them is the route through Russia and Belarus, from where they try to cross the EU borders and reach Lithuania, Latvia and Poland[95]. This direction, used by regimes in Minsk and Moscow as a tool of a political pressure, confronts EU border countries with both a migration crisis and security threats.

The stakes for Europe and NATO have never been higher. The lack of a coordinated international strategy in the face of the Sahel's complex challenges carries the risk of escalating crisis and a lack of control. The current situation will lead to larger migratory movements and more sophisticated terrorist operations targeting European cities. Without adequate border control mechanisms and international cooperation, migratory movements can turn into a crisis that destabilises the security system not only in border states but also in the entire EU. Migration is also a kind of weapon. Thousands of unidentified people, among whom are members of terrorist groups, have a direct influence on the security of EU and NATO countries, and in this case the possibility of military response is limited. The Alliance is therefore obliged to protect the borders[96].

[94] V. Malingre, P. Jacqué, *European Union wants to toughen fight against illegal immigration*, Le Monde, 18 X 2024, https://www.lemonde.fr/en/international/article/2024/10/18/european-union-wants-to-toughen-fight-against-illegal-immigration_6729757_4.html [accessed: 12 XII 2024].

[95] Z. Śliwa, A. Olech, *Wyzwania w kontekście migracji i kryzys na granicy polsko-białoruskiej*, "Wiedza Obronna" 2022, vol. 278, no. 1, pp. 87–105. https://doi.org/10.34752/2022-d278.

[96] Ibid.

Summary

The deterioration of the situation in the Sahel will continue in the coming years. The rise of the jihadist threat, the brutality of military regimes, climate changes and migration movements are all issues that will continue to challenge both Africa and Europe. The current state of security in the Sahel indicates a degradation of social, economic and political life. Local armies are unable to control more than 60% of their own territory[97]. There is no question of investment or development in societies that are, after all, so different from one another.

Financial aid to the countries of the region is too low. The Sahel needs a new economic development strategy and direct military assistance such as air support, permanent military bases or special operations against terrorists carried out on the territory of Africa. Leaving the terrorists and rebels to fend for themselves may seem an easy and safe solution, but in the decades to come, poorly prepared West African states will be targets for terrorist organisations, including ISIS and Al-Qaeda, which promote mainly Islamic fundamentalism.

The Sahel states are increasingly entering into new partnerships, especially with China, Russia and countries in the Arabian Peninsula. Unlike the financial support offered by Western states, which often impose conditions on transparency, democratisation and respect for human rights, the new partners do not require political change. Moreover, they provide immediate financial benefits, which for the military juntas ruling the region is an important factor in supporting the maintenance of power and control[98].

In the face of a difficult situation, the strategy for NATO is to cooperate with countries of the region. This means co-operating with countries close to the Sahel, i.e. allied to NATO and the West, in order to train the troops of African countries there and prevent terrorist groups from proliferating. Even if these activities are not directly related to the Sahel, NATO and EU countries, they will soon be forced to interact with states and organisations in Maghreb and the Sahel anyway.

---

[97] A. Antil, *Un an après sa création, une Alliance des États du Sahel qui se cherche*, IFRI, 16 IX 2024, https://www.ifri.org/fr/presse-contenus-repris-sur-le-site-presse-lien-externe-avec-citation/un-apres-sa-creation-une [accessed: 28 XII 2024].

[98] A. Olech, *The Wagner Group in Africa. The sham battle of Russian mercenaries against terrorism*, "Terrorism – Studies, Analyses, Prevention" 2024, no. 5, pp. 273–309. https://doi.org/10.4467/27204383TER.24.010.19398.

From a military point of view, it is important to maintain the presence of international forces in Africa, close to the regions where ISIS and Al-Qaeda are active, and consequently where the military authorities cooperate with Russia. This applies in particular Mali, Burkina Faso and Niger.

Military action should be complemented by support from the governments of other African countries, including those of the African Union, which are engaged in the region. Positive relations with the civilian population must be nurtured, which can result in greater respect for the law of armed conflict and the rule of law. The armed forces must exemplify the values promoted by the states of the region and enjoy the trust of the civilian population. This is lacking in Africa. The difficulty is the cultural and ethnic diversity of this continent, but even a small common denominator should be used to build an agreement.

It is worrying that after more than a decade of violence, a new phase of crisis is emerging. Although there are similarities with the situation in 2012 (before the arrival of troops from NATO and EU countries, led by Operation Barkhane) it is now a more complicated security situation in the Central Sahel. The region is increasingly unstable and at the same time the influence of international organisations in the region is diminishing. Underestimating the gravity of the situation and ignoring the build-up of complex problems in the Sahel will mean that, in a few years' time, the decisions that NATO will make in relation to the region will only have a military mission dimension. The contemporary crisis in the Sahel must therefore not go unanswered. The first step should be the development of a political presence in the region, followed by the training of African soldiers and then the implementation of measures to effectively monitor and manage the situation in order to minimise the losses, above all in terms of human lives.

It is necessary to take advantage of the existing opportunity, as the threat of terrorism is increasing in Europe. The Russian Federation and other states hostile to the Alliance are pursuing a very active policy in the Sahel region, which requires a strong response from NATO and partners. The challenge of simultaneous engagement on eastern and southern flanks may prove too much for the Alliance and EU.

Bibliography

As-Sazid S., *Emerging Security Challenges in the Sahel and the Need for an Adaptative Approach towards Peacebuilding*, "International Day of United Nations Peacekeepers Journal" 2023, vol. 9, no. 9, pp. 17–34.

Benjaminsen T.A., Svarstad H., *Climate Change, Scarcity and Conflicts in the Sahel*, in: T.A. Benjaminsen, H. Svarstad, *Political Ecology. A Critical Engagement with Global Environmental Issues*, n.p. 2021, pp. 183–205. https://doi.org/10.1007/978-3-030-56036-2_8.

Lounnas D., *Le djihadisme au Sahel après la chute de Daech*, "Politique étrangère" 2019, no. 2, pp. 105–114.

Olech A., *Grupa Wagnera w Afryce* (Eng. The Wagner Group in Africa), Defence24.

Olech A., *The Wagner Group in Africa. The sham battle of Russian mercenaries against terrorism*, "Terrorism – Studies, Analyses, Prevention" 2024, no. 5, pp. 273–309. https://doi.org/10.4467/27204383TER.24.010.19398.

Śliwa Z., Olech A., *Wyzwania w kontekście migracji i kryzys na granicy polsko-białoruskiej* (Eng. Challenges in the context of migration and the Polish-Belarus border crisis), "Wiedza Obronna" 2022, vol. 278, no. 1, pp. 87–105. https://doi.org/10.34752/2022-d278.

Internet sources

Al Qaeda affiliate says 200 soldiers killed in Burkina Faso attack, Reuters, 16 V 2025, https://www.reuters.com/world/africa/al-qaeda-affiliate-says-200-soldiers-killed--attack-burkina-military-site-reports-2025-05-15/ [accessed: 16 V 2025].

Antil A., *Un an après sa création, une Alliance des États du Sahel qui se cherche*, IFRI, 16 IX 2024, https://www.ifri.org/fr/presse-contenus-repris-sur-le-site-presse-lien--externe-avec-citation/un-apres-sa-creation-une [accessed: 28 XII 2024].

Atalan Y., *The Future of NATO's Southern Flank*, Center for Strategic & International Studies, 10 VII 2024, https://www.csis.org/analysis/future-natos-southern-flank [accessed: 23 XII 2024].

Banchereau M., *US hands over its last military base in Niger to the ruling junta*, The Associated Press, 7 VIII 2024, https://apnews.com/article/niger-united-states--troops-army-military-bases-junta-sahel-coup-1ae5334bc68eb6b45e1e2d612bfb2b6f [accessed: 5 I 2025].

Bhattacharya S., *China's Great Game in the Sahel*, Vivekananda International Foundation, 12 X 2022, https://www.vifindia.org/article/2022/china-s-great-game-in-the-sahel [accessed: 7 XII 2024].

Bihan J. le, *Former Niger minister launches movement to overthrow junta*, The Africa Report, 27 IX 2024, https://www.theafricareport.com/363047/former-niger-minister-launches-movement-to-overthrow-junta/ [accessed: 5 I 2025].

Borrell J., *Together for the security, stability and development of the Sahel*, European Union External Action, 8 V 2020, https://www.eeas.europa.eu/eeas/together-security-stability-and-development-sahel_en [accessed: 27 V 2025].

Breton L., *Terrorisme: l'État islamique avait des projets d'attentats visant les Jeux olympiques de Paris et l'Euro de football*, La Depeche, 17 VI 2024, https://www.ladepeche.fr/2024/06/17/terrorisme-letat-islamique-avait-des-projets-dattentats-visant-les-jeux-olympiques-de-paris-et-leuro-de-football-12022418.php [accessed: 21 XI 2024].

Burkina Faso: Unlawful Killings, 'Disappearances' by the Army, Human Rights Watch, 29 VI 2023, https://www.hrw.org/news/2023/06/29/burkina-faso-unlawful-killings-disappearances-army [accessed: 5 I 2025].

Center for Preventive Action, *Violent Extremism in the Sahel*, Council on Foreign Relations, 23 X 2024, https://www.cfr.org/global-conflict-tracker/conflict/violent-extremism-sahel [accessed: 16 XII 2024].

Colombo S., Fakir I., *NATO, North Africa, and the Sahel: Squaring the triangle of insecurity*, Middle East Institute, 5 VII 2024, https://www.mei.edu/publications/nato-north-africa-and-sahel-squaring-triangle-insecurity [accessed: 23 XII 2024].

Crisis in Burkina Faso: What you need to know and how you can help, International Rescue Committee, 14 II 2024, https://www.rescue.org/article/crisis-burkina-faso-what-you-need-know-and-how-you-can-help [accessed: 5 I 2025].

Czerep J., *Konsekwencje powołania Konfederacji Państw Sahelu* (Eng. The consequences of establishment of the Confederation of Sahel States), Polski Instytut Spraw Międzynarodowych, 14 VIII 2024, https://www.pism.pl/publikacje/konsekwencje-powolania-konfederacji-panstw-sahelu [accessed: 15 I 2025].

D'Amato S., Baldaro E., *Does the Sahel need NATO?*, ICCT, 26 VIII 2024, https://icct.nl/publication/does-sahel-need-nato-0 [accessed: 24 XII 2024].

David T., *Troops Foil Boko Haram, ISWAP Drone Attack In Buni Gari*, Leadership, https://leadership.ng/troops-foil-boko-haram-iswap-drone-attack-in-buni-gari/ [accessed: 5 I 2025].

Davidson J., *Four steps that NATO's southern flank strategy needs to succeed*, Atlantic Council, 25 VI 2024, https://www.atlanticcouncil.org/blogs/new-atlanticist/four-steps-that-natos-southern-flank-strategy-needs-to-succeed/ [accessed: 23 XII 2024].

Deaths Linked to Militant Islamist Violence in Africa Continue to Spiral, Africa Center for Strategic Studies, 29 I 2024, https://africacenter.org/spotlight/mig2024-deaths-militant-islamist-violence-africa-rise/ [accessed: 5 I 2025].

Defining a New Approach to the Sahel's Military-led States, International Crisis Group, 22 V 2025, https://www.crisisgroup.org/africa/sahel/burkina-faso-mali-niger/defining-new-approach-sahels-military-led-states [accessed: 27 V 2025].

Desert to Power initiative, African Development Bank Group, https://www.afdb.org/en/topics-and-sectors/initiatives-partnerships/desert-power-initiative [accessed: 15 XII 2024].

Dieng A., *The Sahel: Challenges and opportunities*, "International Review of the Red Cross" 2021, vol. 103, no. 918, pp. 765–779, https://international-review.icrc.org/articles/editorial-the-sahel-challenges-opportunities-adama-dieng-918 [accessed: 15 XII 2024]. https://doi.org/10.1017/S1816383122000339.

Douce S., *Burkina Faso's Djibo city struggles under jihadist siege*, La Croix International, 7 XI 2024, https://international.la-croix.com/world/burkina-fasos-djibo-city-struggles-under-jihadist-siege [accessed: 5 I 2025].

Doxsee C., Thompson J., Harris M., *The End of Operation Barkhane and the Future of Counterterrorism in Mali*, Center for Strategic & International Studies, 2 III 2022, https://www.csis.org/analysis/end-operation-barkhane-and-future-counterterrorism-mali [accessed: 19 XII 2024].

Duhamel J., *Central Sahel – Map of jihadist militant groups activity (Jan–May 2024)*, Jules Duhamel, 21 VI 2024, https://www.julesduhamel.com/central-sahel-map-of-jihadist-militant-groups-activity-jan-may-2024/ [accessed: 15 I 2025].

Ecological Threat Report 2024. Analysing ecological threats, resilience & peace, The Institute for Economics & Peace, https://www.economicsandpeace.org/wp-content/uploads/2024/10/ETR-2024-web.pdf [accessed: 15 XII 2024].

Ehl D., *How the Russian Wagner Group is entrenching itself in Africa*, Deutsche Welle, 27 X 2024, https://www.dw.com/en/russia-kremlin-wagner-group-influence-in-central-african-republic-sudan-mali/a-70599853 [accessed: 5 I 2025].

Estonia's strategy for Africa, Republic of Estonia Ministry of Foreign Affairs, 7 V 2021, https://vm.ee/en/estonias-strategy-africa [accessed: 11 XII 2024].

European Parliament, *New EU strategic priorities for the Sahel. Addressing regional challenges through better governance*, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/696161/EPRS_BRI%282021%29696161_EN.pdf [accessed: 14 XII 2024].

Fakhry A., *More than borders: effects of EU interventions on migration in the Sahel*, Institute for Security Studies, 16 VIII 2023, https://issafrica.org/research/west-africa-report/more-than-borders-effects-of-eu-interventions-on-migration-in-the-sahel [accessed: 30 XII 2024].

Fleming L., Issoufou T.I., *Niger confirms anti-junta rebels behind oil attack*, BBC, 22 VI 2024, https://www.bbc.com/news/articles/c511n4edl7lo [accessed: 5 I 2025].

Forecast of the total population of Africa from 2020 to 2050, Statista, 22 III 2024, https://www.statista.com/statistics/1224205/forecast-of-the-total-population-of-africa [accessed: 27 XII 2024].

G5 Sahel Region: Country Climate and Development Report – Annex, World Bank Group, https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099150106302237600/p1773430dc79a10c09f600cf2ac1e0e9f3 [accessed: 27 V 2025].

Global Terrorism Index 2025, Institute for Economics & Peace, https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf [accessed: 27 V 2025].

Grammer R., *Top counterterrorism official warns of ISIS' rapid rise in Africa*, Politico, 25 XI 2024, https://www.politico.com/news/2024/11/25/top-counterterrorism-official-warns-of-isiss-rapid-rise-in-africa-00191571 [accessed: 20 XII 2024].

Hauchard A., *In Violence-shattered Central Mali, Victims Recount Their Lives*, Barron's, 9 II 2022, https://www.barrons.com/news/in-violence-shattered-central-mali-victims-recount-their-lives-01644458408 [accessed: 5 I 2025].

Ibrahim H.O., *The Sahel – a Land of Opportunity*, United Nations, 10 VI 2019, https://unpartnerships.un.org/news/2019/sahel-land-opportunity [accessed: 14 XII 2024].

Independent expert group supporting NATO's comprehensive and deep reflection process on the southern neighbourhood. Final Report. May 2024, NATO, https://nato.int/nato_static_fl2014/assets/pdf/2024/5/pdf/240507-NATO-South-Report.pdf [accessed: 16 XII 2024].

Islamic State group nearly doubled its Mali territory in under a year, UN says, France 24, 26 VIII 2023, https://www.france24.com/en/africa/20230826-islamic-state-group-doubled-controlled-territory-in-mali-in-under-a-year-un-experts-say [accessed: 5 I 2025].

Jadoon A., Sayed A., Webber L., Valle R., *From Tajikistan to Moscow and Iran: Mapping the Local and Transnational Threat of Islamic State Khorasan*, "CTC Sentinel" 2024, vol. 17, no. 5, https://ctc.westpoint.edu/from-tajikistan-to-moscow-and-iran-mapping-the-local-and-transnational-threat-of-islamic-state-khorasan/ [accessed: 5 I 2025].

Jeannin M., *Ghana worries about rise of terrorist threat in Gulf of Guinea*, Le Monde, 7 VI 2022, https://www.lemonde.fr/en/le-monde-africa/article/2022/06/07/ghana-concerned-about-extension-of-terrorist-threat-to-coastal-states-of-gulf-of-guinea_5985936_124.html [accessed: 5 I 2025].

Joscelyn T., *Analysis: Al Qaeda groups reorganize in West Africa*, FDD's Long War Journal, 13 III 2017, https://www.longwarjournal.org/archives/2017/03/analysis-al-qaeda-groups-reorganize-in-west-africa.php [accessed: 5 I 2025].

Kadivar J., *Exploring Takfir, Its Origins and Contemporary Use: The Case of Takfiri Approach in Daesh's Media*, "Sage Journals" 2020, vol. 7, no. 3, https://journals.sagepub.com/doi/full/10.1177/2347798920921706 [accessed: 5 I 2025]. https://doi.org/10.1177/2347798920921706.

Karr L., *Africa File, April 24, 2025: JNIM's Growing Pressure on Benin; Turkey to Somalia; Salafi-Jihadi Cells Continue to Grow Across Nigeria*, Critical Threats, 24 IV 2025, https://www.understandingwar.org/backgrounder/africa-file-april-24-2025-jnim%E2%80%99s-growing-pressure-benin-turkey-somalia-salafi-jihadi/ [accessed: 20 V 2025].

Kasroui S., *Morocco's BCIJ Foils Terrorist Plot, Arrests 4 ISIS-Affiliated Suspects Near Casablanca*, Marocco World News, 26 I 2025, https://www.moroccoworldnews.com/2025/01/367913/morocco-s-bcij-foils-terrorist-plot-arrests-4-isis-affiliated-suspects-near-casablanca [accessed: 20 V 2025].

Kum P., *Niger: L'ancien rebelle nigérien, Rhissa Ag Boula, annonce son intention de reprendre les armes pour chasser les putschistes*, Alwihda Info, 21 VIII 2023, https://www.alwihdainfo.com/Niger-L-ancien-rebelle-nigerien-Rhissa-Ag-Boula-annonce-son-intention-de-reprendre-les-armes-pour-chasser-les_a125857.html [accessed: 5 I 2025].

Maclean R., Jammeh S., *Africa Received Billions in U.S. Aid. Here's What It Will Lose*, The New York Times, 8 III 2025, https://www.nytimes.com/2025/03/08/world/africa/africa-usaid-funds.html/ [accessed: 20 IV 2025].

Mali and Niger rebels met to 'strengthen' ties amid political turmoil, Al Arabiya News, 2 IX 2024, https://english.alarabiya.net/News/world/2024/09/02/mali-and-niger-rebels-met-to-strengthen-ties-amid-political-turmoil [accessed: 5 I 2025].

Malingre V., Jacqué P., *European Union wants to toughen fight against illegal immigration*, Le Monde, 18 X 2024, https://www.lemonde.fr/en/international/article/2024/10/18/european-union-wants-to-toughen-fight-against-illegal-immigration_6729757_4.html [accessed: 12 XII 2024].

Marangio R., *Sahel reset: time to reshape the EU's engagement*, European Union Institute for Security Studies, 5 II 2024, https://www.iss.europa.eu/publications/briefs/sahel-reset-time-reshape-eus-engagement [accessed: 15 XII 2024].

Martin G., *Burkina Faso receives huge batch of Chinese military equipment*, Defence Web, 27 VI 2024, https://www.defenceweb.co.za/land/land-land/burkina-faso-receives-huge-batch-of-chinese-military-equipment [accessed: 12 XII 2024].

McMakin W., *UN food agency says 40 million people are struggling to feed themselves in West and Central Africa*, AP, 20 XII 2024, https://apnews.com/article/africa-food-insecurity-hunger-304b66ef7b9b56262fe1114a4b28c7e6 [accessed: 26 XII 2024].

Military juntas in Africa's 'coup belt' fail to contain extremist violence, Financial Times, 24 XI 2024, https://www.ft.com/content/d0af5533-ecdd-4be0-bbb8-e5b3e4bb11b4 [accessed: 30 XII 2024].

Mintoiba F., *Footsteps of change: Rising influence of China and Russia in Africa*, Daily Sabah, 3 X 2024, https://www.dailysabah.com/opinion/op-ed/footsteps-of-change--rising-influence-of-china-and-russia-in-africa [accessed: 7 XII 2024].

More than 50 million in West and Central Africa at risk of hunger, United Nations, 9 V 2025, https://news.un.org/en/story/2025/05/1163086 [accessed: 30 V 2025].

Morocco: ISIS-instigated plot foiled, 12 suspects arrested, The North Africa Post, 19 II 2025, https://northafricapost.com/84516-morocco-isis-instigated-terror-plot--foiled-12-suspects-arrested.html [accessed: 20 V 2025].

Moscow's winning return to Africa, Le Monde, 21 VIII 2024, https://www.lemonde.fr/en/international/article/2024/08/21/moscow-s-winning-return-to-africa_6719241_4.html [accessed: 7 XII 2024].

Nasr W., *ISIS in Africa: The End of the "Sahel Exception"*, New Lines Institute, 2 VI 2020, https://newlinesinstitute.org/nonstate-actors/isis-in-africa-the-end-of-the-sahel-exception/ [accessed: 10 I 2025].

NATO, *Strategic foresight analysis. Regional perspectives report on North Africa and the Sahel*, https://www.act.nato.int/wp-content/uploads/2023/05/NU_SFA_Report_North_Africa_and_the_Sahel_SACT_approved_final_edited_version.pdf [accessed: 14 XII 2024].

Nsaibia H., *Actor Profile: Jama'at Nusrat al-Islam wal-Muslimin (JNIM)*, Armed Conflict Location & Event Data, 13 XI 2023, https://acleddata.com/2023/11/13/actor-profile-jamaat-nusrat-al-islam-wal-muslimin-jnim/ [accessed: 5 I 2025].

Nsaibia H., *Actor Profile: Volunteers for the Defense of the Homeland (VDP)*, Armed Conflict Location & Event Data, 26 III 2024, https://acleddata.com/2024/03/26/actor-profile-volunteers-for-the-defense-of-the-homeland-vdp/ [accessed: 5 I 2025].

Nsaibia H., Weiss C., *The End of the Sahelian Anomaly: How the Global Conflict between the Islamic State and al-Qa`ida Finally Came to West Africa*, "CTC Sentinel" 2020, vol. 13, no. 7, pp. 1–14, https://ctc.westpoint.edu/wp-content/uploads/2020/07/CTC-SENTINEL-072020.pdf [accessed: 5 I 2025].

Olech A., *Cooperation of the Maghreb countries with NATO for security in the region*, Instytut Nowej Europy, 12 X 2021, https://ine.org.pl/en/cooperation-of-the-maghreb-countries-with-nato-for-security-in-the-region/ [accessed: 19 XII 2024].

Olech A., *Francja i USA będą ponownie wojskowo współpracować w Afryce* (Eng. France and the US will again cooperate militarily in Africa), Defence24, 20 II 2024, https://defence24.pl/geopolityka/francja-i-usa-beda-ponownie-wojskowo-wspolpracowac-w-afryce [accessed: 11 XII 2024].

Olech A., *French Operation Barkhane in Africa – success or failure?*, Stosunki Międzynarodowe – International Relations, 18 XII 2023, https://internationalrelations-publishing.org/articles/3-17 [accessed: 3 XII 2024]. https://doi.org/10.12688/stomiedintrelat.17737.1.

Olech A., Wójcik P., *Wojna o Sahel [Raport]* (Eng. The war for the Sahel [Report]), Defence24, 17 XI 2024, https://defence24.pl/geopolityka/wojna-o-sahel-raport [accessed: 15 XII 2024].

Olech A., Wójtowicz B., *Rywalizacja o surowce w Sahelu – region konfliktu mocarstw* (Eng. Competition for resources in the Sahel – a region of conflict between powers), Trimarium.pl, 18 XI 2022, https://trimarium.pl/projekt/rywalizacja-o-surowce-w-sahelu-region-konfliktu-mocarstw/ [accessed: 7 XII 2024].

Pertier E., *After Military Took Power, Terrorist Attacks Only Got Worse*, The New York Times, 22 XII 2024, https://www.nytimes.com/2024/12/22/world/africa/niger-war-coup.html [accessed: 5 I 2025].

Phillips M.M., Faucon B., *U.S. Forces Try to Regroup as al Qaeda, Islamic State Sow Terror in West Africa*, The Wall Street Journal, 11 IX 2024, https://www.wsj.com/world/africa/u-s-moves-aircraft-commandos-into-west-africa-in-fight-against-islamist-militants-0b15c41b [accessed: 11 XII 2024].

Polyakova A., Lucas E., Boulègue M., Sendak C., Kindsvater S., Kuz I., Stone S., *A New Vision for the Transatlantic Alliance: The Future of European Security, the United States, and the World Order after Russia's War in Ukrain*e, Center for European Policy Analysis, 30 XI 2023, https://cepa.org/comprehensive-reports/a-new-vision-for-the--transatlantic-alliance-the-future-of-european-security-the-united-states-and-the--world-order-after-russias-war-in-ukraine/ [accessed: 23 XII 2024].

Portillo L.V. del, *Challenges in the Sahel: Opportunities for Europe*, Eurodefense Network, 21 II 2021, https://eurodefense.eu/2021/02/21/challenges-in-the-sahel-opportunities-for-europe/ [accessed: 18 XII 2024].

Raineri L., Strazzari F., *Jihadism in Mali and the Sahel: evolving dynamics and patterns*, European Union Institute for Security Studies, 29 VI 2017, https://www.iss.europa.eu/publications/briefs/jihadism-mali-and-sahel-evolving-dynamics-and--patterns [accessed: 16 XII 2024].

Renoult J., *L'Italie, dernier partenaire occidental du Niger*, Le Monde, 23 VII 2024, https://www.lemonde.fr/afrique/article/2024/07/23/l-italie-ultime-partenaire-occidental-du-niger_6256111_3212.html [accessed: 6 XII 2024].

Roger B., Eydoux T., *Drones turcs, avions russes… au Sahel, la guerre des airs est déclarée*, Le Monde, 20 XI 2024, lemonde.fr/afrique/article/2024/11/20/drones-turcs-avions-russes-au-sahel-la-guerre-des-airs-est-declaree_6405083_3212.html [accessed: 7 XII 2024].

Sahel, Britannica, https://www.britannica.com/place/Sahel [accessed: 14 XII 2024].

Sahel Showdown: How Türkiye Can Help NATO With Russian and Chinese Advances, TRT World Research Centre, 29 VII 2024, https://researchcentre.trtworld.com/featured/perspectives/sahel-showdown-how-turkiye-can-help-nato-with-russian-and-chinese-advances/ [accessed: 10 XII 2024].

Sanjuan L., *Los soldados más temidos del mundo: hay una unidad española*, AS, 24 X 2024, https://as.com/actualidad/politica/los-soldados-mas-temidos-del-mundo-n [accessed: 4 XII 2024].

Tesfaye B., *Climate Change and Conflict in the Sahel*, Council on Foreign Relations, November 2022, https://www.cfr.org/report/climate-change-and-conflict-sahel [accessed: 27 V 2025].

The Federal Government realigns its Sahel policy, Federal Foreign Office, 3 V 2023, https://www.auswaertiges-amt.de/en/newsroom/news/2595298-2595298 [accessed: 4 XII 2024].

Toutate I., *BCIJ Links 'Highly Dangerous' Foiled Terror Plot to Sahel Terrorist Groups*, Morocco World News, 24 II 2025, https://www.moroccoworldnews.com/2025/02/174948/bcij-links-highly-dangerous-foiled-terror-plot-to-sahel-terrorist-groups/ [accessed: 20 V 2025].

Tuareg rebels driven out of Timbuktu, Al Jazeera, 29 VI 2012, https://www.aljazeera.com/news/2012/6/29/tuareg-rebels-driven-out-of-timbuktu [accessed: 5 I 2025].

US military says withdrawal from Niger is complete, France24, 16 IX 2024, https://www.france24.com/en/live-news/20240916-us-military-says-withdrawal-from-niger-is-complete [accessed: 5 I 2025].

US troops pull out of Niger's Air Base 101, Reuters, 8 VII 2024, https://www.reuters.com/world/africa/us-troops-pull-out-nigers-air-base-101-2024-07-07/ [accessed: 5 I 2025].

Vilnius Summit Communiqué, NATO, 11 VII 2023, https://www.nato.int/cps/en/natohq/official_texts_217320.htm [accessed: 23 XII 2024].

Weiss C., *AQIM's Imperial Playbook. Understanding al-Qa'ida in the Islamic Maghreb's Expansion into West Africa*, n.p., April 2022, https://ctc.westpoint.edu/wp-content/uploads/2022/04/AQIMs-Imperial-Playbook.pdf [accessed: 5 I 2025].

Weiss C., *Tuareg rebels, JNIM each claim victory over Russia's Wagner Group in Mali*, Foundation for Defense of Democracies, 29 VII 2024, https://www.fdd.org/analysis/op_eds/2024/07/29/tuareg-rebels-jnim-each-claim-victory-over-russias-wagner-group-in-mali/ [accessed: 5 I 2025].

Wójcik J., *Sahel pogrąża się w terrorystycznej rebelii* (Eng. The Sahel plunges in a terrorist rebellion), Defence24, 30 IX 2023, https://defence24.pl/geopolityka/sahel-pograza-sie-w-terrorystycznej-rebelii [accessed: 12 XII 2024].

Wójcik P., entry on the portal X, 19 I 2025, https://x.com/SaladinAlDronni/status/1881013944443363547 [accessed: 24 I 2025].

Zelin A.Y., *The Islamic State on the March in Africa*, The Washington Institute for Near East Policy, 1 III 2024, https://www.washingtoninstitute.org/policy-analysis/islamic-state-march-africa [accessed: 5 I 2025].

Zelin A.Y., Cahn S., *Exploiting a "Vast jihad Arena": The Islamic State Takes Territory in Mali*, The Washington Institute for Near East Policy, 26 IX 2023, https://www.washingtoninstitute.org/policy-analysis/exploiting-vast-jihad-arena-islamic-state-takes-territory-mali [accessed: 5 I 2025].

Zenn J., *Brief: JNIM Attacks in Benin Represented Group's Growing Operational Strength in Periphery*, The Jamestown Foundation, 11 XII 2024, https://jamestown.org/program/brief-jnim-attacks-in-benin-represented-groups-growing-operational-strength-in-periphery/ [accessed: 5 I 2025].

Aleksander Olech, PhD

Head of International Cooperation at Defence24 and Editor-in-Chief of Defence24.com. Lecturer at both national and international universities, NATO associate, analyst, and publicist. Former deputy director of the Department of Africa and the Middle East at the Ministry of Foreign Affairs. Graduate of the European Academy of Diplomacy and War Studies University. Main research interests: French-Russian relations, challenges in Africa and NATO security policy.

Contact: a.olech@defence24.pl

Paweł Wójcik

Researcher on Islamic terrorism. Expert at Opportunity Institute for Foreign Affairs. He specialises in the Islamic State and Al-Qaeda and the risk assessment of these organisations. His research interests also include politics in Syria, the Durand Line and the Sahel region.

Contact: chrzestogniapl@gmail.com

Terrorism – Studies, Analyses, Prevention, 2025, no. 7: 425–460

https://doi.org/10.4467/27204383TER.25.038.21815

Article

Biosecurity of dual-use items

ANNA BIELECKA-ODER
Polish Association for National Security
https://orcid.org/0009-0002-6952-0023

Abstract

Most of biological warfare agents are simultaneously serious biological threats for public health. The way in which these factors are used is mainly determined by the anthropogenic factor. Accelerated progress in life sciences and biological engineering stopped the COVID-19 pandemic (mRNA vaccine), on the other hand, opened the way for advanced research using biological agents for unethical purposes. The paper provides an introduction to biological security issues. It presents the concept of biological security in a cross-cutting manner, in terms of international disarmament, non-proliferation agreements on biological and toxin weapons as well as the regulations referring to them. The author reviews and analyses measures to secure and protect biological agents and related technologies, with reference to activities particularly vulnerable to abuse in the area of such protection. Effective countering of biological threats requires an interdisciplinary approach to biosecurity. At stake is the prevention of the use of biological materials with dual-use potential as a weapon or terrorist agent.

Keywords

biosecurity, multilateral treaties, dual-use items

Biological hazard

It is generally accepted that biohazards are mainly caused by biological agents – bacteria, viruses, biological toxins[1]. Sources of danger can be, for example, the *Bordetella pertusis* bacterium, which causes whooping cough, a highly contagious disease that poses a public health threat, and the *Bacillus anthracis* bacterium, the cause of anthrax. Due to a number of factors (including environmental, biological, epidemiological, health, medical, social, community, behavioural, ethnographic, geopolitical) and their variables, anthrax can pose a threat at different levels. It can pose an epidemic or public health threat if it applies to human cases, and an endemic threat if it applies to a specific population or is common in a geographical region. In addition, anthrax may pose an epizootic threat if it affects animal infections, as well as a terrorist threat in the case of deliberately causing human and/or animal infections. Because of the possibility of different forms of anthrax among humans (pulmonary, cutaneous, gastrointestinal), requiring slightly different types of treatment and post-exposure measures, assessing the risk of contracting the disease is complex and beyond the jurisdiction of a single scientific discipline.

A consequence of the existence of a biohazard may be that the technology used for the selection, proliferation or modification of micro-organisms, apparatus for biological synthesis or biotransformation used in the production, isolation and purification of products of organic origin (proteins, including toxins) may be misused. For example, a bioreactor (fermentor) used for the production of bacteria under large-scale continuous culture conditions can be used in two ways depending on its intended use, i.e. as equipment prohibited by international law if used for the production of biological agents for warfare purposes, and as equipment permitted for use and dissemination if used for the production of biological agents for peaceful purposes, e.g. health care (production of vaccines, antibiotics, antiviral drugs, therapeutic proteins) or environmental protection (production of plant protection products). In both of these cases, the same technology and instrumentation is used during manufacture. Therefore, during the initial inspection of a site, it is often difficult to resolve whether an activity involving the production

[1] The article builds on issues analysed in the author's doctoral dissertation. The article has updated the text in relation to the dissertation. Moreover, it has been expanded to include threads on events that occurred after September 2018.

of microorganisms or biological toxins is being carried out for peaceful, hostile or both purposes. Because of the dualistic nature of technology using living biological systems in industrial production, it is referred to as dual-use technology. A slight modification of it can make it serve offensive instead of defensive purposes[2].

Ensuring effective biosecurity is a major challenge. This is due to the multitude of factors that influence it. These include, among others: the profile of human activity and its objectives, the diversity of biological agents, the possibility of modifying them at different stages of gene expression, the multiplicity of biotechnological processes and methods, the variability of environmental conditions affecting the distribution and availability not only of the agents themselves, but also of vectors (carriers) of infectious diseases, the different ways in which they are released, the specificity of individual conditions at the cellular level, which have a direct impact on susceptibility to disease.

International agreements on biosecurity

The broad spectrum of human activities and the biological threats that result from them means that, despite the common goal of effective biosecurity, the means to achieve it may be different. Stakeholders from a wide range of backgrounds debated approaches to such protection, including specialists in international law dealing with bioweapons and toxin prohibition, environmental and biodiversity protection, public health and epidemiology, animal health protection, phytosanitary protection, occupational safety and health protection in laboratory, health crisis response, as well as representatives from a wide range of academia. Each of these communities identified as leading those demands that coincided with its subjective objectives. These objectives included, among others: disarmament and non-proliferation of weapons of mass destruction (hereinafter: WMD), countering bioterrorism, protecting human health and emergency response to epidemics, protecting biodiversity, protecting

[2] With malicious intent, a biohazard can be created through equipment that is also used by other industries, such as fuel production equipment or installations designed to ferment food beverages. In addition, such apparatus can be cleaned or dismantled within hours, making it possible for criminals to quickly hide signs of their activities.

the health of animals and crops, occupational safety and health protection against harmful biological agents, raising awareness of biological risks.

The concept of biosecurity originates from international agreements on disarmament and non-proliferation of biological and toxin weapons. The first agreement banning the use of biological warfare agents was the *Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare*, commonly referred to as the Geneva Protocol[3]. Poland was also involved in the work on this document. This was a huge step forward in sanctioning the ban, even though the protocol covered only the use of these agents in times of war. Nevertheless, if the biological weapons research, production and stockpiling were not oficially banned, they were allowed in silent consent. In addition, some signatories (France, the United States, the United Kingdom) reserved the right to use them in retaliation if the adversary used the agent first, which was an additional limitation of the ban. Despite this, the Geneva Protocol never lost its relevance, as evidenced by the reference to it in the preambles of two later agreements: the 1972 *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction*, commonly referred to as the Biological and Toxin Weapons Convention (hereinafter: BTWC)[4], and the 1993 *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction*, commonly referred to as the Chemical Weapons Convention (hereinafter: CWC)[5].

The BTWC is a key agreement concerning biosafety and biosecurity issues. This topic was also addressed in United Nations Security Council Resolution 1540 of 2004[6] on the global ban on all four types of WMD. International control regimes over biological and toxin weapons introduced by members of The Australia Group (AG)[7], including Poland, serve to

[3] *Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare*, 1925.

[4] *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, 1972.*

[5] *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction*, 1993.

[6] *Resolution 1540 (2004) / adopted by the Security Council at its 4956th meeting, on 28 April 2004*, 2004.

[7] *Fighting the spread of chemical and biological weapons*, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/index.html [accessed: 22 II 2025].

control the transfer and export of biological agents, toxins and dual-use technologies.

The topic of biological security is also addressed in other international agreements to which Poland is a state party. These include the Convention on Biological Diversity[8] and its two Protocols – on the supervision of living genetically modified organisms[9] and on the protection of biological diversity and the Earth's natural ecosystems[10], the International Health Regulations[11] established by the World Health Organization (WHO), and agreements on the transport of dangerous goods[12]. Handbooks and recommendations on biosafety and biosecurity in the laboratories, repositories, transport, research and development or in the event of the intentional use of chemical, biological, radiological and nuclear (CBRN) agents are also a valuable source of knowledge on biosecurity.

Biological and Toxin Weapons Convention (1972)

The text of the BTWC comprises 15 articles. It is the first multilateral legally binding agreement and currently the most important treaty in the field of non-proliferation of biological and toxin weapons in the world. It forms the basis for subsequent biosafety and biosecurity considerations and therefore requires more attention.

Representatives of the States Parties, including Poland, have been meeting every 5 years or so since 1980 and hold review conferences. The purpose of these deliberations is to review the operation of the BTWC to date and to develop a final document. It presents newly adopted arrangements to better interpret and understand the objectives of the Convention in the context of currently applicable normative documents, advances in knowledge and technology as well as activities undertaken in international fora in this area.

[8] *The Convention on Biological Diversity*, 1993.

[9] *The Cartagena Protocol on Biosafety to the Convention on Biological Diversity*, 2003.

[10] *The Nagoya Protocol on Access to Genetic Resources and the Fair and Equitable Sharing of Benefits Arising from their Utilization to the Convention on Biological Diversity*, 2014.

[11] *The International Health Regulations*, World Health Organization 2005.

[12] *European Agreement Concerning the International Carriage of Dangerous Goods by Road* (ADR); *The Regulation concerning the International Carriage of Dangerous Goods by Rail* (RID); *The European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways* (ADN); *The IATA Dangerous Goods Regulations* (IATA DGR).

In addition, the States Parties to the BTWC are required to submit so-called confidence-building measures (CBMs) in the form of reports each year. Their purpose is to eliminate possible doubts or suspicions about activities carried out for peaceful purposes in the field of biological sciences and to promote transparency and information sharing. The report includes below data:

1) information on research centres, laboratories and national biological defence research and development programmes;
2) information on outbreaks of infectious diseases and similar occurrences caused by biological toxins in the last year;
3) last year publication of results and promotion of use of knowledge in the coming year;
4) list of national legislation, regulations and other measures that have been established with reference to the BTWC;
5) information on past activities in offensive and/or defensive biological research and development programmes conducted after 1 January 1946;
6) data on national vaccine production facilities[13].

The BTWC was the first Convention to address the topic of biosafety and biosecurity, particularly in Articles I, III, IV, VII, IX and X. The review conferences over the past 44 years have successively detailed the provisions in this regard.

Article I

The BTWC does not specify biological agents and toxins that can be used as weapons, which is an advantage and disadvantage at the same time. This allows it to cover a wide range of biological agents that pose a risk to humans, animals and plants and that are acquired in different ways. For example, the final documents of the review conferences assume that Article I applies to all harmful microorganisms or other microbial agents or toxins occurring naturally and artificially produced or modified[14]. It also covers particles and cellular elements of agents and toxins, including synthetic equivalents obtained chemically or structural analogues of naturally occurring compounds, regardless of their source or method of production,

[13] *Confidence Building Measures,* United Nations, Office for Disarmament Affairs, https://disarmament.unoda.org/biological-weapons/confidence-building-measures/ [accessed: 13 X 2024].

[14] *Final Document of the Sixth Review Conference,* Geneva 2006. BWC/CONF.VI.I.1.

type and amount, the production of which has no prophylactic, protective or peaceful justification[15], as well as toxins of bacterial, animal and plant origin, including their synthetically produced analogues[16].

With regard to equipment and technology, the situation is identical. The Convention does not introduce equipment names or technical specifications, which makes it possible to prohibit all equipment and technology that could be potentially used for proliferation of biological warfare agents or their release[17].

Article III

It applies directly to biosecurity issues, as it obliges to refrain from transferring biological agents or their means of transfer for hostile purposes, assisting in and affecting their development work. The review conferences detailed this provision and obliged States Parties to ensure protection during transfer for all Article I agents. It was postulated that this should be done, inter alia, through national implementation of the BTWC, legal norms for the transfer of biological agents and the facilities that may be used for their production, the obligation to supervise and control these transfers. In 1996, ways to prevent the acquisition of these agents by a broad group of potential recipients (an individual, a state, a group of states or an international organisation) and their transfer within the national territory were discussed[18]. Unfortunately, this has proved problematic, since under the same convention, States Parties are obliged to allow the widest possible exchange of equipment, materials as well as scientific and technical knowledge for the peaceful use of biological agents, toxins and technology (Article X). For this reason, there have been repeated calls for the creation of instruments to establish a control regime over all biological agents, biological toxins, dual-use devices and their components for which there is a risk that they could be used for offensive biological and toxin weapons development programmes[19].

[15] *Final Document of the Third Review Conference*, Geneva 1991. BWC/CONF.III.I.3; *Final Document of the Fourth Review Conference*, Geneva 1996. BWC/CONF. IV.I.5.

[16] *Final Document of the Second Review Conference*, Geneva 1986. BWC/CONF.II.I.5.

[17] *Final Document of the Seventh Review Conference,* Geneva 2011. BWC.CONF.VII.I.1; *Final Document of the Eighth Review Conference*, Geneva 2016. BWC/CONF.VIII.I.1; *Final Document of the Ninth Review Conference*, Geneva 2022. BWC/CONF.IX/CRP.2/Rev.1.II.I.

[18] *Final Document of the Fourth Review Conference*... BWC/CONF.IV.III.3.

[19] *Final Document of the Third Review Conference*... BWC/CONF.III.III.1; *Final Document of the Fourth Review Conference*... BWC/CONF.IV.III.2; *Final Document of the Sixth Review*

It was proposed that export controls should issue licences or permits, which would be granted once there was assurance that the goods in question would reach a pre-approved consignee and be used for purposes consistent with the agreement[20]. It was recommended that States Parties create a system of safeguards and protection for each of the measures applying to the article[21], which was problematic given the absence for a long time of an arbitrary list of these measures.

After the terrorist attacks in 2001, the need to regulate the protection of agents included in the Article I of the BTWC has increased. It was concluded that the threat posed by biological terrorism should imply the need for more effective measures to control the carriage and transfer of these agents. This was particularly true for countries not party to the BTWC, regardless of whether the transfer would be to an individual or to members of groups representing the views of specific nationalities or other groups. This generated considerable debate, as it was feared that the proposed measures could harm traditional trade and impede cooperation between States Parties for peaceful purposes[22].

Polarisation of positions on this issue is still evident. A large divergence is observed between highly developed countries with adequate capacities, scientific and technical backgrounds, making extensive use of biological agents in the (commercial) health sphere, and countries without sufficient specialist knowledge and biological capacity. They call for unfettered access to biological materials and technology as well as the provision of far-reaching assistance rather than the prior introduction of control and surveillance mechanisms for biological agents[23].

Article IV

It obliges States Parties to take all measures to prevent the production of biological and toxin weapons, but does not specify these measures explicitly, thus allowing the possibility of introducing arbitrary tools

Conference... BWC/CONF.VI.III.8-9; *Final Document of the Seventh Review Conference*... BWC/CONF.VII.III.9; *Final Document of the Eighth Review Conference*... BWC/CONF/VIII.III.9.

[20] *Final Document of the Sixth Review Conference*... BWC/CONF.VI.III.8.

[21] Ibid. BWC/CONF.VI.III.9.

[22] *Final Document of the Fifth Review Conference*, Geneva 2001–2002. BWC/CONF.V.COW/CRP.1.III – *Annex to the draft report of the Committee of the Whole*.

[23] *Biological Weapons Convention – Ninth Review Conference*, United Nations, Office for Disarmament Affairs, https://meetings.unoda.org/bwc-revcon/biological-weapons-convention-ninth-review-conference-2022 [accessed: 8 III 2025].

and measures. The final documents of the review conferences assumed that undertakings should derive from the legal instruments in force in the country, both from the penal provisions for the implementation on the territory of the country of the prohibition of the development, production, storage, acquisition and maintenance of biological agents and equipment listed in Article I, and from the provisions related to the prevention of such activities by exercising control over them[24].

In order to effectively fulfil Article IV obligations, the security of biological agents was repeatedly addressed at review conferences. For example, the implementation of international standards for biosafety management and biosecurity[25], the implementation of regulations for the physical protection of property and the safeguarding of facilities where particularly dangerous biological agents and toxins are used were considered particularly important. It was emphasised that the establishment of regulations in this area would significantly affect not only public health security in the event of epidemic threats, but also the safeguarding of infectious agents and toxins against their release or hostile takeover[26]. In enhancing the effectiveness of this article, the need to secure biological agents and biotoxins was pointed out, not only in laboratories or storage areas, but also during transport[27]. When in 2005 WHO published the International Health Regulations addressing the issue of building national preparedness for detecting, identifying and responding to cross-border health threats, the close correlation of this legal instrument with Article IV of the BTWC was recognised. The States Parties to the BTWC, which are to a large extent also WHO Member States, began to advocate for national measures towards improving diagnostic methods, strengthening epidemiological surveillance and the capacity to detect infectious disease

[24] *Final Document of the Second Review Conference*... BWC/CONF.II.IV.4; *Final Document of the Third Review Conference*... BWC/CONF.III.IV.3; *Final Document of the Fourth Review Conference*... BWC/CONF. IV.IV.1-4; *Final Document of the Sixth Review Conference*... BWC/CONF.VI.IV.11.i; *Final Document of the Seventh Review Conference*... BWC/CONF.VII.IV.11.i; *Final Document of the Eighth Review Conference*... BWC/CONF.VIII.IV.11.a-b.

[25] *Final Document of the Seventh Review Conference*... BWC/CONF.VII.IV.13a.

[26] *Final Document of the Second Review Conference*... BWC/CONF.II.IV.4ii; *Final Document of the Third Review Conference*... BWC/CONF.III.IV.3ii; *Final Document of the Fourth Review Conference*... BWC/CONF. IV.IV.3; *Final Document of the Sixth Review Conference*... BWC/CONF.VI.IV.11.iii; *Final Document of the Seventh Review Conference*... BWC/CONF.VII.IV.11.iii; *Final Document of the Eighth Review Conference*... BWC/CONF.VIII.IV.11.b-c.

[27] *Final Document of the Seventh Review Conference*... BWC/CONF.VII.IV.11.

outbreaks at the national, regional and international levels in order to simultaneously implement both agreements. In doing so, it was recognised that by continuously monitoring epidemiological trends through national disease surveillance system, the detection of atypical outbreaks or other biological threats would be much more efficient and faster. Especially the outbreaks, which could be a potentially result of works conducted in contrary to the BTWC[28].

Article IV also called for the implementation of legal instruments for the control and rationing of persons handling pathogens, the dissemination of knowledge among them and the promotion of ethical attitudes. It was considered that education and awareness-raising on the possibility of using particularly dangerous biological agents, biological toxins and devices as well as means of their transmission with the intention of contravening the provisions of the BTWC could enhance the effectiveness of Article IV activities. It was suggested that content about the BTWC and the Geneva Protocol should be included in training programmes and educational materials for medical, life sciences and military students[29]. In 2022, it was requested that the audience be expanded to include those in the public and private sectors as well as academia, and to become more actively involved in early identification of risks of non-compliance with the BTWC, including acts of bioterrorism. Particular scrutiny should be given to persons who have gained access to harmful biological agents and toxins applicable to the BTWC and to professionals who, through their knowledge and skills, are able to modify biological agents and increase the virulence of pathogens or exacerbate the course of diseases caused by them. This was considered as one of the possible measures to prevent the production of biological and toxin weapons[30].

[28] *Final Document of the Sixth Review Conference*... BWC/CONF.VI.IV.13; *Final Document of the Seventh Review Conference*... BWC/CONF.VII.IV.13vi; *Final Document of the Eighth Review Conference*... BWC/CONF.VIII.IV.13f.

[29] *Final Document of the Second Review Conference*... BWC/CONF.II.IV.4iii; *Final Document of the Third Review Conference*... BWC/CONF.III.IV.3iii; *Final Document of the Fourth Review Conference*... BWC/CONF.IV.IV.3iii.

[30] *Final Document of the Seventh Review Conference*... BWC/CONF.VII.IV.13ii-iv; *Final Document of the Eighth Review Conference*... BWC/CONF.VIII.IV.13b-d; *Final Document of the Ninth Review Conference*... BWC/CONF.IX/CRP.2/Rev.1.II.IV.

Article VII

It obliges treaty States Parties, international, governmental and non-governmental organisations to provide support to countries against which the UN Security Council has confirmed violations of the BTWC. The article compels mutual assistance in investigations in the event of the commission or suspected commission of an act prohibited by the convention. In order to effectively fulfil the provisions of this article, the review conferences recommended that the UN should play a coordinating role in the investigation, with the support of relevant international organisations, including the WHO, which is the international organisation with jurisdiction over global human health issues, including epidemiological investigations. It was felt that the involvement of epidemiologists, alongside other organisations, including those competent to investigate the commission and/or suspicion of an act prohibited by the Convention, would improve the detection and identification of the source of disease, describe the routes of transmission of the infectious agent and indicate the appropriate course of action if the agent were to be used as a weapon or a terrorist agent[31]. In 2006, the list of these organisations was expanded, as it was accepted that mutual assistance would strengthen global security and minimise the impact of similar incidents[32].

In addition, there was a call, similar to Article IV, for national efforts to strengthen surveillance of infectious diseases and the capacity to detect and identify biological agents that could be the source of infectious disease outbreaks[33].

Article IX

It commits to the establishment of a ban on chemical weapons and agents that may contribute to their production and proliferation, which on the face of it, correlates poorly with biosecurity issues. However, it should be remembered that during the deliberations on the BTWC, the issue of chemical warfare agents was repeatedly addressed and the need for

[31] *Final Document of the Third Review Conference*... BWC/CONF.III.VII.4; *Final Document of the Fourth Review Conference*... BWC/CONF. IV.VII.5.

[32] *Final Document of the Sixth Review Conference*... BWC/CONF.VI.VII.34; *Final Document of the Seventh Review Conference*... BWC/CONF.VII.VII.36.

[33] *Final Document of the Sixth Review Conference*... BWC/CONF. VI.VII.35; *Final Document of the Seventh Review Conference*... BWC/CONF. VII.VII.38; *Final document of the Eighth Review Conference*... BWC/CONF.VIII.VII; *Final Document of the Ninth Review Conference*... BWC/CONF.IX/CRP.2/Rev.1.II.VII.

a Chemical Weapons Convention was raised. This resulted in the emergence immediately after its promulgation of 181 instruments of ratification and applications for accession[34].

It was in the context of Article IX of the BTWC that the issue of the increasing convergence of biology and chemistry and the challenges of their security began to be recognised. The 2011 review conference recognised that the risks at the interface between biology and chemistry, and the convergence of biological and chemical technologies applicable to biosafety and the protection of humans and the environment, should suggest a concerted effort to prevent biological and chemical risks in relation to both treaties, i.e. the BTWC and the CWC[35].

This is important insofar as the differences between chemically synthesised pathogens and chemical compounds produced using living organisms are very often blurred. Using chemical systems, a dangerous pathogen can be developed, and using bacterial cultures, the biological toxins, including their synthetically produced analogues, can be made[36].

Article X

It is primarily concerned on the broad cooperation of States Parties in scientific research, bioengineering work, specific knowledge and technology transfer. It commits to the development and use of bioscience and technology for the benefit of mankind and the environment. This obligation should be implemented by allowing the exchange of equipment, materials, scientific and technical information on the use of bacteriological (biological) agents and toxins to the fullest extent possible, provided they are for peaceful purposes. This article obliges cooperation in contributing to the further development and use of scientific discoveries in the field of bacteriology for disease prevention or other peaceful purposes.

It was requested that States Parties to the BTWC, especially developed countries, expand scientific and technological cooperation with developing countries. The cooperation would include, inter alia: transfer of knowledge, experience and technological solutions for peaceful uses of biological agents and toxins, transfer and exchange of information, training

[34] *Final Document of the Fourth Review Conference*... BWC/CONF. IV.IX.45; *Final Document of the Seventh Review Conference*... BWC/CONF. VII.IX.48.

[35] *Final Document of the Seventh Review Conference*... BWC/CONF. VII.IX.49.

[36] *Final Document of the Second Review Conference*... BWC/CONF.II.I.5.

of scientists and experts, as well as transfer of materials and resources[37]. Access to expertise would include bacteriology, biotechnology, genetic engineering, microbiology and related scientific and technical fields[38].

During the 2016 review conference, the issue of cooperation, viewed differently by Western and developing countries, was particularly debatable, in addition to the introduction of a legally binding verification mechanism. The need to strengthen it within the framework of Article X was particularly highlighted by developing countries (e.g. Iran, Venezuela, Cuba) grouped in the Non-Aligned Movement (NAM) and other States. They demanded wider access to modern biotechnology developments and equipment, know-how, training and scientific and academic exchange, which was not welcomed by other states (e.g. USA, UK, Sweden and Germany)[39]. It was only during the agreement of the final document of the last review conference in 2022 that it was decided to establish an expert working group. Its purpose will be, among other things, to develop a mechanism for reviewing and assessing scientific and technological developments relevant to the BTWC[40].

The concept of biosecurity

The terms *biosafety* and *biosecurity* have repeatedly been treated as either identical or synonymous definitions. The term *biosafety* appeared earlier than *biosecurity* and for a long time included biosecurity issues. As a result, in some countries (e.g. France, Germany, Russia and China), the term biosecurity did not function at all, which often caused practical problems.

In order to better understand the differences between these terms, the 2003 BTWC participants proposed their informal interpretation. They assumed that biosafety is the protection of humans from micro-organisms, while biosecurity focuses on the protection and containment of micro-organisms from hostile human activities. Five years later, it was clarified that biosafety should focus on measures to create safe working conditions with harmful biological agents and to protect people and

[37] Ibid. BWC/CONF.II.X.3ii-iv; *Final Document of the Third Review Conference*... BWC/CONF. III.X.3ii-iv; *Final Document of the Fourth Review Conference*... BWC/CONF.IV.X.12ii-iv, viii.; *Final Document of the Sixth Review Conference*... BWC/CONF. VI.X.49; *Final Document of the Seventh Review Conference*... BWC/CONF.VII.X.58.

[38] *Final Document of the Second Review Conference*... BWC/CONF.II.X.2.; *Final Document of the Third Review Conference*... BWC/CONF.III.X.2; *Final Document of the Fourth Review Conference*... BWC/CONF.IV.X.2.

[39] *Final Document of the Eighth Review Conference*... BWC/CONF.VIII/4.X.59.

[40] *Final Document of the Ninth Review Conference*... BWC/CONF.IX/CRP.2/Rev.1. X.71.

the environment from accidental releases. Biosecurity, in turn, should be understood as the various means and ways of protecting biological agents and dual-use technologies from theft or unauthorised acquisition or acquisition and their use to cause harm. It comprises: physical protection of premises and facilities where particularly dangerous pathogens and toxins are stored, control of the transfer of dual-use products and technologies, proper packaging, labelling and secure during the transport of consignments containing infectious material, secure of knowledge, technology and the results of scientific and research work that could be a potential source of information on how to produce biological and toxin weapons, counteracting biological terrorism. Biosecurity also addresses issues of enforcing compliance with international agreements, countering agroterrorism (protecting the environment from the deliberate release of alien or invasive species to cause damage to agricultural crops), conducting investigations using biological traces as evidence and investigative efforts to apprehend perpetrators of bioterrorist acts[41].

The UN Security Council Resolution 1540 (2004)

The UN Security Council Resolution 1540 (hereinafter: Resolution 1540)[42] is the first international legally binding instrument comprehensively addressing all three types of WMD. The implementation of this resolution implies the need for national implementation of the provisions of the three agreements: the BTWC, the CWC and the Nuclear Non-Proliferation Treaty (NPT)[43].

The intent of Resolution 1540 directly supports the implementation of the obligations under the BTWC, as it details and specifies biosecurity measures to counter the illicit possession, manufacture, storage, transport, transit and trade in biological and toxin weapons materials and technologies. Measures are implemented in four areas:

1) adoption and enforcement of criminal law regarding non-compliance with the ban on the production of biological and toxin weapons and their means of proliferation,

[41] *Biosafety and Biosecurity – Submitted by the Implementation Support Unit,* 24 June 2008, BWC/MSP/2008/MX/INF.1; A. Bielecka-Oder, *Safety and Security Regulations Against Biological Threats,* in: *Defence Against Bioterrorism,* V. Radosavljevic, I. Banjari, G. Belojevic (eds.), Springer Netherlands 2018.

[42] *Resolution 1540 (2004)*...

[43] *The Nuclear Non-Proliferation Treaty* (NPT), 1968.

2) adoption of measures to reduce or eradicate illicit trafficking in WMD and materials used for their production,
3) not to hamper trade and the provision of commercial health services conducted in accordance with the applicable legislation,
4) to encourage dialogue and exchange of experiences between countries on security measures in place and on the protection of territorial borders and export controls.

In order to verify the effectiveness of national implementation of these assumptions, the 1540 Committee has developed the 1540 Matrices to describe the degree of implementation[44]. In the section on biological and toxin weapons and related materials, each country is obliged to:

- provide information on membership of international and regional agreements,
- provide information on national legally binding and non-binding instruments prohibiting the provision of services, assistance and funding activities listed in the matrix, including but not limited to production, extraction, storage, development, transport, transfer of ownership to other economic operators and/or individuals,
- provide information on the type of measures applied to national mechanisms for the control of compliance with biosafety and biosecurity regarding the production, use, storage, transport and other methods of obtaining biological agents, toxins and their means of dissemination, and the licensing of facilities involved in the abovementioned activities, the registration of persons handling the abovementioned materials, the verification of their trustworthiness, the use of physical protection, compliance with regulations on genetic engineering work and other regulations on biosafety and security,
- include national regulations, procedures, measures, including listing institutions responsible for, inter alia, exercising trade controls, negotiating the sale of goods and technology as well as brokering, conducting investigative and/or intelligence activities, verifying credentials and licences, conducting export controls based on control lists of biological agents, toxins and dual-use technologies and controlling their sources of funding.

[44] *Approved 1540 Committee Matrix of [State]*, https://www.un.org/en/sc/1540/documents/Matrix%20Template%202013%20(E).pdf [accessed: 17 XI 2024].

The Resolution 1540 is one of the main pillars of the international non-proliferation and WMD trafficking control order, as reflected in the 2022 EU Counter-proliferation Strategy Progress Report. It indicates that EU countries consider it as (...) *a key part of the global efforts to prevent the proliferation of Weapons of Mass Destruction, including to terrorists and other non-state actors*[45].

Australia Group (1985)

Currently, there are several multilateral export control regimes for security-sensitive materials and agents in the world (e.g. the Wassenaar Arrangement, the Zangger Committee, the Australia Group, the Nuclear Suppliers Group, the Missile Technology Control Regime). The most important body in the area of export control of biological warfare agents and dual-use technologies, significantly contributing to countering the proliferation and spread of biological and toxin weapons agents, is the Australia Group[46]. Its activities directly support the implementation of the provisions of the BTWC by coordinating the export policies of strategic goods by its members and enhancing the effectiveness of national dual-use licensing measures. The AG members, including Poland, are simultaneously States Parties to the BTWC and CWC[47].

As part of its control regime over biological and toxin weapons, the AG has developed three control lists: a) a list of biological dual-use equipment, technology and software, b) a list of human and animal pathogens and toxins, c) a list of plant pathogens that are subject to specific export controls because of their potential for use in the production of biological and toxin weapons. These are important lists as they are the first to indicate the specific species names and technical specifications of equipment with dual-use potential that should be subject to specific controls. These

[45] *Sprawozdanie roczne z postępów w realizacji strategii Unii Europejskiej przeciw rozprzestrzenianiu broni masowego rażenia (2022)* (Eng. Annual Progress Report on the Implementation of the European Union Strategy against the Proliferation of Weapons of Mass Destruction (2022)), Prawo.pl, https://www.prawo.pl/akty/dz-u-ue-c-2023-383,72216862.html [accessed: 28 IX 2024].

[46] *Introduction*, The Australia Group, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/introduction.html [accessed: 21 IX 2024].

[47] *Participants*, The Australia Group, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/participants.html [accessed: 21 IX 2024].

lists should become a point of reference for national regulations[48]. When examining the individual items on these lists, it should be borne in mind that, for example, the control regime does not apply to biological agents that are components of protective vaccines (peaceful purpose). It would apply if these agents were exported in the form of pure live cultures or, in the case of toxins, pure isolates (dual use possibility).

Both the BTWC Convention and Resolution 1540 have not lived up to such specificity. This can be presumed to be a consequence of the universality of these agreements, which necessitated a certain level of generality and the need for consensus. This does not apply to the AG, which is an independent grouping and thus perhaps more effective in implementing its resolutions.

It is worth mentioning that the AG members frequently address the topics of potential threats as a consequence of changing geopolitical and international conditions. For example, the 2022 Plenary discussed the possibility of the use of chemical and biological weapons agents by the Russian Federation. The possibility of attacks on Ukrainian civilian facilities where biological and chemical agents are used or deposited was not ruled out. The global threat posed by disinformation on the subject was also discussed[49]. This theme was also taken up in 2023–2024. It was emphasised that, because of the threat of chemical and biological terrorism, particular vigilance must be exercised with regard to ongoing procurements that could support hostile activities, and there is a need to guard against the misuse of chemical and biological technologies and equipment by non-state actors. Attention was also drawn to the risks posed by the transfer of intellectual resources and expertise in areas of science that may be applicable to non-proliferation agreements, or the sharing of such resources and knowledge through mass media or other channels of exchange, and the need for effective controls over intangible transfers of technology (ITT)[50].

[48] *Australia Group Common Control Lists*, The Australia Group, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/controllists.html [accessed: 30 XI 2024].

[49] *Statement by the Chair of the 2022 Australia Group Plenary*, The Australia Group, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/2021-ag-plenary-statement.html [accessed: 22 IX 2024].

[50] *Statement by the Chair of the 2023 Australia Group Plenary*, Paris 2023; *Statement by the Chair of the 2024 Australia Group Plenary*, Paris 2024; K. Hyuk, *Intangible Transfer of Technology (ITT): Open-source Information Analysis for the Implementation of Sanctions on North Korea*,

The AG members attend meetings of BTWC States Parties and support the performance of its provisions. In 2024 it was indicated that they are looking forward to the development of two new mechanisms – concerning international cooperation and assistance and relating to scientific and technological development, as well as progress in the implementation of biosecurity measures[51].

Convention on Biological Diversity (1993)

The Convention on Biological Diversity (hereinafter: CBD Convention)[52] is the most important international agreement dedicated to the protection of environmental biodiversity from the risks posed by the use of modern biotechnologies. Its objectives, in addition to conservation, are the sustainable use of the elements of biodiversity, the fair and equitable sharing of the benefits arising from the use of genetic resources, the respect of rights over them and adequate funding[53]. Through the protocols arising from the implementation of its objectives, it indirectly addresses the issue of biosafety and security in the context of the BTWC.

Cartagena Protocol on Biosafety (2003)

It is a legally binding instrument that implements the first objective of the CBD Convention, namely the protection of biodiversity, including the protection of human, animal, plant and environmental health from the harmful effects of the products of modern biotechnology[54].

It is well known that, alongside the many benefits of the achievements of modern biotechnology, particularly molecular biology and genetic engineering techniques, there is a narrow margin of potentially hostile uses. Therefore, according to the BTWC, the production and use of bacteria, viruses and their toxins and the application of technology for purposes other than peaceful or protective are prohibited, and consequently the introduction into the environment and the spread of biological agents that could be used as weapons, cause human disease (bioterrorism), cause

38 North, 10 III 2023, https://www.38north.org/2023/03/intangible-transfer-of-technology-itt-open-source-information-analysis-for-the-implementation-of-sanctions-on-north-korea/ [accessed: 9 III 2025].

51 *Statement by the Chair of the 2024 Australia Group Plenary*..., para. 14.

52 *The Convention on Biological Diversity*, 1993.

53 Ibid., art. 1.

54 *Cartagena protocol on biosafety to the Convention on biological diversity*.

damage to the agricultural economy (agroterrorism) – whether through the deliberate contamination of food (food bioterrorism) or the deliberate destruction of environmental resources. Therefore, the deliberate modification of micro-organisms with dual-use potential for the purpose of releasing them into the environment or creating a threat to the health of humans, animals and wildlife is one of biosecurity aspects in the context of the BTWC.

The Cartagena Protocol was prompted by the need to establish rules for the safe use of living modified organisms (LMOs), including genetically modified microorganisms (GMMs), and to regulate international trade in them. The absence of these rules could have a negative impact on the conservation or sustainable use of environmental biodiversity and consequently pose a threat to public health[55]. The protocol also sets out the precautionary measures necessary to be taken in the event of a release of LMOs. Under this agreement, countries party to the protocol have the full right to restrict the import or use of these organisms, prohibit them if there is no scientific evidence or certainty about their safety[56].

Genetic modification of living infectious agents may create a weapon with new abilities, i.e. a known gene, but not present in the agent in question because it has been artificially incorporated into the genome, or an innovative payload, i.e. equipped with a newly created gene. Therefore, modifications such as transferring drug resistance genes to microorganisms previously lacking them in order to reduce the pathogen's sensitivity to the drug and deliberately altering the surface protein structures of pathogens responsible for antibody formation in the organism (defence), i.e. modifying the antigenic properties of pathogenic bacteria, are considered to require special attention. Work aimed at modifying the lipopolysaccharide structures of bacteria in such a way as to impede their early detection and recognition by the immune system and involving the addition of genes responsible for toxin production are also debatable. Potentially hazardous may be modifications of bacteria to increase their stability in the external environment, e.g. increasing their resistance to harmful atmospheric conditions (UV radiation) or mechanical stress (strength), resulting from their release into the environment and prolonged or vigorous mixing during bioreactor culture. The both transformation

[55] Ibid., art. 4.

[56] Ibid., art. 16–18.

of nonpathogenic micro-organisms into pathogenic by the deliberate transfer of genes responsible for pathogenic properties, as well as molecular changes programming micro-organisms to produce specific chemical compounds, including bioware toxins, which can be used as weapons, may be potentially dangerous[57].

Both the BTWC and the Cartagena Protocol regulate transfers. Article III of the Convention on transfer control of biological and toxin weapons agents and facilities, as well as Article X on the transfer of materials and technology and mutual cooperation for peace purposes. The Cartagena Protocol, on the other hand, on transboundary movements of LMOs as well as knowledge and technology transfer. Both agreements further emphasise the need to promote the exchange of information on experiments carried out and on national strategies implemented to counter the threats posed by biotechnology. In the case of the Protocol, this is the Biosafety Clearing-House[58], and in the case of the BTWC, it is the CBMs. However, it should be noted that the objectives of the two documents are different[59].

Despite the distant regulatory areas, the scopes of content of the two agreements – the BTWC and the Cartagena Protocol – converge in terms of assessing the effects of genetic modification. All biological agents subjected to modifications that alter their genotype qualify as agents covered by the prohibition expressed in the BTWC, as long as the purpose of the modifications is hostile use of the agents, since the prohibition covers all biological agents, including those produced by methods of modern biotechnology.

Nagoya Protocol on Access to Genetic Resources (2014)

The object of the regulation is to protect genetic resources from their illegal acquisition and use, which is referred to as biopiracy[60]. It mainly concerns the unlawful extraction and use of wild plants, exotic animals, endemic micro-organisms, their gene pools and the traditional knowledge

[57] K. Nixdorff, D. Schilling, M. Hotz, *Critical Aspects of Biotechnology in Relation to Proliferation*, in: *The Implementation of Legally Binding Measures to Strengthen the Biological and Toxin Weapons Convention*, M. Chevrier et al. (eds.), NATO Science Series II, vol. 150, 2004.

[58] *The Convention on Biological Diversity…*, art. 20.

[59] Ibid., art. 22.

[60] *Collins English Dictionary – Complete and Unabridged*, 12th edition, Collins 2014; E. Hammond, *Biopiracy Watch: A compilation of some recent cases*, vol. 1, Third World Network 2013.

associated with them[61] acquired from their region by pharmaceutical companies in order to research new medicines, patent them and then reap the material benefits.

The Nagoya Protocol implements the third objective of the CBD Convention, namely (...) *the fair and equitable sharing of the benefits arising from the utilization of genetic resources, including by appropriate access to genetic resources and by appropriate transfer of relevant technologies, taking into account all rights over those resources and to technologies, and by appropriate funding, thereby contributing to the conservation of biological diversity and the sustainable use of its components*[62].

The States Parties to the Nagoya Protocol are mostly developing countries, for which the provision gives them the opportunity to legitimately raise their economic status by deriving material and immaterial benefits[63]. It states that genetic resources are pools of genes of species occurring naturally in nature (Latin: in situ), as well as man-made (Latin: ex situ) collections of resources – gene banks and microbial culture collections, including both living and dead biological material in the form of DNA or RNA.

And although the Nagoya Protocol does not cover human genetic material, it applies to micro-organisms or pathogenic micro-organisms isolated from human tissue, blood or body fluids. The analogy is with food commodities – the protocol does not apply directly to them, but it does apply to pathogens isolated from food[64]. In addition, it introduces concepts important for biosecurity and the protection of intellectual property[65].

The Nagoya Protocol is of indirect relevance to biosecurity, as its main purpose is to protect the rights of states to biological resources and intellectual property about them. It treats the protection of biological

[61] Traditional knowledge should be understood as folk, indigenous knowledge.

[62] *Nagoya Protocol on Access to Genetic Resources and the Fair and Equitable Sharing of Benefits Arising from their Utilization to the Convention on Biological Diversity*, art. 1.

[63] E. Martyniuk, *Nowe uregulowania prawne dotyczące dostępu do zasobów genetycznych zwierząt i ich potencjalny wpływ na prace hodowlane i badania naukowe* (Eng. New regulations on access to animal genetic resources and their potential impact on breeding work and research), "Przegląd Hodowlany" 2016, no. 5, pp. 10–14.

[64] G. Verkley, M. Dunja, D. Smith, *The Nagoya Protocol and mBRCs: towards a MIRRI Best Practice for Access and Benefit Sharing (ABS)* – presentation at ECCO 34 Conference, Session 2 BRCs and Regulations, Paris, 28 V 2015.

[65] *Nagoya Protocol on Access to Genetic Resources...*, art. 2c and 2d.

collections, including agents hazardous to health, indirectly. However, its provisions translate into the need to establish safeguards in facilities where pathogen genetic resources and knowledge about them are collected and stored, in order to prevent their theft or other illegal use. This has indirect implications for reducing the risk of their unlawful use for hostile purposes as defined in Article I of the BTWC[66].

International Health Regulations (2005)

The International Health Regulations (IHRs)[67] are a legally binding instrument developed by the WHO to strengthen national capacities for prevention, epidemiological surveillance, detection and early warning and response to public health emergencies of international concern (PHEICs).

States Parties to this agreement, including Poland, are obliged to implement the IHRs and to build or improve national capacities for detection, identification, surveillance, prophylaxys, prevention of the spread of communicable diseases, biological risk assessment and preparedness to respond to major public health threats of international concern, with coordinated cooperation of national services involved in the response (in the absence of such capacities – in cooperation with the services of other states). However, IHRs should not disrupt cross-border passenger traffic and trade and should be based on national measures (legislative, legal, organisational, training)[68]. They include, inter alia, recommendations for the introduction of measures to safeguard human health when crossing border crossings, applying to travellers, their luggage, containers, means of transport, goods and consignments[69]. Each year at the World Health Assembly (WHA), progress in above mentioned aspects is discussed among Member States in relations to the implementation of IHRs[70].

The IHRs apply to infectious diseases and health threats that may spread beyond the administrative borders of countries, and whose control may require a coordinated response by several countries. This includes biological, chemical and radiological threats of unknown etiology that

[66] *The Workshop on Nagoya Protocol for "Collection Holders"*, Brussels 2017.

[67] *The International Health Regulations…*

[68] Ibid., art. 2, 12–13.

[69] *The International Health Regulations…*, art. 15–22, 23–39.

[70] *Implementation of the International Health Regulations (2005): Report by the Director-General*, World Health Organization 2024, https://apps.who.int/gb/ebwha/pdf_files/WHA77/A77_8-en.pdf [accessed: 8 III 2025].

have the potential to cause significant harm to human populations, as well as outbreaks of naturally occurring diseases, accidental events involving biological agents and toxins due to work-related accidents or negligence, acts of vandalism or sabotage, and deliberate criminal use[71]. Thus, the IHRs also indirectly refer to the BTWC.

In the IHRs, biosafety and biosecurity issues are concerned on national public health security capacities. Each country should have its own diagnostic capacity and, and in the absence of this, should establish cooperation with another country's facility to ensure an optimal level of health security for all countries[72]. It is also obliged to develop, strengthen and maintain preparedness to respond quickly and effectively to health threats and emergencies of international concern[73]. The Member State should also provide occupational safety and health measures to minimise risks associated with biological agents in laboratories[74], procedures for responding to the natural, accidental and intentional use of biological agents and toxins that may have adverse effects on the health of the public[75], and ways to prevent and control the transboundary spread of communicable diseases and other health threats[76]. Similarly, the BTWC, in its Article IV, calls on States Parties to nationally implement all possible biosecurity and biosafety measures, including improved detection methods and means of surveillance for infectious diseases. This was emphasised during the 2011 and 2016 review conferences. Also during the intersessional period between 2007 and 2010, issues related to the protection of workers in laboratories, secure of pathogens, toxins and equipment, applicable to the provisions of the Convention (2008), and issues related to improving response capacity for detection, identification, diagnosis and control of infectious diseases (2009) were addressed.

The health threats that have emerged over the past two decades, including the COVID-19 pandemic, have prompted the revision and

[71] *The International Health Regulations...*, Appendix II, 2005.

[72] Ibid., art. 5.1, 14, Annex 1, paragraph 6(b), 2005.

[73] Ibid., art. 13.1, 2005.

[74] The World Health Assembly Resolution 58.29, *Enhancement of laboratory biosafety*, 2005.

[75] The World Health Assembly Resolution 55.16, *Global public health response to natural occurrence, accidental release or deliberate use of biological and chemical agents or radionuclear material that affect health*, 2002.

[76] The World Health Assembly Resolution 58.3, *Revision of the International Health Regulations*, 2005.

updating of IHRs in some areas (e.g. data protection, use of digital documents). In May 2024, amendments were adopted to adapt the IHRs to current and future health security challenges.

It is also worth mentioning the currently drafted Pandemic Treaty, which aims to better prepare countries for future health threats. Similar to the BTWC, here as well, during the negotiation process the dichotomy of statements between developing and developed countries was observed. Mostly related to the access to genetic material of biological agents with pandemic potential, biomedical technology, scientific results and intellectual property protection of medical devices used during a pandemic[77].

Safe transport of biological substances

Infectious substances are classified as dangerous goods, the uncontrolled acquisition or release of which may cause biological contamination of the environment and create health risks. The main framework regulations for the classification, packaging and transport of hazardous materials have been defined by the UN Committee of Experts on the Transport of Dangerous Goods (UNCETDG). On the basis of these, and with the support of international organisations playing a leading role in relation to specific types of hazards and modes of transport (road, rail, air and sea), specific regulations were developed. The WHO has advised the UN in the development of regulations for the transport of toxic and infectious substances.

The main piece of legislation concerning the international carriage of dangerous goods by road, including infectious materials, is the *Agreement concerning the International Carriage of Dangerous Goods by Road* – ADR[78]. Among other things, it introduces the obligation to ensure the safe transport of infectious materials and sets out the responsibilities of the shipper, carrier and driver.

The WHO Guidance on regulations for the transport of infectious substances[79], which compiles the applicable regulations and provides a lot

[77] *Intergovernmental Negotiating Body*, World Health Organization, https://apps.who.int/gb/inb/index.html [accessed: 17 XI 2024].

[78] *ADR 2023 – Agreement concerning the International Carriage of Dangerous Goods by Road*, United Nations 2022.

[79] *Guidance on regulations for the transport of infectious substances, 2023–2024*, World Health Organization 2024.

of practical advice on how to classify a consignment, how to pack it safely, how to label it and how to handle it during loading and carriage, is also helpful in addressing transport issues. All biohazardous substances are classified into Class 6 – toxic and infectious substances and Subclass 6.2 – infectious substances. Individual Class 6.2 materials have been assigned classification code numbers: I1 – hazardous materials for humans, I2 – hazardous materials for animals only, I3 – clinical waste, I4 – diagnostic samples. They should be additionally marked with one of the following UN codes for the time of transport: UN 2814 – infectious substances affecting humans, UN 2900 – infectious substances having an animal effect, UN 3373 – diagnostic speciments from human and animal materials, UN 3291 – infectious clinical waste. The individual codes determine the method of packaging. For example, UN 2814 and UN 2900 should be packed in accordance with Instruction P620, UN 3291, in accordance with Instruction P621, and in case of UN3373 the packaging instruction P650 applies. On the other hand, genetically modified biological agents that do not meet the definition of 'toxic substance' or 'infectious substance' are included in Class 9 – miscellaneous dangerous substances and articles, including substances hazardous to the environment, which must be labelled UN 3245 and packed according to instruction P904.

In addition to this, the transport of infectious biological materials is divided into Category A and Category B. Category A is infectious material known or suspected to be capable of causing a fatal disease, a life-threatening disease or capable of causing permanent damage to health in man or animals. Category B is infectious material that does not meet the criteria of Category A, such as clinical specimens transported to the laboratory for diagnostic purposes.

According to WHO recommendations, it is the responsibility of the sender to properly classify the biological material, to pack and label the package so that it reaches its destination and does not pose a risk to humans, animals and the environment during transportation. It is the responsibility of the sender to attach transport documentation, select the appropriate mode of transport and inform the consignee of the date of shipment to ensure that the package is protected at every stage of the journey.

The carriage of infectious materials is further detailed in the regulations applicable to the type of means of transport. Poland is also obliged to comply with them.

International recommendations on biosecurity

The BTWC, in its Article IV, obliges States Parties to take all possible measures and actions to prevent the development and production of biological agents, toxins and biotechnologies that could be used as weapons or as means of bioterror. This provision obliges not only to enact criminal law, but also to implement preventive measures that would allow peaceful work with micro-organisms to be carried out safely and protect them from hostile use. The wide range of places and activities where harmful biological agents and toxins are used (medical activities, including therapeutic entities, medical diagnostic laboratories, genetic engineering facilities, laboratories of sanitary and epidemiological stations, veterinary activities, including vivaria, veterinary clinics, scientific research activities, the pharmaceutical, biotechnology, agri-food sectors) required the use of supporting tools in addition to legally binding regulations. Handbooks, manuals, guidelines and other measures that discussed how to properly handle biological agents in order to protect health and facilities for their use were effective. International organisations, centres, institutions and associations specialising in narrow areas of safety and biosecurity in different spheres of activity have also played an important role.

Moreover, non-binding legal instruments proved to be clearer than prescriptive acts and easier to use in practice. It was much shorter and simpler, compared to amending existing legal acts, to amend them in order to adapt them to changing conditions, including current biological risks and advances in science.

Biosafety and biosecurity in the laboratory

Beside the health protection of workers exposed to harmful biological agents, no less important is the prevention of criminal acts in which these agents are used (bioterrorism, sabotage, etc.).

One of the most important recommendations is the WHO manual on laboratory biosafety[80], the first edition of which was published in 1983[81]. It accepts that biological agents are a major cause of risk and identifies the conditions for safe laboratory work and the principles for classifying biological agents, defines containment levels to delimit exposure and discusses equipment and apparatus as well as good practices for

[80] *Laboratory biosafety manual. Fourth edition*, World Health Organization 2020.

[81] *Laboratory biosafety manual. First edition*, World Health Organization 1983.

the different groups of hazardous agents and toxins. Standard operating procedures are described taking into account contingencies, personal protective equipment, rules for handling biological waste and infectious material, disinfection measures and sterilisation techniques. Subsequent editions of the manual have developed topics related to the individual responsibility of persons for safety and security, addressed bioethical aspects, issues of new developments in life sciences and biotechnology, issues of safe transport of consignments. A chapter on the physical protection of the facility and the premises of use of biological agents has been added, and the need for inventories of microorganisms and equipment, the protection of information and knowledge resources and the control of personnel with access to them has been developed.

Upon examination of the WHO's approach to laboratory biosafety, starting in 1983 and ending with the latest version of the manual, which was published in 2020, it can be seen that it was decided to move away from the original premise and accept that agents belonging to a given risk group need not be strictly subject to the rules assigned to a given biosafety level. The rationale for this was that the actual risk is not so much influenced by the biological agent as by the surrounding circumstances (staff competence, discipline in following internal laboratory procedures). Consequently, after taking into account the assumptions of the three previous editions of the handbook and in order to meet the needs of developing countries, it was assumed that the risk assessment of a hazard should take into account the individual, site- and situation-specific circumstances (e.g. the epidemic situation in the region or country, the level of containment of the laboratory, its equipment, the qualifications of the staff, the availability and type of personal protective equipment, as well as the geopolitical situation, including the likelihood of robbery, the presence of extremist groups).

In 2024, the WHO published guidelines in a publication entitled *Laboratory biosecurity guidance*[82]. This is a continuation of the above-mentioned handbook and supplements it with issues related to biosecurity in the laboratory. It provides an overview of practices and principles to help prevent serious biological incidents and discusses potential causes of these incidents and actionable steps at institutional, national and international levels. It covers topics such as:

[82] *Laboratory biosecurity guidance*, World Health Organization 2024.

a) biosecurity risk assessment using risk management methodologies, including storage conditions for biological agents, transport and possible use of micro-organisms and technologies in experimental research by type of activity (diagnostic, research, repository, biobank),
b) emerging and new technologies as well as potential risks associated with them (genetic engineering, including genome-editing technology[83], gene drive[84], epigenetic modification[85], synthetic biology, artificial intelligence, information protection and cyber-security, do-it-yourself (DIY) techniques, publication of research results that may provide information on how to produce biological and toxin weapons),
c) existing regulations in this area and guidelines for the development of national regulations (international and national law),
d) strengthening the role and responsibility of institutional biosafety committees,
e) critical situations – war, civil unrest, natural disasters.

When analysing these guidelines, it is also worth noting the background, namely the affiliation of the authors of the publications and the subject matter experts who supplemented their knowledge. It is then not difficult to interpret the intention of this endeavour, especially when one looks through the prism of variables such as the epidemic situation of the region, endemic diseases, the risk of serious public health threats with a cross-border impact, the current geopolitical situation, national positions presented at meetings on international disarmament and non-proliferation agreements, as well as taking into account the country of origin and profile of the financial backer. This gives hope that the guidelines developed,

[83] Genome editing technology – involves cutting out one or more genes and replacing them with another or others, or deactivating a gene. This technology is used in many areas of biological science and as an innovative therapeutic method for some previously incurable genetic diseases.

[84] Gene drive – a technique involving the genetic design of individuals so that they deliberately introduce new genes into the entire population of a species, which are then passed on in subsequent generations. It is mainly used to alter an entire free-living population or destroy it, e.g. crop pests, but also to regulate certain mosquito species that are vectors of infectious diseases, e.g. malaria or endemic haemorrhagic fevers.

[85] Epigenetic modifications – chemical changes affecting hereditary mechanisms of gene activity regulation, among others, pathogenicity, host immune response, pathogenesis and/or clinical picture of the disease.

by building on the experience of developed countries, will more effectively reach the right addressees in developing countries and thus, by promoting biosecurity at the source of the potential threat, strengthen the security and protection of biological resources and technologies globally.

The promotion of the principles of biosafety and biosecurity is also being addressed by other centres worldwide. An interesting reference is the textbook *Biosafety in Microbiological and Biomedical Laboratories*[86] published by the US National Institutes of Health, which extends the discussion of these issues to biomedical laboratories, veterinary facilities and vivaria used for research purposes.

In contrast, another handbook, authored by Peter Clevestig, titled *Handbook of Applied Biosecurity for Life Science Laboratories*[87], is a source of knowledge on how to secure facilities using particularly hazardous biological agents. It provides many useful instructions on laboratory biosecurity. Among other things, it describes in an easy-to-understand manner how to carry out a risk assessment for biosecurity and how to put the results into practice; what an employee's responsibility is for the agents he or she works with; how to exercise qualitative and quantitative control over laboratory resources; how to protect sensitive information relating to lists of infectious agents in possession, apparatus and equipment on the premises, personal data of patients from whom pathogens have been isolated and personal data of employees; how to secure the transfer and transport of particularly dangerous pathogens to minimise the risk of their illegal acquisition.

In contrast, the guidelines for the protection of biological resources developed by the Organisation for Economic Co-operation and Development (OECD) address the protection of microbial culture collections, their gene pools, biotechnology and the safety of laboratory workers and scientists potentially exposed to harmful biological agents. This is all the more so because the definitions of biosafety and biosecurity developed by the delegates of the States Parties participating in the BTWC meetings are the same as those used in the OECD publications[88]. The guidelines

[86] P.J. Meechan, J. Potts, *Biosafety in Microbiological and Biomedical Laboratories. 6th edition*, Centers for Disease Control and Prevention, National Institutes of Health 2020.

[87] P. Clevestig, *Handbook of Applied Biosecurity for Life Science Laboratories*, Stockholm International Peace Research Institute 2009.

[88] OECD, *Biological Resource Centres: Underpinning the Future of Life Sciences and Biotechnology*, Paris 2001. https://doi.org/10.1787/9789264193550-en; OECD, *OECD Best Practice Guidelines for Biological Resource Centres*, Paris 2007. https://doi.org/10.1787/9789264128767-en.

of specialised organisations and federations (World Federation for Culture Collections (WFCC)[89]; World Data Centre for Microorganisms (WDCM)[90]; European Culture Collections' Organisation (ECCO))[91] provide additional substantive and practical support in safeguarding the world's microbial cultures and enhancing biosecurity.

Medical and veterinary activities are some of the most important areas for the use of biological agents, so biosecurity at these sites is of particular importance. Unauthorised acquisition of biological agents and technology can also occur in other sensitive sites. Dissemination of dual use research of concern (DURC) is another area that needs to be monitored and protected, which is why it is important to educate and raise the awareness of those dealing with harmful biological agents about the risks, as well as to develop attitudes of responsibility[92]. Biosecurity is also an important element in countering intentional threats and acts of bioterrorism[93], safeguarding food resources from deliberate contamination (food terrorism) and deliberately causing damage to crops and livestock (agroterrorism)[94].

Summary

The aim of biosecurity is to prevent biological threats, including intentional ones. Given the wide range of potential threats (microorganisms, biological toxins, biological equipment, technology and specialised knowledge),

[89] *Guidelines for the Establishment and Operation of Collections of Cultures of Microorganisms. 3rd edition*, World Federation for Culture Collections 2010.

[90] World Data Centre for Microorganisms, https://www.wdcm.org/ [accessed: 24 XI 2024].

[91] The European Culture Collections' Organisation (ECCO), https://www.eccosite.org/ [accessed: 24 XI 2024].

[92] *Biosecurity – Freedom and Responsibility of Research*, Deutscher Ethikrat 2014; *Responsible Conduct in the Global Research Enterprise*, The InterAcademy Partnership (IAP) 2012; *Research and methods*, Robert Koch Institut, https://www.rki.de/EN/Content/infections/Dual_Use/code_of_conduct.html [accessed: 29 XI 2024]; *Dual-use research*, RIVM / Bureau Biosecurity, https://www.bureaubiosecurity.nl/en/dual-use [accessed: 29 XI 2024].

[93] *Preparedness for the deliberate use of biological agents : a rational approach to the unthinkable*, World Health Organization 2001; *Mental health of populations exposed to biological and chemical weapons*, World Health Organization 2005; *Public health response to biological and chemical weapons: WHO guidance*, World Health Organization 2004.

[94] *Terrorist threats to food: Guidance for establishing and strengthening prevention and response systems*, World Health Organization 2002.

their sources (natural, accidental, intentional) and the potential for the use of biological agents and biological technology (type of activity), biosecurity must be approached in a multifaceted manner. Disarmament and non-proliferation agreements and WMD control regimes (BTWC, Resolution 1540, CWC, AG) clearly indicate what should be the common denominator for effective protection of biological agents with dual-use potential and how to establish these measures at the national level[95]. Regulations referring to them indirectly (CBD and its protocols, IHRs, transport agreements) can strengthen biosecurity, even though they pursue completely different objectives. In turn, the recommendations and guidelines of the leading centres in the field provide valuable knowledge and guidance for their practical implementation at not only institutional and departmental level, but also at national level. They thus contribute to strengthening biosafety and security on a global scale.

Bibliography

Bielecka-Oder A., *Safety and Security Regulations Against Biological Threats*, in: *Defence Against Bioterrorism*, V. Radosavljevic, I. Banjari, G. Belojevic (eds.), Springer Netherlands 2018.

Biosecurity – Freedom and Responsibility of Research, Deutscher Ethikrat 2014.

Clevestig P., *Handbook of Applied Biosecurity for Life Science Laboratories, Stockholm International Peace Research Institute 2009.*

[95] Namely: a) ensure the physical protection of laboratories and storage and collection sites for biological agents referred to in Article I of the BTWC against unauthorised access and illegal seizure; b) take appropriate measures to ensure the protection of biological agents, toxins and technologies relevant to the BTWC, including through access control measures, the proper handling of such agents and specialised equipment during their use and transport; c) adopt, in accordance with the constitutional arrangements of States Parties, legislative, administrative, judicial and other measures, including penal legislation, to ensure the safety and security of biological agents, toxins and technologies in laboratories, facilities for their use and during their transportation; d) establish comprehensive and specific national measures to control the use of biological agents, toxins and technologies for peaceful purposes; e) periodically review these agents, toxins and technologies and, where necessary, enact or update national legislation, including regulatory and penal measures, to ensure the effective implementation of the prohibition in Article I of the BTWC, and update the lists of biological agents and facilities relevant to ensure the safety, security and maintenance of regimes during the transfer of these agents.

Collins English Dictionary – Complete and Unabridged, 12th edition, Collins 2014.

Guidance on regulations for the transport of infectious substances, 2023–2024, World Health Organization 2024.

Guidelines for the Establishment and Operation of Collections of Cultures of Microorganisms. 3rd edition, World Federation for Culture Collections 2010.

Hammond E., *Biopiracy Watch: A compilation of some recent cases*, vol. 1, Third World Network 2013.

Laboratory biosafety manual. First edition, World Health Organization 1983.

Laboratory biosafety manual. Fourth edition, World Health Organization 2020.

Laboratory biosecurity guidance, World Health Organization 2024.

Martyniuk E., *Nowe uregulowania prawne dotyczące dostępu do zasobów genetycznych zwierząt i ich potencjalny wpływ na prace hodowlane i badania naukowe* (Eng. New regulations for access to animal genetic resources and their potential impact on breeding work and research), "Przegląd Hodowlany" 2016, no. 5, pp. 10–14.

Meechan P.J., Potts J., *Biosafety in Microbiological and Biomedical Laboratories. 6th edition*, Centers for Disease Control and Prevention, National Institutes of Health 2020.

Nixdorff K., Schilling D., Hotz M., *Critical Aspects of Biotechnology in Relation to Proliferation*, in: *The Implementation of Legally Binding Measures to Strengthen the Biological and Toxin Weapons Convention*, M. Chevrier et al. (eds.), NATO Science Series II – vol. 150, 2004.

OECD, *Biological Resource Centres: Underpinning the Future of Life Sciences and Biotechnology*, Paris 2001. https://doi.org/10.1787/9789264193550-en.

OECD, *OECD Best Practice Guidelines for Biological Resource Centres*, Paris 2007. https://doi.org/10.1787/9789264128767-en.

Preparedness for the deliberate use of biological agents: a rational approach to the unthinkable, World Health Organization 2001.

Public health response to biological and chemical weapons: WHO guidance, World Health Organization 2004.

Responsible Conduct in the Global Research Enterprise, The InterAcademy Partnership (IAP) 2012.

Terrorist threats to food: Guidance for establishing and strengthening prevention and response systems, World Health Organization 2002.

Internet sources

Approved 1540 Committee Matrix of [State], https://www.un.org/en/sc/1540/documents/Matrix%20Template%202013%20(E).pdf [accessed: 17 XI 2024].

Australia Group Common Control Lists, The Australia Group, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/controllists.html [accessed: 30 XI 2024].

Biological Weapons Convention – Ninth Review Conference, United Nations, Office for Disarmament Affairs, https://meetings.unoda.org/bwc-revcon/biological-weapons-convention-ninth-review-conference-2022 [accessed: 8 III 2025].

Confidence Building Measures, United Nations, Office for Disarmament Affairs, https://disarmament.unoda.org/biological-weapons/confidence-building-measures/ [accessed: 13 X 2024].

Dual-use research, RIVM / Bureau Biosecurity, https://www.bureaubiosecurity.nl/en/dual-use [accessed: 29 XI 2024].

Fighting the spread of chemical and biological weapons, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/index.html [accessed: 22 II 2025].

Hyuk K., *Intangible Transfer of Technology (ITT): Open-source Information Analysis for the Implementation of Sanctions on North Korea*, 38 North, 10 III 2023, https://www.38north.org/2023/03/intangible-transfer-of-technology-itt-open-source-information-analysis-for-the-implementation-of-sanctions-on-north-korea/ [accessed: 9 III 2025].

Implementation of the International Health Regulations (2005): Report by the Director-General, World Health Organization 2024, https://apps.who.int/gb/ebwha/pdf_files/WHA77/A77_8-en.pdf [accessed: 8 III 2025].

Intergovernmental Negotiating Body, World Health Organization, https://apps.who.int/gb/inb/index.html [accessed: 17 XI 2024].

Introduction, The Australia Group, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/introduction.html [accessed: 21 IX 2024].

Participants, The Australia Group, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/participants.html [accessed: 21 IX 2024].

Research and methods, Robert Koch Institut, https://www.rki.de/EN/Content/infections/Dual_Use/code_of_conduct.html [accessed: 29 XI 2024].

Sprawozdanie roczne z postępów w realizacji strategii Unii Europejskiej przeciw rozprzestrzenianiu broni masowego rażenia (2022) (Eng. Annual Progress Report on the Implementation of the European Union Strategy against the Proliferation of Weapons of Mass Destruction (2022)), Prawo.pl, https://www.prawo.pl/akty/dz-u-ue-c-2023-383,72216862.html [accessed: 28 IX 2024].

Statement by the Chair of the 2022 Australia Group Plenary, The Australia Group, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/2021-ag-plenary-statement.html [accessed: 22 IX 2024].

The European Culture Collections' Organisation (ECCO), https://www.eccosite.org/ [accessed: 24 XI 2024].

World Data Centre for Microorganisms, https://www.wdcm.org/ [accessed: 24 XI 2024].

Legal acts

ADR 2023 – Agreement concerning the International Carriage of Dangerous Goods by Road, United Nations 2022.

Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, 1993.

European Agreement Concerning the International Carriage of Dangerous Goods by Road (ADR).

Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, 1925.

Nagoya Protocol on Access to Genetic Resources and the Fair and Equitable Sharing of Benefits Arising from their Utilization to the Convention on Biological Diversity, (Official Journal of the EU L 150/234 of 20 May 2014).

Resolution 1540 (2004) / adopted by the Security Council at its 4956th meeting, on 28 April 2004, 2004.

The Cartagena Protocol on Biosafety to the Convention on Biological Diversity, 2003.

The Convention on Biological Diversity, 1993.

The Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, 1972.

The European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways (ADN).

The IATA Dangerous Goods Regulations (IATA DGR).

The International Health Regulations, World Health Organization 2005.

The Nuclear Non-Proliferation Treaty (NPT), 1968.

The Regulation concerning the International Carriage of Dangerous Goods by Rail (RID).

Official positions and documents

Biosafety and Biosecurity – Submitted by the Implementation Support Unit, 24 June 2008.

Final Document of the Ninth Review Conference, Geneva 2022.

Final Document of the Eighth Review Conference, Geneva 2016.

Final Document of the Seventh Review Conference, Geneva 2011.

Final Document of the Sixth Review Conference, Geneva 2006.

Final Document of the Fifth Review Conference, Geneva 2001–2002.

Final Document of the Fourth Review Conference, Geneva 1996.

Final Document of the Third Review Conference, Geneva 1991.

Final Document of the Second Review Conference, Geneva 1986.

Mental health of populations exposed to biological and chemical weapons, World Health Organization 2005.

Statement by the Chair of the 2023 Australia Group Plenary, Paris 2023.

Statement by the Chair of the 2024 Australia Group Plenary, Paris 2024.

The Workshop on Nagoya Protocol for "Collection Holders", Brussels 2017.

The World Health Assembly Resolution 58.29, *Enhancement of laboratory biosafety*, 2005.

The World Health Assembly Resolution 58.3, *Revision of the International Health Regulations*, 2005.

The World Health Assembly Resolution 55.16, *Global public health response to natural occurrence, accidental release or deliberate use of biological and chemical agents or radionuclear material that affect health*, 2002.

Verkley G., Dunja M., Smith D., *The Nagoya Protocol and mBRCs: towards a MIRRI Best Practice for Access and Benefit Sharing (ABS)* – presentation during ECCO 34 Conference, Session 2 BRCs and Regulations, Paris, 28 V 2015.

Anna Bielecka-Oder, PhD

Biologist in microbiology, epidemiology specialist, doctor of medicine and health sciences. She specialises in the area of biosafety and biosecurity as well as epidemiology of highly infectious biological agents, including biological agents used as weapons. She also deals with planning issues related to prevention as well as preparedness and response capacity to such events.

Contact: a.bieleckaoder@gmail.com

REVIEW ARTICLES / REVIEWS

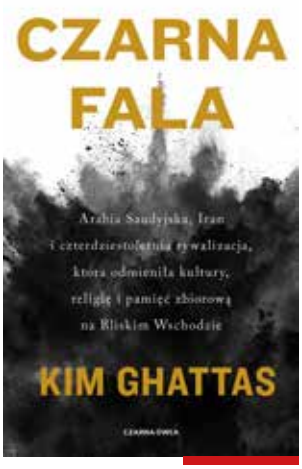
Terrorism – Studies, Analyses, Prevention, 2025, no. 7: 463–480

https://doi.org/10.4467/27204383TER.25.039.21816

Review

Kim Ghattas, Black Wave: Saudi Arabia, Iran and the Forty-Year Rivalry that Unraveled Culture, Religion, and Collective Memory in the Middle East[1]

Krzysztof Izak
Independent author
https://orcid.org/0000-0001-9815-6035



Kim Ghattas is a journalist and writer who was born and grew up in Lebanon and now lives alternately in Beirut and Washington, DC. For 20 years she has reported and commented on events in the Middle East for the BBC and the *Financial Times*. The author is a fellow of the Carnegie Endowment for International Peace think tank in Washington, DC and a member of the Board of Trustees of the American University of Beirut.

The reviewed publication was published in English in 2020. Against the backdrop of numerous works on the Middle East, it is

[1] K. Ghattas, *Black Wave: Saudi Arabia, Iran and the Forty-Year Rivalry that Unraveled Culture, Religion, and Collective Memory in the Middle East,* Warszawa 2023, Czarna Owca, 496 p.

an outstanding and unique position as it details the rivalry between Saudi Arabia and Iran. Shortly after its publication, *The New York Times* named it one of the best non-fiction books.

The author used many different types of sources in the publication, including: archival documents, academic papers and newspaper articles. Particularly noteworthy is the number of interviews she has conducted, including with well-known personalities such as Saudi Prince Turki al-Faisal, the leader of the Tunisian Renaissance Party (Arabic: Hizb al-Nahda) Rachid al-Ghannouchi and Saudi journalist Jamal Khashoggi, who was assassinated in 2018. Ghattas has portrayed history not through the prism of only important personalities, but has taken into account the participation of many lesser-known or even unknown political players who nevertheless had a significant impact on events. It is worth noting that such an approach is rare.

The book *Black wave*... facilitates understanding of events in the Middle East from 1979 to 2019. The fact that different countries and periods were covered certainly complicated the work on the book, but it allows the reader to see a broader perspective, covering the whole region. The author has skilfully combined historical, religious, cultural and geopolitical themes, providing extensive knowledge of the relatively little-known (apart from specialists) rivalry between Saudi Arabia and Iran. Since the victory of the Islamic Revolution in 1979, this rivalry has often been inspired by the United States. In the reviewed book, however, US foreign policy in the Middle East is presented as secondary to the situation in the region, to decisions made in Tehran, Riyadh, Cairo and other capitals, and to the ambitions of local decision-makers. According to the author, the people there are not just victims of Western policy, but suffer the consequences of the decisions of their own authorities. Relations between Sunni-Wahhabi Saudi Arabia and Shiite Iran translate into international relations in the Muslim world and become a source of many tensions, political murders, terrorism and armed conflicts. The author has masterfully combined historical issues with information from witnesses to the events. The book confronts readers with the harsh realities faced by ordinary people in the Middle East, experiencing the tragic consequences of antagonism in Lebanon, Syria, Iraq and Yemen, and religious fanaticism in Egypt and Pakistan. The suffering experienced by millions is a proof of how geopolitical rivalries translate into human misery.

Ghattas presented a fascinating gallery of characters whose lives were often intertwined. Many of them ended their lives tragically, others had to flee their country to save themselves. A list with a brief description of 59 key individuals, out of the hundreds of decision-makers, dissidents, participants and witnesses to the events mentioned in the text, is included at the beginning of the book. Thanks to this, while reading it is possible to back to the note about the character you are currently reading about. The list is divided by country. These are as follows: Lebanon, Iran, Saudi Arabia, Iraq, Syria, Pakistan and Egypt.

The introduction begins with the question: *What happened to us?*[2] (p. 19), which the rational thinking part of Arab society asks itself. This includes the author, as well as her interlocutors, who remember the days before the black wave[3] and the dramatic change of life when this wave spread in their countries. The question is meant to prompt reflection on when and why religious fanaticism, sectarian killings and amorphous wars spread in the Arab and Muslim world. The book's subtitle: *Saudi Arabia, Iran and the Forty-Year Rivalry that Unraveled Culture, Religion, and Collective Memory in the Middle East* may suggest one of the answers. The author repeats the question towards the end of the book (p. 450) and tries to answer it with a brief summary of the events presented.

The book consists of three parts entitled: *Revolution, Competition* and *War*. These titles, as well as the titles of most chapters, such as: *Darkness, I killed the Pharaoh, No Dupatta* or *Cain and Abel*, clearly indicate that Ghattas did not write it with Middle East experts in mind, but wanted to reach a wide readership. In my opinion she succeeded perfectly. At the beginning of each chapter, in addition to the title and motto, countries and time period covered are listed.

Part I of the book contains four chapters. In the first, entitled *Cassette Revolution*, the author presents the events unfolding between 1977 and 1979 in Lebanon, Iran, Iraq and France. She devoted chapter two to Iran 1979–1980, chapter three to Saudi Arabia in 1979 and chapter four focused

[2] The quotes come from the electronic version of the original: Kim Ghattas, *Black Wave: Saudi Arabia, Iran and the Forty-Year Rivalry that Unraveled Culture, Religion, and Collective Memory in the Middle East* (New York, 2020), Kindle version. The review is about the Polish translation of the book.

[3] The term comes from the colour of the flags used by Muslim terrorist organisations such as Al-Qaeda or the Islamic State. Fighters of the latter organisation flew them as they seized city after city in Iraq and Syria.

on the bloody events unfolding between 1979 and 1980 in Saudi Arabia, Iraq, Iran, Syria and Afghanistan. The history starts in Lebanon in 1977, when there was a civil war in the author's homeland. Before it happened, the state was home to oppositionists, revolutionaries and terrorists from various countries. Among them were Palestinian militants from Al-Fatah (Arabic: Harakat at-Tahrir al-Filastini) and the Palestine Liberation Organisation (PLO, Arabic: Munazzamat at-Tahrir al-Filastiniyyah), local armed nationalist and religious groups, and secular nationalists from the Freedom Movement of Iran (Persian: Nehzat-e Azadi-e Iran) headed by Mostafa Chamran, who had established contacts with local Shiites. He urged the Shah of Iran Mohammad Reza Pahlavi to relinquish the throne. Chamran played a very important role in the subsequent Islamic Revolution and was the first Minister of Defence in post-revolutionary Iran. Another Iranian refugee, Musa Sadr, founded an organisation in Lebanon called the Movement of the Disinherited (Arabic: Harakat al-Mahrumin) to defend the interests of the Shiite population, which is the poorest religious community in the country. He also established the Supreme Shiite Council (Arabic: Al-Majlis al-Alam ash-Shia). The Iranian revolution, accompanied by mass protests in the streets, activated not only oppressed Shiites in Lebanon, but also French Marxist intellectuals such as Michel Foucault and Jean-Paul Sartre. They wondered whether the waning tide of Arab and European socialist revolution was now being supported by a Persian revival.

In October 1978, Ayatollah Ruhollah Khomeini arrived in France with some activists of the Freedom Movement of Iran, who were forced to leave Iraq. Saddam Hussein took over there and reignited hostilities between Arabs and Persians as well as between Sunnis and Shiites, and in 1980 declared war on Iran. In France, Khomeini was able to enjoy freedom to speech and unlimited access to the world press. There he recorded calls for the overthrow of the Shah, then sent to Iran and played in mosques. His stay in Neauphle-le-Château in the suburbs of Paris lasted less than four months. On 16 January 1979, the Shah and his family left Iran for exile. Two weeks later, Khomeini triumphantly returned there and after ten days declared the victory of the Islamic Revolution. The first foreign leader to meet with him was Yasser Arafat – chairman of Al-Fatah and the PLO. He arrived in Tehran on 17 February on a plane lent to him by Syrian President Hafez al-Assad. The course of this visit is described by Ghattas in interesting detail.

The Saudis were very concerned about the revolution in Iran. Events in their own country were also of great concern to members of the ruling dynasty and religious officials. On 20 November 1979, several hundred Islamic extremists, led by Juhayman ibn Muhammad al-Otaibi and Muhammad ibn Abdullah al-Qahtani, overran the Grand Mosque in Mecca (Arabic: Al-Masjid al-Haram). Al-Otaibi subjected Riyadh's policies to criticism – he accused the monarchy of apostasy and alliance with Christians. He demanded that foreign experts, engineers and military advisers leave Saudi Arabia. He called for the introduction of "pure" Wahhabism, which he claimed the Saudis and pro-government Muslim scholars had abandoned. He proclaimed that his companion, al-Qahtani, was *the mahdi*, or messiah. The rebellion was brutally suppressed by the authorities. It took two weeks for government forces, supported by French commandos, to retake the mosque. The permission for the French infidels to enter the shrine was given by the Grand Mufti of Saudi Arabia and his supreme religious authority Abdel Aziz bin Baz, whose vision of Islam was no less conservative than Khomeini's. The French soldiers, of course, had to accept Islam first. Bin Baz then used the whole event to force the royal family and the public to live according to the precepts of Islam, as demanded by the rebels occupying the mosque. After the events in the Grand Mosque, which resulted in the deaths of all the rebels (some during storming of the shrine, others in executions), the Saudi Arabian authorities, fearing further revolts launched by religious fanatics, began to implement the demands of their leaders and made many changes to the legal system in accordance with Sharia rules. After 1979, women were barred from hosting television programmes, banned from publishing photos in newspapers and advertisements featuring them and from being employed, as well as forced to cover their entire bodies in public spaces. Clubs and cinemas were closed. The religious police, i.e. officers of the Committee for the Promotion of Virtue and Prevention of Vice (Arabic: Hayat al-Amr bi al-Maaruf wa al-Nahi an al-Munkar), were given ample funding and autonomy of action. The radical imams and preachers who inspired al-Otaibi, and later Osama bin Laden and other terrorists, have led to consolidate Wahhabi principles in Saudi society – from school books promoting intolerance of dissenting religious beliefs to the rollback of human rights for women and religious minorities, as in Iran. The country's authorities were interested in the Saudi ruling elite. Khomeini was a staunch critic of the Saud dynasty and called for their

overthrow. "Exporting the Islamic Revolution" became a central theme of Iranian foreign policy. Due to active efforts of Iran's new leadership, the Saudis began to promote their own version of radical Islam abroad in order not only to protect but also to increase their influence. Riyadh has spent billions of dollars building mosques and religious schools abroad and funding religious charities loyal to radical Wahhabi ideology and considering Shiites as heretics. The Iranians have done the same in countries with large Shia populations, such as Lebanon, Afghanistan and Pakistan. They have tried to portray Iran and its leaders as the true vanguard of Islam, going against all its enemies, including the Saudis.

On 25 December 1979, the invasion of Afghanistan by Soviet troops took place. The three events of 1979: the revolution of Iran, the seizure of the mosque in Mecca and the entry of Soviet forces into Afghanistan had nothing to do with each other, but their occurrence led to disaster. The fall of Shah was initially supported by merchants, nationalists and the Iranian left, but supporters of Khomeini and the theocratic Shiite state quickly gained the upper hand. The attack on Mecca was carried out by extremists who saw the Saud dynasty as traitors to the rigours of Wahhabi Islam. Afghanistan became the first battlefield of international jihad in modern times. These events changed the Middle East forever and started the process of re-Islamisation of the Muslim world in the spirit of radical Islam.

The Islamic revolution in Iran and seizure of the mosque in Mecca triggered far-reaching changes in Saudi Arabia with the slow but determined expansion of Salafi puritanism. These were accelerated by the Soviet occupation of Afghanistan and the attack by Iraqi troops on Iran on 22 September 1980. This was the beginning of the eight-year war that both sides called Arab-Persian, referring to a division dating back to the 7th century[4]. Ghattas saw an imbalance in the way events in Iran, Afghanistan and Saudi Arabia were reported at that time. While news from the former two countries made headlines around the world, events in Saudi Arabia received little media attention. However, according to the author: *There were two Islamic revolutions in 1979.* (...) *Both were misunderstood. One was a sudden, dramatic reversal of progress and rejection of centuries of history, the other was a slow but forceful expansion of Salafist puritanism. Both of them would transform their country of origin and then ripple across the Arab and*

[4] The division of the followers of Islam into Sunnis and Shiites occurred in the 7th century. After the death of the third caliph of the righteous dynasty, Uthman ibn Affan, in 656, a confrontation between the two began.

Muslim world for decades to come (p. 112). This – according to Ghattas – became the source of the black wave that swept across the Muslim world in the following years.

The author of the book interestingly describes the changes taking place in the two countries that were the cradle of the black wave, i.e. Iran and Saudi Arabia. They were becoming increasingly oppressive towards their citizens. After the declaration of the victory of the Islamic Revolution in Iran, terror began. All universities were closed down. Their activities relaunched after three years, but with different staffing. Purges were carried out among the lecturers, but also in the student community. They were also carried out in the army and state institutions. In time, "the revolution began to devour its own children". Thousands of people died. The revolt in Iran inspired opponents of Syrian President Hafez al-Assad and in 1982 there was a rebellion organised by the Muslim Brotherhood (Arabic: Al-Ichwan al-Muslimin) in the city of Hama. Both uprisings were bloodily suppressed by government forces. The Muslim Brotherhood have never forgiven Khomeini and Iran for being abandoned by them. Said Hawwa – one of the leaders of the Syrian Muslim Brotherhood, who initially praised Khomeini and his revolution – began to denounce the Ayatollah as a threat to the Sunni Muslim world. The Islamic world once again entered, as in the Middle Ages, a phase of fighting between different religious trends.

Part II of the book has eight chapters. The first and seventh are devoted to events in Egypt (1977–1995), the second and fourth to events in Pakistan (1978–1988), the third to events in Lebanon (1980–1988), and the fifth and eighth to events in Saudi Arabia (1987–2001). In the sixth chapter, titled *Culture Wars*, the author described the changes that took place in the above-mentioned countries between 1988 and 1990. The transformation under the influence of radical Islam took place rapidly and covered all areas of life. Ghattas devoted a great deal of space to Egypt. In 1928, the aforementioned Society of Muslim Brotherhood (Arabic: Jamiyat al-Ichwan al-Muslimin)[5] was established in the country and successfully developed, which over the following decades spread throughout the Muslim world and became

[5] The organisation that originated in Egypt was called the Society of Muslim Brotherhood. Over the years, it became international in character and there was the disappearance of the word "society" in the name and the emergence of a shorter form – the Muslim Brotherhood.

the source of many terrorist organisations[6]. Before this, however, secular science, culture and art developed. Egyptian women were the pioneers and key figures of Arab feminism. Singer Umm Kulsum had an international career and fame, and Egyptian President Gamal Abdel Nasser treated her like a national asset. According to Ghattas, Egypt is a prime example of the acceleration and exacerbation of radical re-Islamisation as a result of the Iranian revolution and the resurgence of Saudi Wahhabism. One manifestation of this re-Islamisation was the rise of the Egyptian Islamic Jihad organisation (Arabic: Al-Jihad al-Islami al-Misri), founded in 1978 by the group's chief ideologue and strategist Muhammad Abd as-Salam Faraj and Egyptian army officer Abbud Abd al-Latif az-Zummur. The main aim of this organisation was to overthrow the authorities in Egypt. Faraj's book entitled *Al-Farida al-Ghajba* (English: Neglected Obligation), published underground in 1980, became a new interpretation of jihad. In it, the author stated, among other things, that the means to achieve the ultimate goal of reconstituting a Muslim state was through armed struggle and the killing of those who had embezzled from the principles of Islam. Faraj's concept of holy war became an apologia for terrorism and legitimised the assassination of Egyptian President Anwar Sadat, who had betrayed Islam by signing a peace agreement with Israel in March 1979. The assassination of Sadat took place on 6 October 1981 in Cairo. During a military parade, organised to mark the anniversary of the 1973 war with Israel, four members of the Egyptian Islamic Jihad, under the command of Lt Khalid Ahmed Shavki al-Islambuli, armed with automatic assault rifles and grenades, broke away from the parading subdivision and attacked the stand where the president and his guests of honour were located. Apart from Sadat, eight people were killed and around 30 wounded, including US army officers[7]. Four of the direct bombers and Faraj were sentenced to death, while many others received prison terms. Among them was

[6] From the 1970s onwards, factions began to play a major role in the national structures of the Muslim Brotherhood, which decided to achieve their goals, including the overthrow of infidel rule and Islamisation, not by continuing organic work but by armed struggle. In Egypt, the Egyptian Islamic Jihad emerged from the Muslim Brotherhood; in Lebanon – the Islamic Unification Movement; in Gaza – Hamas; in Sudan – the National Islamic Front.

[7] The author of the book erroneously attributed the attack to the Islamic Group Arabic: (Al-Jama'a al-Islamiyya). It was carried out by the Islamic Jihad Arabic: (Al-Jihad al-Islami). The author of the review briefly elaborated on the course and consequences of this attack. See: K. Izak, *Leksykon organizacji i ruchów islamistycznych* (Eng. Lexicon of Islamist organisations and movements), Warszawa 2014, pp. 158–159.

doctor Ayman al-Zawahiri. He was accused of involvement in the planning of the attack and arms trafficking. He was sentenced to three years in prison. After his release in 1984, he went to Peshawar, Pakistan, where he took up a cooperation with Osama bin Laden.

The second half of the 1980s saw a number of attacks on Egyptian politicians and intellectuals. In 1987, former Minister of the Interior Hassan Abu Basha was severely injured and Makram Mohamed Ahmed, editor-in-chief of the weekly Al-Musawar (English: The Shaper), was assassinated. In 1989, former Interior Minister Zaki Badr was the victim of an assassination attempt, and in 1990 – Rifat Mahjub, Speaker of Parliament. In 1992, Farag Foda, a well-known intellectual and opponent of Islamic radicalism, was killed. During the trial of Foda's killers, Mohammad al-Ghazali, a leading Muslim scholar and charismatic preacher, who was called as a defence witness, stated that when a person born a Muslim fights against Sharia, as Foda did, he or she commits an act of apostasy punishable by death. Ghattas writes: (...) *it was up to the state to carry out the sentence of death against apostates after a trial, but since the state had failed to curb Foda, the sentence could be carried out by righteous Muslims. Chillingly, Ghazali declared there was no punishment for a Muslim stepping in to carry out this deadly duty* (p. 270). In 1993, extremists attempted to assassinate Prime Minister Atef Sidki, Interior Minister Hassan Muhammad al-Alfi and Information Minister Safwat al-Sharif. They also attacked Nobel Prize for Literature laureate Naguib Mahfouz. In 1994, he was stabbed in the neck. He survived, but his hand was severely damaged. University lecturer Nasr Abu Zeid became another target. Inappropriate content was found in his works and he was labelled an apostate. The court divorced him from his wife against his will, as according to Islamic principles a Muslim woman cannot be married to a dissenter (Abu Zeid became one as an apostate). His wife disobeyed the verdict and in 1995 they both left for Europe. They settled in Leiden, in the western Netherlands, where Abu Zeid was offered a job at the local university. These events made it clear that radical Islam was influential in Egyptian legal circles, and not only among advocates, whose union the Muslim Brotherhood had already taken control of in 1992, but also among judges. It turned out that moderate and radical Islamists began to act together – the latter murdering victims identified by the former. Targeting secular intellectuals served to deepen religious fanaticism.

The black wave also reached Pakistan. The author begins her narrative on the country with the story of Mehtab Channa (after her

husband: Mehtab Akbar Rashdi), a well-known TV and radio presenter and lecturer at the University of Sindh, who went to the United States to study international relations. She returned to Pakistan in 1978, a year after the dictatorship was introduced there. In July 1977, the charismatic and popular Prime Minister Zulfiqar Ali Bhutto, a follower of Shiite Islam in its moderate version, was arrested. He was deposed by the commander of the armed forces, General Mohammad Zia ul-Haq, who promised that the situation created after the coup would be temporary. He declared: *My sole aim is to organize free and fair elections which would be held in October this year* (...)*Soon after the polls, power will be transferred to the elected representatives of the people. I give a solemn assurance that I will not deviate from the schedule* (p. 162). However, elections never took place and in September 1977 the general declared himself president. In April 1979, despite worldwide protests, Zulfiqar Ali Bhutto was executed. Ghattas devotes considerable attention to the events unfolding in Pakistan. He recalls that Islamist groups have been active there for decades. The largest and best known, the Muslim Association (a.k.a. Jama'at-e Islami), was established as early as 1941, six years before the creation of Pakistan. It was founded in the city of Lahaur by the well-known radical Muslim scholar Abu Al al-Mawdudi. However, changes in the country leading to its Islamisation were slow. They accelerated after the seizure of power by Zia ul-Haq, who called himself a soldier of Islam. He was a deeply believing, orthodox Muslim, usurping the moral right to undertake a broad policy of Islamising the state. His ambition was to make every Pakistani a devout and God-fearing Muslim. On 10 February 1979, the day before the declaration of the victory of Islamic Revolution in Iran, Zia ul-Haq introduced strict Shariah laws. Mehtab Channa watched these changes with horror. She was fired from television because she disagreed with an order to cover her hair on camera. This order soon began to apply to women in public spaces. At the same time, Saudi Arabia's religious influence in Pakistan had been growing since the early 1980s. Aid, mainly American and Saudi, flowed through the country for the Afghan mujahideen fighting the Russians. Saudi financial support for Quranic schools educating children and young people who had fled Afghanistan was also growing. The young generation gave birth to the Taliban.

At the time, the city of Peshawar, known as "mini Arabistan" and a kind of melting pot of international jihad, played an important role. Volunteers coming from all over the world to fight the Red Army in

neighbouring Afghanistan gathered there. Al-Qaeda founders Abdallah Azzam, Osama bin Laden and Ayman al-Zawahiri also stayed there. In turn, Jamal Khashoggi, to whom Ghattas devoted the last chapter of the book, was a correspondent in Peshawar, sending admiring dispatches to Saudi newspapers. He was fascinated by the jihadist international in which he saw the unity of the ummah, i.e. the worldwide Muslim community. In his eyes, the Afghan mujahideen were waging a just and glorious war against the infidels, i.e. the Soviet invaders. Armed groups and militias were being formed with the approval of the Pakistani special services to attack the Shia minority. In 1987, Afghan and Pakistani militants attacked villages belonging to the Shiite Turi tribe in the Kurram region, on the border with Afghanistan. The Shiites repelled the attack. In the fighting, which lasted two weeks, 52 Shiites and 120 Sunnis were killed and 14 villages were partially or completely destroyed. According to Ghattas: *Here then was the epicentre of modern-day sectarian bloodletting, the first of its kind in modern times. Sectarianism had been weaponized. Targeted assassinations came next* (p. 230). The rivalry between Saudi Arabia and Iran spilled over into Pakistan, where Sunnis and Shiites began to systematically murder each other. This hatred was skilfully fuelled by the Saudi Arabian authorities, who persecuted Shiites in their country and detained their religious leaders. The Saudis have poured many millions of dollars into rebuilding the temple complex in Mecca, destroyed in the 1979 events, and erecting hotels for pilgrims around it. This task was outsourced to the Saudi Binladin Group, a construction holding company founded in 1931 by Muhammad Bin Laden, Osama's father. In the process, many monuments remembering the time of the first Muslims were demolished. The Wahabbi religious establishment, fighting against any commemoration of ancestors, was most pleased with these measures. At the same time, religious rigour was intensifying. In order to bring about reform in Saudi Arabia, to divert attention from their own Western lifestyle and to secure the legitimacy of their exercise of power with Muslim scholars, the Saudis gradually increased their privileges and their ability to control social life. In 1984, King Fahd opened the Holy Quran Printing Complex named after him (Arabic: Majma al-Malik Fahd al-Itibit al-Mushaf al-Sharifi), one of the largest printing houses in the world, capable of producing 8 million copies of the Quran per year. It printed a new, supposedly perfect, version of the holy book, complete with annotations and commentaries, and its English translation. Plenty of copies of this version of Quran (and its

subsequent reprints), containing, among other things, violent content against Jews and Christians, were distributed to pilgrims and abroad through Saudi embassies.

In 1986 – as Ghattas writes – (...) *King Fahd announced he was officially replacing the title of His Majesty the King with that of Custodian of the Two Holy Mosques. First introduced by Saladin during the Crusades, the title had never been officially used, until King Fahd* (p. 241). Throughout the Iraq-Iran war (1980–1988), Fahd supported Baghdad with billions of dollars. Wahhabi ideology, which inspired Saudis and other Muslims to fight against the Soviet occupation of Afghanistan, became a tool for spreading ideas of intolerance, radicalisation and terrorism in the Islamic world. The government in Riyadh viewed Saudi jihadi fighters differently at home and abroad. It fought the former and treated the latter as Wahhabi martyrs. The detachment of the Saudis from Wahhabism was what the Americans wanted. However this was not possible. This ideology had brought them to power and they derived their legitimacy from it. The country's religious elite enjoyed the patronage of many princes and a conflict with the Wahhabis could have deprived the Saudis of power.

After the US attack on Afghanistan in October 2001 and Iraq in 2003, a new wave of radicalisation emerged in Saudi Arabia, similar to that which followed the 1991 Iraq war. However, the allegations against the royal family were different. In the 1990s, members of the fundamentalist revival known as the Awakening (Arabic: *sahwa*) accused King Fahd of summoning infidels to liberate Kuwait. In the early 2000s, al-Qaeda jihadist sympathisers accused the Saudis of providing assistance to infidels from the West in their war against Iraq and Taliban-ruled Afghanistan, which gave refuge to Bin Laden and his followers. The illegitimacy of the Saud dynasty's rule and the need to drive the Americans out of the country were highlighted. Despite much effort and deference to the religious authorities, propagating Wahhabi ideology in the Muslim world, the Saudis thus had a hostile, radical opposition outside their state.

Just as Peshawar was a "mini-Arabistan" in the 1980s, Lebanon's Baalbek and Beqaa Valley became an outpost of Tehran. It was in this region that Hezbollah (Arabic: Hizb Allah – Party of God) was founded. The direct influence of the formation of this organisation came from the entry of Israeli troops into Lebanon on 6 June 1982 and the actions of the Iranian ambassador in Beirut – Ayatollah Ali Akbar Mohtashamipur. At his request, some 1500 soldiers of the Islamic Revolutionary Guard

Corps (Persian: Sepah-e Pasdaran-e Enqelab-e Eslami) were flown from Tehran to the Beqaa Valley with the task of training Lebanese Shia fighters. The main figures associated with the implementation of this venture were the well-known Shiite cleric Raghib Harb and the first Hezbollah leader Sobhi Tufayli. His deputy was Naim Qassem, who had previously been active in the Lebanese Resistance Troops (Arabic: Afwaj al-Muqawama al-Lubnaniyya, Amal). In addition to them, the core of Hezbollah consisted of a group of Shiite clerics, led by Sayyed Hassan Nasrallah. Hezbollah's armed wings were the Islamic Resistance (Arabic: Al-Muqawama al-Islamiyya) and the Islamic Jihad (Arabic: Al-Jihad al-Islami), which organised suicide attacks on Israeli, US and French military headquarters. These were the first such attacks in the Middle East. People living under Hezbollah's control were forced to endure social and legal restrictions and were subjected to ideological indoctrination, something hitherto alien to Lebanon. The author of the book captures the reader's attention with a description of the first eight years of Hezbollah's terrorist activities and the fate of its leaders.

Ghattas also interestingly describes the case of Salman Rushdie's book *The Satanic Verses*, which was much talked about at the time of the withdrawal of Soviet forces from Afghanistan in early 1989[8]. When the novel was published in September 1988, Ayatollah Khomeini raised no objection. Instead, it provoked heated protests in Britain. They were supported by Saudi Arabia and various Muslim organisations. Nevertheless, the book was translated into Persian and sold in Tehran. The situation changed when Saudi Arabia, as the guardian of Islam, directly joined the campaign against *The Satanic Verses*. With the help of its embassy in London, it organised a campaign to ban the dissemination of this novel and bring its author to justice. Khomeini could not remain passive in the face of the Kingdom's actions. He called not only for a ban on the sale of the book, but also for the killing of its author and any person involved in the publication of this work. He has set a 3 million US dollars reward for Rushdie's head. Saudi religious authorities, "defeated" by the Iranian

[8] The title of the book refers to the words encouraging the worship of the pagan goddesses Al-Lat, Manat and Al-Uzza, which Satan allegedly whispered to the Prophet Muhammad. The prophet was said to have stated that the place of these goddesses was with Allah. With this statement, Muhammad gained allies in the hostile tribe of the Quraysh, but he denied this narration a few days later. Its contents, however, were to be found in the original version of the 53rd surah of the Quran entitled *The Star* (Arabic: An-Najm).

fatwa, announced that the courts there should try Rushdie to convict in absentia for blasphemy. However, the author of *The Satanic Verses* did not stand trial and avoided death[9]. However, the translators of his novels into Japanese and Turkish and the publisher of the Norwegian translation were murdered. The race to religious intolerance between Saudi Arabia and Iran is just one of the themes of Ghattas book. She writes: *Death by blasphemy had now been introduced to the Muslim world by a strange twist in the competition between Iran and Saudi Arabia to position themselves as the standard-bearer of global Islam* (p. 256). Since then, people accused of blasphemy began to be killed in many Muslim countries. Muslim radicals usually carried out executions in the streets.

Part III of the book consists of seven chapters and covers the period 2003–2019, and is devoted to events and the fate of the people in the countries that were the subject of the previous chapters, and additionally Syria and Turkey. In the last part of the publication, the author has interestingly portrayed the subsequent course of the Saudi-Iranian ideological-religious rivalry and struggle for power in the Middle East as well as the seizure of control by Muslim extremists in Syria and Yemen. This struggle has largely evolved into proxy wars between Riyadh and Tehran.

In the first chapter, on Iraq, Ghattas went back to the 1990s, in which Saddam Hussein's regime bloodily cracked down on Shiites and exterminated their religious leaders. The entry of US troops into the country in 2003 raised hopes of positive social change. However, the opposite happened. Iraqi soldiers discharged from the army by the Americans, as well as officials of the former regime, formed the secret grouping The Return (Arabic: Al-Awda). The majority of Sunnis felt that the banning of the Iraqi Baath (English: renaissance or resurrection)[10] party and the demobilisation and dismissal of its members from public institutions were unjust. Moreover, these actions were perceived as a blow to all Sunni adherents, not just those who belonged to Baath. Excluded from public life, unemployed party members began to organise themselves into insurgent groups, fighting the Americans and acting against Iraqi Shiites. During Saddam Hussein's rule they were persecuted, but after his overthrow they

[9] In August 2022, a Muslim radical attacked Salman Rushdie with a knife. The incident occurred during an author meeting in the town of Chautauqua near Buffalo, New York. As a result of his injuries, the writer lost sight in one eye and power in his left hand.

[10] The party's name is an acronym for Hizb al-Baas al-Arabi al-Ishtiraki (Arab Socialist Baath Party).

began to dominate political life, as they outnumbered the population (they made up 60%). The disillusioned, especially the former military men, quickly joined the anti-American resistance movement. The mistakes that were made[11] at the time triggered a wave of violence and led to a Sunni uprising and bloody fighting between the Shiite Mahdi Army (Arabic: Jaysh al-Mahdi) and the Sunnis, led by members of the organisation Supporters of Islam (Arabic: Ansar al-Islam). In the first few years after the invasion, Saudis accounted for almost half of the foreign fighters taking part in the insurgency, and Saudi jihadists carried out more suicide attacks than Islamic volunteers from any other country. Ghattas writes: *The Saudis had warned the Americans not to invade, telling them it served no one's interests and would cause a resurgence of fundamentalism that would reach the United States and Europe. They warned about the destruction of Iraq, but what they really worried about was a Shia-ruled Iraq where Iran called the shots. A Sunni insurgency was the deadly antidote* (p. 326–327).

The Islamic State, which turned out to be the largest, richest and most murderous terrorist organisation in the world, emerged from organisations then linked to al-Qaeda. It gained followers and created affiliates in many Muslim countries. Even then, Saudi Arabia did not stop supporting the spread of Wahhabi extremism. Its victim in Pakistan was Salmaan Taseer, governor of Punjab province, who was assassinated by his own bodyguard in January 2011. The killer could not accept that the politician defied the blasphemy law and stood up for the Christian woman Asia Bibi accused of the offence. The murderer was sentenced to death and hanged in 2016. He was declared a martyr and a mosque built in his honour in a suburb of Islamabad gathers thousands of worshippers. Ghattas states: *Since the end of the war against the Soviets in Afghanistan, Saudi influence in Pakistan had become less obvious but perhaps more insidious. Saudi intelligence officials didn't need to fly to Peshawar twice a month anymore with bags of cash, as they had done in the 1980s. Their network of influence was well established, with both formal and informal networks* (p. 357).

The author of the book took too cursory an approach to the situation in Syria. She blamed Iran for its problems, just as she blamed Saudi Arabia for the rise of the Islamic State. Meanwhile, the causes

[11] Paul Bremer, the US civilian administrator of Iraq, concentrated all power in the country and disbanded the Iraqi army, leaving a multitude of men unemployed. This was one of the sources of the insurgency. By delaying the Iraqis taking charge of the country, Bremer contributed to the recognition of the Americans as occupiers rather than liberators.

of the outbreak of civil war in Syria in 2011 were more complex, with the regime in Damascus playing a major role. The United States, which sent large quantities of arms there and supported the rebels, had a significant impact on the course of the war in Syria, which the author failed to mention. Turkey's involvement in the Syrian conflict was also passed over in silence. Moreover, the book lacked commentary on Libya. Ghattas mentions the country only marginally, in relation to the various figures she describes who spent some time there. However, during the Arab Spring in 2011, there was an anti-government rebellion in Libya. It was supported by NATO aviation, contrary to the UN Security Council's decision to allow only air zones, not aerial bombing and support for the rebels. Furthermore, the author did not write about the attack on the US consulate in Benghazi carried out on 11 September 2012 by Islamist extremists linked to al-Qaeda. The American ambassador Chris Stevens and four other people were killed at the time. The Arab Spring in Egypt, on the other hand, was interestingly described. It led to the fall of President Hosni Mubarak and the election of Mohammad Morsi, a Muslim Brotherhood figure, to the post in 2012. Mohammad Morsi, who came from the Muslim Brotherhood, was elected to office in 2012. The changes in Egypt were watched with great concern by the Saudis, as the political success of the Muslim Brotherhood in that country could have inspired a coup in Saudi Arabia. However, after a year in office, the "troublesome" president was overthrown by the military.

Sofana Dahlan, a Saudi lawyer and one of the author's interviewees, said she wanted to believe (...) *that Mohammad bin Salman was the hero that her generation had long been waiting for* (p. 434). Young Salman, also known as MbS[12], became defence minister after his father, King Salman, took the throne in 2015, and soon afterwards also the heir to the throne exercising real power in the country. He lifted the ban on women driving and freed up many professions for them. He ordered the reopening of cinemas and concert halls and launched a propaganda attack on the Kingdom's religious conservatism, which won him the applause of young Saudis. His statements and actions attracted worldwide media attention. Ghattas writes: *When he declared that the 1979 era was over, he was right in one respect: religion was no longer enough to motivate society and mobilise the masses* (p. 440). Behind this

[12] MbS i san acronym created from the name of the prince, in which the word "ibn" has been replaced by "bin". Both words mean "son" in Arabic.

pose of reformer, however, was a cruel tyrant, intolerant of opposition and criticism. Hence the kidnappings and arrests of opponents of the Saudi regime, including the high-profile death of the aforementioned journalist Jamal Khashoggi. The author devoted the final chapter, entitled *Murder on the Bosporus*, to him. Khashoggi was murdered on 2 October 2018 at his country's consulate in Istambul, and his corpse was quartered. The journalist's life and death may provide an epilogue to the book in relation to Saudi Arabia and the assassin's perception of it – from his early support for the Afghan Mujahideen to his later, fateful realisation that the successor to the throne's reforms were designed to keep the Saud dynasty in power. In 2019, five of Khashoggi's killers were sentenced to death by a Riyadh court. However, their principals and those who oversaw the journalist's murder were never brought to justice. Among them was Prince Salman and his right-hand man for menial jobs – Saud al-Qahtani. After a period of diplomatic isolation for the Kingdom, and even after the publication of a report by the United Nations High Commissioner for Human Rights acknowledging Saudi Arabia's responsibility for the "extrajudicial premeditated execution" of Khashoggi, things returned to normal, and the West was ready to join in the implementation of the "Vision 2030" project announced by MbS in April 2016.

In summary, Iran and Saudi Arabia have for 40 years used religion as a weapon to consolidate the state, exercise internal control over society and discredit the opposition. At the same time, they have provided support to the authorities of other countries and NGOs to promote a militant religious ideology. One would have to wonder, however, whether the Black Wave could have been created without the opportunistic exploitation of the Arab-Israeli conflict by the Ayatollah Khomeini or Osama bin Laden. However, the author did not pay much attention to Israel.

The book by Kim Ghattas can be a fascinating read both for academics and professionals who devote their time to analysing the situation in the Middle East, as well as for those who are simply interested in the region and want to understand the complexity of the issues that affect it. In her conclusion, the author states: *I wrote it for those who believe the Arab and Muslim worlds are more than the unceasing headlines about terrorism, ISIS, or the IRGC. Perhaps above all I wrote it for those of my generation and younger in the region who are still asking, "What happened to us?" and who wonder why their parents didn't, or couldn't, do anything to stop the unraveling.* As well as seeking answer to this question, readers of *Black wave*... will find in

the book of Ghattas explanations of the origins of many conflicts in that part of the world and poignant descriptions of the hopes and desires of the people who live there. It reads like a good novel. I strongly encourage to read it.

Krzysztof Izak

Retired officer of the Internal Security Agency, who served, inter alia, in divisions carrying out tasks in the field of counteracting terrorist threats. Author of more than 20 articles on terrorism, which were published in many scientific journals. Creator of *Lexicon of Islamist organisations and movements* published by the ABW.

Contact: lizior3@wp.pl

Terrorism – Studies, Analyses, Prevention, 2025, no. 7: 481–487

https://doi.org/10.4467/27204383TER.25.040.21817

Review

Waldemar Zubrzycki, Jarosław Cymerski
Terrorism and its financing methods[1]

Jakub Grelewicz
Independent author
https://orcid.org/0009-0006-8659-1690

Oliwia Łubowska
Independent author
https://orcid.org/0009-0006-8659-1690

A thorough analysis and interpretation of the occurrence of terrorism in the modern world, the threats involved and the methods of financing it, help to understand the essence of the problem and to develop effective strategies to counter this phenomenon.

Professor Waldemar Zubrzycki and Jarosław Cymerski, PhD have joined forces to produce a comprehensive study on terrorism and its financing. The first author is a retired

[1] J. Cymerski, W. Zubrzycki, *Terroryzm i sposoby jego finansowania* (Eng. Terrorism and its financing methods), Szczytno 2022, Wydawnictwo Wyższej Szkoły Policji w Szczytnie, 185 p.

policeman, Representative of the Commander-in-Chief of the Police for the establishment of the Bureau of Anti-Terrorist Operations and a practitioner with extensive experience in the Ministry of Internal Affairs and Administration. The second author is a graduate of the Police Academy in Szczytno and National Defence Academy in Warsaw, a specialist in political science, for 28 years an officer – first of the Government Protection Bureau and now of the State Protection Service. Their competences and professional achievements allow them to be called experts in the field of terrorism research. The book entitled *Terrorism and its financing methods* is a characterisation of contemporary terrorism, a detailed analysis of the functioning of the terrorist organisations and their financing methods. The publication was reviewed by Prof. Bernard Wiśniewski, PhD, and Aleksander Babiński, PhD, which further emphasises its value. The publisher of the book is the Publishing House of the Police Academy in Szczytno.

The book consists of an introduction, four parts divided into chapters with their summary, a conclusion and a bibliography, which form a coherent and logical structure. The first part characterises the various aspects of contemporary terrorism. The authors discuss its origins and point out the difficulties in defining such risks. In the second part, they focus on selected elements of the functioning of the terrorist organisations, including categories of expenditure, propaganda activities, methods of members' recruitment and training. The third part examines the financing of terrorist organisations' activities, including legal and illegal sources of revenue. The fourth part of the book illustrates these issues by presenting examples of fundraising by selected terrorist organisations.

In the first part, *Characteristics of the phenomenon of contemporary terrorism*, the authors meticulously analyse the issue. They divide the sources of contemporary terrorism into political, social and religious. They report their observations in a way that helps the reader to understand the complexity of motivations behind terrorist actions. Another element of this part of the book is the chapter on the definition of the concept of terrorism. The authors cite and compare the interpretations of various researchers and describe how the term has evolved over the decades. They also discuss the definitions proposed by international organisations and show the differences in the approach to this type of act. They refer to the definitions of the European Commission and selected special services around the world, which allows the perspectives of different institutions

to be compared. They note the difficulty of clearly defining the phenomenon and its complexity. They consider the possibility of defining terrorism in terms of the methods of the attackers, which in turn emphasises the technical and tactical aspects of their activity. They draw attention to the social dimension of terrorism by analysing its impact on society and the individual. They then present a typology of terrorism through the prism of the methods of action and the motivations of the perpetrators, e.g. political or religious. After summarising these considerations, they move on to the chapter on how terrorists operate. They introduce the reader to the subject of raising funds for terrorist activities and indicate the various methods of financing. They describe in detail the forms of attacks with firearms and melee weapons, with explosives, with aircraft and with hostage-taking. They also discuss the use of weapons of mass destruction and unmanned mobile platforms in operations, emphasising the innovative and adaptive methods used by terrorist organisations. Cyber-attacks and simultaneous attacks, which are a growing challenge for modern security systems, are not overlooked. The authors then report on a selection of terrorist attacks. They begin with the 2002 attack carried out in Bali and go on to describe attacks using false information. They pay a particular attention to the attacks in France, Belgium and Germany, which have shocked global public opinion. They examine in detail the Paris attacks of 13 November 2015, which were among the largest terrorist attacks in modern Europe. They left 130 people dead and more than 350 injured. The authors then discuss the coordinated bomb attacks in Brussels on 22 March 2016 – two at Zaventem Airport and one at Maelbeek metro station, in which 35 people were killed, including the three bombers, and some 340 injured – and the attack at a Christmas market in Berlin on 19 December 2016, during which a truck driver drove into a crowd killing 12 people and injuring dozens more. Finally, they describe the attack in London on 7 July 2005, when three explosions on the underground and one in a city bus killed more than 50 people, injured several hundred, and paralysed the city centre during the morning rush hours. The examples given are intended to illustrate the variety of forms and methods of perpetrators.

The second part of the book, entitled *Selected elements of the operation of terrorist organisations*, begins with an analysis of the expenditure categories of terrorist organisations. The authors detail areas such as: operations, propaganda, recruitment, training, remuneration and compensations for members, social welfare, area management and administration.

This division helps the reader to understand how complex and elaborate structures for terrorist financing are, which in turn demonstrates the professionalism of terrorists and the ability to manage resources effectively. The researchers then focus on the propaganda activities carried out by terrorist groups, citing many examples in the process. They show how important a role propaganda plays not only in spreading ideology, but also in recruiting new members and building the organisation's image internationally.

An important issue in this part of the book is gaining supporters. The authors describe selected methods of recruitment and highlight the variety of methods used by terrorist organisations. They discuss passive recruitment, prison recruitment and the costs associated with this process. They note how important the recruitment of new members is to the continuity and growth of the organisation, and how manipulation and ideology are used to attract sympathisers. They also describe selected elements of the training of members of terrorist organisations, and attribute a particular role in this process to psychological manipulation. They show how, through indoctrination and psychological influence, the attitudes and beliefs of future terrorists are shaped. They present the characteristics of a well-trained professional, ability to operate in extreme conditions, high mental resilience and high level of physical and tactical preparation. In the conclusion, the authors draw attention to the complexity and professionalism of the activities of terrorist organisations. Through this analysis, the reader can better understand the mechanisms of functioning of these groups and the challenges their activities pose to security services and international society in the context of counter-terrorism.

The third part of the book is entitled *Financing the activities of terrorist organisations*. The authors begin by defining the concept of terrorist financing, citing terms proposed by the World Bank and the International Monetary Fund. Next, the international dimension of the fight against this phenomenon and the position of the United Nations towards terrorist financing are presented. The authors also look at the regulation of Polish law and how Poland fits into these global efforts. They assess the effectiveness of Polish regulations in countering financial flows to terrorist organisations. In the following chapters, they focus on various methods of fundraising by terrorist organisations. The use of non-profit organisations, that are often a front for illicit financial activities, is discussed. They explore the issue

of support given to terrorist organisations by their sympathisers, while highlighting the role of ideology and propaganda in resource mobilisation. Business entities are another important element in the financing of terrorist organisations. The authors show how legitimate businesses can be used to money laundering and transferring funds. They go on to detail illegal sources of revenue for terrorists. Among these are activities such as: drug production and trafficking, smuggling and trafficking of goods, including diamonds and human trafficking. Extortion, kidnapping and petty crime – also discussed in the book – are important sources of funding for many organisations. The authors highlight the use of banking institutions to transfer and conceal funds, while emphasising the need for increased control and regulation of the financial sector. They also analyse the role of modern technology, such as the internet, in facilitating the flow of funds and communication between members of terrorist organisations. Other methods of fundraising by terrorists discussed include art trafficking, tax fraud and exploitation of natural resources. The authors also describe the involvement of selected countries in terrorist financing. They begin with Iran discussing its alleged support for various terrorist groups. They then focus on Sudan and Syria outlining the complex relationship these countries have with terrorist organisations and the impact of international policy on this relationship. In the conclusion, they highlight the complexity of the problem of terrorist financing and the need for international cooperation to effectively counter this phenomenon.

In the final part of the book, entitled *Examples of fundraising by selected terrorist organisations*, the authors present the results of their research on three aspects of the functioning of selected terrorist organisations: the financial strategy along with the means of financing, the recruitment of members and the training system. These aspects are discussed in relation to Al-Qaeda, Boko Haram, Hezbollah and Islamic State (ISIS). They indicate similarities and differences in the functioning of these organisations in the context of fundraising and new members.

The book under review is a comprehensive study of terrorism and its financing methods. The authors have used their extensive professional and practical experience to provide an in-depth study of the issue, which is topical and highly relevant to global security. The work is characterised by a logical and coherent structure, which facilitates the reader's understanding of the complexity of the issues discussed. Each topic is carefully developed, including both theoretical aspects and illustrative examples. Particularly

valuable are the descriptions of specific terrorist organisations, such as Al-Qaeda or ISIS, which allow a better understanding of their mechanisms of operation and methods of fundraising. The book's assets also include the rich analysis of the various definitions of terrorism and the indication of the difficulties involved in defining the phenomenon unambiguously. The authors emphasise that the problem stems from the evolution of terrorism itself and variety of terrorist forms and methods.

The publication is a valuable item on the market of specialist literature due to the features that distinguish it from other valuable, both domestic and foreign, approaches to the problem of terrorism, such as: the monograph by Tomasz R. Aleksandrowicz, PhD *Terroryzm międzynarodowy* (Eng. International Terrorism) (2011), the scientific article *Terroryzm i jego finansowanie w kontekście nowelizacji art. 165a k.k.* (Eng. Terrorism and its financing in the context of the amendment of Article 165a of the Criminal Code) by Anna Golonka, PhD (2020) or the English-language monograph by Magnus Ranstorp, PhD *Terrorism and Human Rights* (2008). The uniqueness of the reviewed position is influenced by factors such as:

1) embedding of the analysis of terrorist financing in the realities of the functioning of the Polish security services, made possible by the authors' extensive professional experience in operational work and comprehensive theoretical knowledge;
2) comprehensive analysis of the issue, covering its three essential elements necessary to the functioning of terrorist organisations, i.e. funding models, membership acquisition patterns and training procedures;
3) addressing the problem of financing the phenomenon in the context of the Polish legal and institutional system, while taking into account global conditions, providing unique practical conclusions relevant to the police-military community and other security policy researchers.

Terrorism and its financing methods is a publication worth recommending. It is a valuable source of information for students, security professionals and representatives of various scientific disciplines interested in terrorism. Waldemar Zubrzycki and Jarosław Cymerski present complex issues in a comprehensive yet accessible way, which makes it possible for the book to reach a wider audience. The publication is an important contribution to the discourse on terrorism and provides a solid basis for further research in this field. It provides the reader with

a fuller picture of the threats posed by terrorism, the challenges faced by the international community in combating this phenomenon and the tools that can be used to do so.

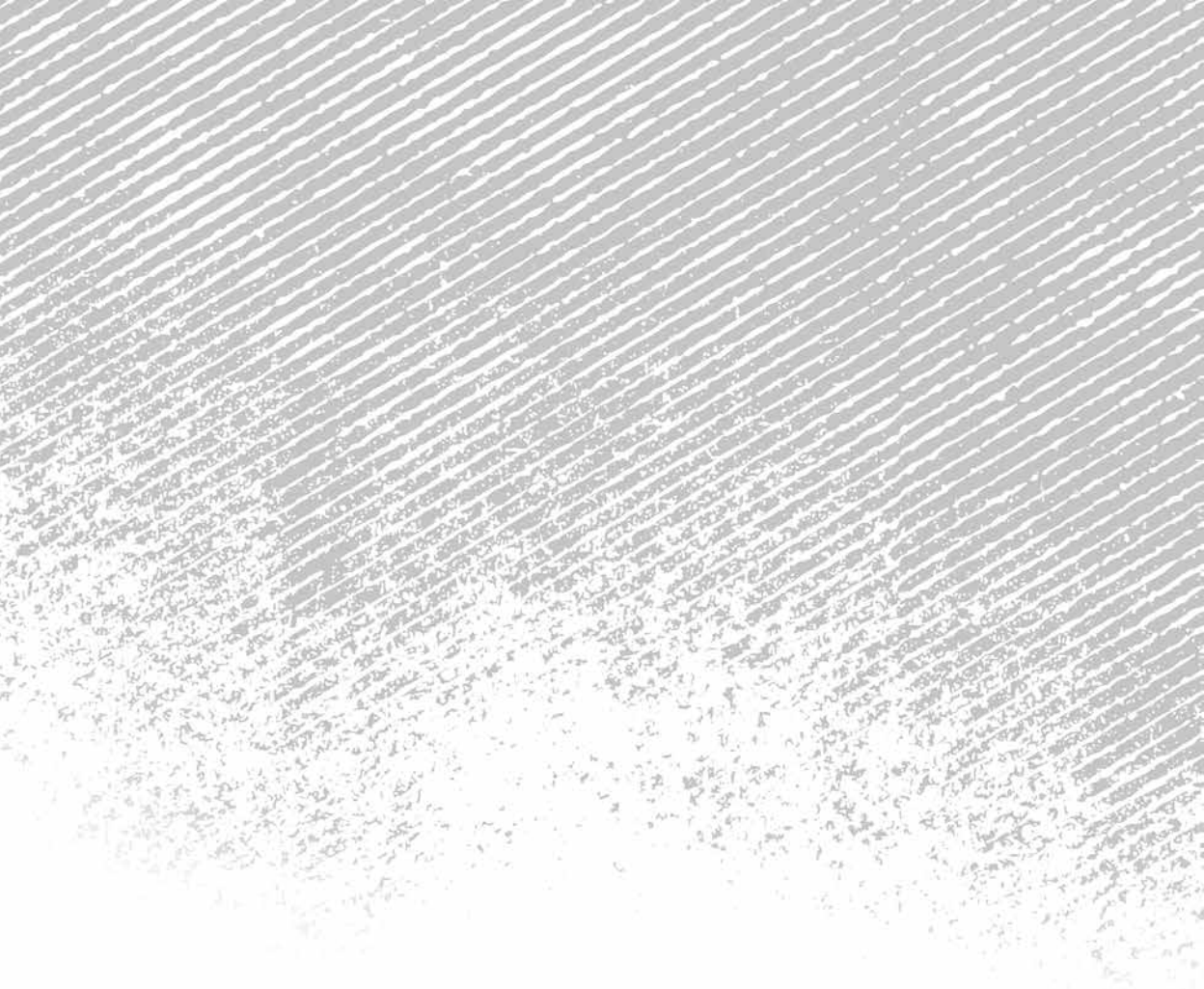
Jakub Grelewicz

Graduated with a Bachelor's degree from the Faculty of Political Science and Security Studies at the Nicolaus Copernicus University in Toruń. He is currently studying at the Faculty of Political Science and Administration at Kazimierz Wielki University in Bydgoszcz. He is interested in issues related to Poland's internal security, the functioning of the armed forces and national defence.

Contact: kubagrelewicz@wp.pl

Oliwia Łubowska

Graduate of the Faculty of Philology, University of Łódź. Her research interests focus on internal security, international relations and conflict challenges.



AWARDED THESES

Terrorism – Studies, Analyses, Prevention, 2025, no. 7: 491–507

https://doi.org/10.4467/27204383TER.25.041.21818

Article

The attacks of 11 September 2001 and legal and administrative changes in US security policy[1]

Franciszek Dziadkowiec-Wędlikowski

Independent author

https://orcid.org/0009-0008-0115-4702

Abstract

This article discusses the implications of terrorist attacks of 11 September 2001 for US security policy. The event triggered a number of significant legal and administrative changes that revolutionised the US approach to counter-terrorism. Major reforms, such as the introduction of *The USA PATRIOT Act of 2001*, establishment of the Department of Homeland Security and the tightening of air safety regulations, were aimed at increasing the effectiveness of prevention and responding more quickly to potential threats. While these changes have brought significant benefits, they have also raised controversy over violations of civil rights. The analysis of the reforms shows the evolution of security policy and points to the challenges facing the contemporary counter-terrorism system.

Keywords

the attacks of 11 September 2001, *The USA PATRIOT Act of 2001*, US security policy, aviation security, administrative reforms, legal reforms, Department of Homeland Security, terrorist attacks

[1] The article is based on a BA thesis entitled *Targeted killings as part of the CIA's strategy in the context of the September 11, 2001 terrorist attacks* defended at the Faculty of International and Political Studies, Jagiellonian University. The thesis was awarded in the 13th edition of the competition of the Head of the ABW for the best doctoral, master's or bachelor's thesis concerning state security in the context of intelligence, terrorist, economic threats.

Introduction

The terrorist attacks of 11 September 2001 in the United States proved to be a turning point in security policy for both that country and most countries in the wider West. The experience of terrorism has triggered the introduction of fundamental changes in US security policy and system and has influenced the formation of new counter-terrorism strategies and approaches around the world. Following the attacks of 9/11, US President George W. Bush delivered an address to the American people, which he began with the words: *Today, our fellow citizens, our way of life, our very freedom came under attack in a series of deliberate and deadly terrorist acts*[2]. The attacks on the World Trade Center (WTC), in which nearly 3000 people were killed, have gone down as some of the most tragic in US history. Three of the four hijacked planes reached their targets – the machine operating flight 11 hit the north tower of the WTC at 8.46am, the one performing flight 175 hit the south tower at 9.03am and the one performing flight 77 hit the Pentagon building at 9.37am. The aircraft performing flight 93 missed its target in Washington DC and crashed in the fields of Pennsylvania shortly after 10am. The number of casualties even surpassed the tragic toll of the Japanese attack on Pearl Harbor in 1941[3].

The aim of the article is to present the administrative and legal changes that were made after the attacks on the WTC. The paper discusses the motives of the perpetrators of the attacks and the legal and institutional changes that resulted from these events, primarily on the basis of *The USA PATRIOT Act of 2001*. Analysing these events and their impact is important for understanding the evolution of the security policy in the United States and for countries to better prepare for security challenges.

Motives of the perpetrators of the 11 September 2001 attacks

The terrorist attacks on the WTC and the Pentagon were carried out by members of Al-Qaeda, a terrorist organisation run by Osama bin Laden

[2] See: *WATCH: President George W. Bush's address to the nation after September 11, 2001 attacks*, YouTube, 19 VIII 2021, https://www.youtube.com/watch?v=WA8-KEnfWbQ [accessed: 30 III 2023].

[3] In the attacks of 11 IX 2001, 2,977 people were killed; in the attack on Pearl Harbor, 2,403 on the US side. See: *14 Interesting Pearl Harbor Facts*, Pearl Harbor Tours, https://www.pearlharbortours.com/pearl-harbor/facts-about-pearl-harbor [accessed: 25 I 2025].

and ideologically linked to Islamic fundamentalism. The reasons for the attack were extensively discussed in the November 2002 *Letter to America* written by the organisation's leader himself[4]. In the manifesto, he stressed that the attack was the result of assassinations on Muslims in many regions of the world, most notably US military interventions in Arab countries, the Israeli-Palestinian conflict, the second war in Chechnya or India's support for discrimination against Muslims in Kashmir. In addition, he expressed his opposition to the American way of life, which deviates significantly from the principles set out by Muhammad, separating religion from government, and to homosexuality, the use of women in advertising and product sales, lobbying or the Western financial system. He very clearly manifested his hatred of Jews and the state of Israel as well as the support given to it by the United States. He also stated that if the American people are free and have the ability to choose their power, they are complicit in the actions of the government. This is how Bin Laden justified his organisation's attack on civilian targets[5].

In addition to the direct motives expressed in the manifesto, it is also possible to find those communicated indirectly, referring to the doctrine, which resounded in the subsequent statements of Bin Laden and members of Al-Qaeda. Michael Scott Doran pointed out that: *When a terrorist kills, the goal is not murder itself, but something else – for example, police crackdown that will create a rift between government and society, that the terrorist can then exploit for revolutionary purposes. Osama bin Laden sought and received international military crackdown, one he wants to exploit for his particular brand of revolution*[6]. Bin Laden intended to draw the US into the fight against the Islamic world, and the actions of Al-Qaeda, according to him, were to be the catalyst for the revolution he wanted to bring about. Doran further stated that: *Bin Laden produced a piece of high political theater he hoped would reach the audience that concerned him the most: the umma*[7] *or universal Islamic community. The script was obvious: America, cast as the villain, was supposed to use its military might like a cartoon character trying to kill a fly with a shotgun. The media would see to it that any use of force against the civilian population*

[4] O. bin Laden, *Letter to America*, https://web.archive.org/web/20040615081002/http://observer.guardian.co.uk/worldview/story/0,11581,845725,00.html [accessed: 26 I 2025].

[5] Ibid.

[6] M.S. Doran, *Somebody Else's Civil War*, "Foreign Affairs" 2002, vol. 81, no. 1, pp. 22–23.

[7] *Umma* – Arabic word meaning community, nation, Muslim community.

of Afghanistan was broadcast around the world, and the umma would find it shocking how Americans nonchalantly caused Muslims to suffer and die[8]. The response of the United States to the events of 9/11 was therefore to reveal to the Muslim population the true face of America, and consequently to reconcile this community in a common struggle against American atrocities. Doran goes on to refer to the polarisation that would emerge between the Muslim community and the wider Western world (i.e. NATO and European Union countries in particular), allied to the United States. It would lead to the achievement of Bin Laden's main objective: an Islamic revolution in Muslim countries, which would at the same time ensure that the extremist strain of Islam could survive and thrive[9].

According to Daniel Benjamin and Steven Simon the attacks of 11 September 2001 were exclusively religiously motivated: *The hijackings were the performance of a sacrament, one intended to restore to the universe a moral order that had been corrupted by the enemies of Islam and their Muslim collaborators*[10]. The response to the attacks in the form of expressions of support for Islam by the American government, led by President Bush, was, in Benjamin and Simon's view, the right decision, showing the followers of Islam that America is opposed not to them, but to the murder of innocent people[11].

The aftermath of the attacks of 11 September 2001

During President Bush's speech, words were spoken that proved to be the prelude to a change in US policy and the beginning of the conflict we now know as the Global War on Terror – the US response to the attack by Al-Qaeda: *We will make no distinction between the terrorists who committed these acts and those who harbor them*[12]. Just one week after the attacks, the US Congress introduced a resolution titled *Joint Resolution to authorize the use of United States Armed Forces against those responsible for the recent attacks launched against the United States*. The resolution – abbreviated as

[8] M.S. Doran, *Somebody Else's Civil War*..., p. 23.

[9] Ibid., p. 41.

[10] D. Benjamin, S. Simon, *The Age of Sacred Terror*, New York 2002, p. 40.

[11] Ibid.

[12] See: *WATCH: President George W. Bush's address to the nation*...

The Authorization for Use of Military Force[13] – allowed the President to use all necessary force against the perpetrators of the 9/11 attacks, those who planned them, those who helped carry them out and those who sheltered these individuals[14].

Less than a month after the attacks, on 7 October 2001, the US, with the support of the UK, launched "Operation Enduring Freedom", targeting the Taliban in power in Afghanistan and Al-Qaeda hideouts deployed on Afghan territory. Its main objectives were to capture or kill top Al-Qaeda leaders, destroy terrorist-owned infrastructure on Afghan territory and remove the Taliban from power[15]. In addition to the successful air strikes carried out by US and British forces, the early phase of the war also relied on the use of US special forces to assist the Pashtuns and the Northern Alliance in their fight against the Taliban. The first US conventional land forces arrived on the ground 12 days later[16].

The investigation launched into the attacks, which was given the code name PENTTBOMB[17], was the largest in the FBI's history to date. It involved more than 4000 officers and 3000 employees. Just three days after the fateful events, the identities of all 19 suspects involved in the attack were established. On 27 September, their photographs were made public. Investigators quickly linked the men to Al-Qaeda and gained access to intelligence gathered on them[18].

Legal and administrative changes

The terrorist attacks of 11 September 2001 triggered a heated debate on the need to adapt the law to the new terrorist threats. As a result of these discussions and intensive legislative work, new laws and regulations were

[13] *Authorization for Use of Military Force*, https://www.govinfo.gov/content/pkg/PLAW-107publ40/pdf/PLAW-107publ40.pdf [accessed: 30 III 2023].

[14] Ibid.

[15] I.H. Daalder, J.M. Lindsay, *The Bush Revolution: The Remaking of America's Foreign Policy*, April 2003, https://www.brookings.edu/wp-content/uploads/2016/06/20030425.pdf, p. 20 [accessed: 25 I 2025].

[16] *1999 – 2021 The U.S. War in Afghanistan*, Council on Foreign Relations, https://www.cfr.org/timeline/us-war-afghanistan [accessed: 30 III 2023].

[17] The abbreviation PENTTBOMB stands for Pentagon/Twin Towers Bombing Investigation.

[18] *A Review of the FBI's Handling of Intelligence Information Prior to the September 11 Attacks*, https://oig.justice.gov/sites/default/files/archive/special/0506/chapter5.htm [accessed: 10 VI 2023].

introduced to strengthen security measures and expand the powers of law enforcement agencies and special services to make counter-terrorism more effective[19].

The next section of the article discusses the Patriot Act, which introduced the expansion of the powers of government agencies to monitor and combat terrorism, and the establishment of the Department of Homeland Security. Changes to aviation security measures were also mentioned.

The USA PATRIOT Act of 2001

The foundation of legal changes is the passed on 26 October 2001, *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, abbreviated as The USA PATRIOT Act of 2001 (hereinafter: Patriot Act)[20]. The Act introduced changes to the competences of national intelligence services and law enforcement agencies[21]. It focused on four key issues:

- expanding the possibilities of surveillance by law enforcement agencies, including wiretapping,
- facilitating communication between the various services so that they can use available resources to combat terrorism,
- updating the law to take account of new technologies and new threats,
- making penalties for offences of a terrorist nature more severe, while at the same time increasing the range of acts which qualify as such offences[22].

Title I of the act describes the creation of an anti-terrorism fund and gives the US Attorney General the authority to request the Department of Defense to ask for assistance from the military in the event of the illegal use of weapons of mass destruction on US territory. In addition, the Director of the United States Secret Service was directed to create the National Electronic Crime Task Force – a nationwide task

[19] L. Fisher, *Presidential War Power*, Lawrence 2004, p. 202.

[20] *The USA PATRIOT Act of 2001*, https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf [accessed: 30 III 2023].

[21] S. Wojciechowski, P. Osiewicz, *Zrozumieć współczesny terroryzm* (Eng. Understanding contemporary terrorism), Warszawa 2017, p. 129.

[22] *The USA PATRIOT Act: Preserving Life and Liberty*, Department of Justice, https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf [accessed: 30 III 2023].

force to prevent, detect and investigate cyber crimes, particularly terrorist attacks on critical infrastructure[23]. It also condemned the discrimination and aggression against Muslims living in the United States that occurred after the 11 September attacks. The most important provision of this title appears to be Section 106, which provided the President with the ability to confiscate assets belonging to foreign individuals and organisations suspected of terrorist activities. Furthermore, where confiscation is undertaken on the basis of classified sources of information, the suspect person or organisation may not be informed of the confiscation[24].

From the point of view of the intelligence services, one of the most important parts is Title II. It deals with the surveillance of persons suspected of terrorism, involvement in computer fraud or abuse, and spies working for foreign powers who are engaged in clandestine activities on US territory. Government agencies are allowed to collect information through foreign intelligence information from both US citizens and foreign nationals[25].

Previous law allowed senior FBI officers to seek a court order, in connection with an investigation, to gain access to records of carriers, hotels, warehouses or vehicle rental companies. Section 215 amended these provisions. Applications can now be made by FBI officers of a lower rank – *assistant special agent-in-charge* (i.e. those in charge of FBI field offices). In addition, court orders began to cover any items in the possession of anyone – any company or individual. The items sought need not, as before, be related to an identified spy or foreign state, but may only be sought as part of an investigation to protect the United States from international terrorism or clandestine intelligence activities, provided that such an investigation is not only conducted on the First Amendment to the US Constitution, but also has other bases[26].

[23] *ECTF and FCTF*, United State Secret Service, https://www.secretservice.gov/contact/ectf-fctf [accessed: 30 III 2023].

[24] *The USA PATRIOT Act of 2001*..., pp. 6–8.

[25] Ibid., pp. 8–25.

[26] Ibid., p. 17. The first amendment refers to the inviolability of freedom of expression. "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances". See: *Constitution of the United States*. The author of the article used the translation by Andrzej Pułło *Konstytucja Stanów Zjednoczonych Ameryki* (Eng. Constitution of the United States), Warszawa 2002.

Section 218 changed the requirements (previously set by *The Foreign Intelligence Surveillance Act of 1978*, FISA) that the intelligence services had to meet in order to undertake surveillance of a person. The existing "the purpose" of surveillance in the form of foreign intelligence gathering was changed to "a significant purpose". Surveillance could be carried out when the collection of foreign intelligence information was only a partial (relevant) objective and the main objective was another offence. This gave the services the ability to surveillance a much larger proportion of the citizenry, with the provision invoked that the collection of foreign intelligence need not be the main, but only an essential, purpose of that surveillance[27]. Title II also includes provisions on trade sanctions against the Taliban and restrictions on the export of agricultural goods, medicines and medical devices[28].

Title III of the act is divided into three subsections. The first deals with the strengthening of banking regulations, particularly in the area of anti-money laundering and terrorist financing. The second discusses communication between law enforcement and financial institutions. The last section of the title is dedicated to currency smuggling and counterfeiting. The purpose of the changes introduced, as indicated by the legislator, was (...) *to increase the strength of the United States measures to prevent, detect, and prosecute international money laundering and the financing of terrorism*[29].

Title IV introduced many changes on *Immigration and Nationality Act of 1965*. It provided more investigative and enforcement powers to the US Attorney General and the Immigration and Naturalization Service (INS). This title was also divided into three subsections. The first subsection deals with the protecting of the country's northern border – the limit on the maximum number of personnel at the border was removed, and resources (both financial and infrastructure) were prepared to triple the number of Border Patrol personnel, Customs Service personnel and INS inspectors. It also gave the INS and the State Department access to the National Crime Information Center files maintained by the FBI. The second subsection strengthens immigration laws. Of particular importance in this part

[27] S.H. Rackow, *How the USA Patriot Act Will Permit Governmental Infringement upon the Privacy of Americans in the Name of „Intelligence" Investigations*, „University of Pennsylvania Law Review" 2002, vol. 150, no. 5, pp. 1676–1677. https://doi.org/10.2307/3312949.

[28] *The USA PATRIOT Act of 2001*..., p. 21.

[29] Ibid., p. 27.

is Section 412, which allows for the detention of persons who pose a threat to the United States (due to links to terrorist groups or support for terrorist activities) for an indefinite period of time (with the need for renewal every six months). The third subsection in turn was devoted to the families of those affected by the 9/11 attacks. Attention was drawn to the fact that some of the victims or their families were immigrants and documents confirming the legality of their stay in the United States may have expired shortly after the attack. For these individuals, it was decided to make an exception and extend the time needed to submit the relevant documents to the office[30].

Title V of the Patriot Act increased the upper limit on rewards that can be paid by the state for assistance in apprehending terrorists. It also reaffirmed the ability of federal intelligence services to cooperate with other law enforcement agencies and expanded powers of the Unites States Secret Service over fraud and other criminal activities targeting federally insured financial institutions.

Section 505 amended three acts: *The Electronic Communications Privacy Act of 1986, The Right to Financial Privacy Act of 1978* and *The Fair Credit Reporting Act of 1970* and authorised third parties to disclose for intelligence purposes, upon written request by the FBI, confidential transaction records, financial reports and credit information[31]. Prior to this legal change, the FBI was required to ensure that the information sought related to a foreign state, a foreign intelligence officer, an international terrorist or a person engaged in covert intelligence activities. After the amendment, the FBI only has to ensure that the data to be released is relevant to an investigation aimed at preventing international terrorism or to covert intelligence activities. This creates a serious risk of abuse by the FBI[32].

Title VI provides assistance to families of officers injured in terrorist attacks (including increasing payments to families of victims from the previous USD 100 000 to USD 250 000). The provisions of *The Victims of Crime Act of 1984* were amended[33].

[30] Ibid., pp. 72–93.

[31] S.H. Rackow, *How the USA Patriot Act...*, p. 1689.

[32] *The USA PATRIOT Act of 2001...*, pp. 93–98.

[33] Ibid., p. 99.

Title VII discusses the issue of changes concerning the exchange of information between government agencies, aimed at improving communication of law enforcement agencies at different levels (federal, state and local) in the event of terrorist attacks[34]. The changes introduced were intended to streamline the work and exchange of information in the case of investigations conducted under the supervision of several authorities simultaneously[35].

Another very important title of the law is Title VIII. Section 801 fills in the loopholes regarding attacks on means of public transport. The previous provisions of the law did not include penalties for attacks directed at means of public transport. Section 802, in turn, completed the definition of domestic terrorism, according to which it is defined (...) *as those criminal acts dangerous to human life, committed primarily within the United States, that appear to be intended to intimidate or coerce a civilian population, or to influence a governmental policy by intimidation or coercion, or to affect the conduct of a government by mass destruction, assassination or kidnaping*[36]. Section 803 introduced, already announced on 11 September, a prohibition against harboring terrorists under penalty of imprisonment or fine. Subsequent sections (804 and 805) added, respectively, amendments related to the extraterritoriality of the legislation (including attacks on embassies, consulates and military bases) and a prohibition on providing material support to terrorists. Under Section 806 addressing the issue of assets belonging to terrorists and terrorist organisations, all such assets, whether within the United States or abroad, are subject to forfeiture. This provision is intended to exclude one of the main sources of funding for terrorist acts. The next major section of Title VIII is Section 808, which amends the definition of a federal crime of terrorism. Several less serious offences, such as assault or destruction of property, have been removed from the definition, while more serious offences, such as attacks on aircraft and airports, the use of biological and chemical weapons, and the assassination and kidnapping of members of the US Congress, Cabinet or Supreme Court judges, have been included. Section 809 introduced the absence of a statute of limitations for terrorism offences. Under Sections

[34] Ibid., p. 104.

[35] Ibid.

[36] Ch. Doyle, *Terrorism: Section by Section Analysis of the USA PATRIOT Act*, https://www.arl.org/wp-content/uploads/2001/12/patriot-act-analysis-2001.pdf, pp. 50–55 [accessed: 30 III 2023].

810 and 811, the penalties for committing or assisting in the commission of terrorist acts were significantly increased. For example, the maximum penalty for causing damage to a nuclear power plant, if there were no fatalities in the attack, increased from 10 to 20 years' imprisonment. Subsequent sections have, among other things, authorised post-release surveillance of those accused of terrorism, increased penalties for the offence of cyber-terrorism and increased funding for the development of national cyber-security, as well as tightened legislation on biological weapons (introducing, among other things, penalties of up to 10 years' imprisonment for the possession of biological agents or toxins[37] which possession cannot be justified by peaceful intent)[38].

The amendments contained in Title IX were intended to streamline intelligence operations, particularly in relation to the collection of foreign intelligence information. The Director of the Central Intelligence Agency (CIA), under Section 901, was given responsibility for establishing requirements and priorities for foreign intelligence information to be collected under FISA and for assisting the Attorney General in disseminating intelligence information. However, the Patriot Act limited the powers of the CIA Director. He no longer had the ability to undertake, based on FISA, electronic surveillance or physical search operations, or to direct and manage them, unless authorised by statute or presidential executive order[39]. Section 902 supplemented the definition of foreign

[37] In accordance with the United States Code, the term "biological agent" means "any microorganism (including, among others, bacteria, viruses, fungi or protozoa), or infectious substance, or any naturally occurring, bioengineered or synthesized component of any such microorganism or infectious substance, capable of causing: (A) death, disease, or other biological malfunction in a human, an animal, a plant, or another living organism; (B) deterioration of food, water, equipment, supplies, or material of any kind; or (C) deleterious alteration of the environment". The term "toxin" means "the toxic material or product of plants, animals, microorganisms (including, among others, bacteria, viruses, fungi or protozoa), or infectious substances, or a recombinant or synthesized molecule, whatever their origin and method of production, and includes: (A) any poisonous substance or biological product that may be engineered as a result of biotechnology produced by a living organism; or (B) any poisonous isomer or biological product, homolog, or derivative of such a substance". Quoted after: https://www.govinfo.gov/content/pkg/USCODE-2023-title18/pdf/USCODE-2023-title18.pdf [accessed: 20 II 2024] – editor's note.

[38] *The USA PATRIOT Act of 2001*..., pp. 104–116.

[39] A. Siegler, *The Patriot Act's Erosion of Constitutional Rights*, "Litigation" 2006, vol. 32, no. 2, pp. 18–21.

intelligence information to include information on international terrorist activities. Section 903 required members of the intelligence community to make every effort to acquire information about terrorists and terrorist organisations. Section 904 allowed the intelligence community to defer until 1 February 2002 the submission of required intelligence reports to Congress. Section 905 directed the Attorney General, in consultation with the Director of the CIA, to develop, within no more than 180 days of the Act's enactment, guidelines for the dissemination to the intelligence community of foreign intelligence information disclosed in the course of a criminal investigation. These guidelines were to allow the American intelligence community to report on actions taken or planned based on information that agaencies of the intelligence community provided to the US Department of Justice. The guidelines may have contained exceptions where there was a threat to an ongoing investigation. Section 907 required the Director of the CIA to report, in consultation with the Director of the FBI, the establishment of a the National Virtual Translation Center (which took place in February 2003) to ensure timely and accurate foreign intelligence translations. Section 908 authorised the necessary resources for the training of government officials who do not normally deal with foreign intelligence matters, and state and local government officials who may encounter members of foreign intelligence during a terrorist attack. The training would help officials identify foreign intelligence information and utilise it in the course of duties[40].

Amendments, which could not be allocated to the earlier titles, are contained in the last – Title X. For example, under Section 1006, foreign nationals who have engaged in money laundering cannot enter the United States. Section 1009 provides USD 250 000 to the FBI to investigate the possibility of providing airlines with computerised access to the names of federal government terrorism suspects, and Section 1014 provides money to individual states to purchase equipment and training for emergency services (police, fire and ambulance)[41].

The introduction of such broad changes to the legislation was accompanied by much controversy. Opponents of the act argued that it had been passed for opportunistic reasons, with the idea that it would not be widely debated in light of 9/11 and would pass quickly through

[40] *The USA PATRIOT Act of 2001*..., pp. 117–121.

[41] Ibid., pp. 121–132.

the legislative process. In addition, it was argued that Section 215 violates the Fourth Amendment of the Constitution[42], Section 505 violates both the First and Fourth Amendments[43]. In the case of Section 215, opponents saw blatant interference with the inviolability of property. This included searches by the services without a warrant of the suspect's residence or workplace, as well as wiretapping or obtaining information without the suspect's knowledge. Section 505 further alleged violations of freedom of expression. Section 412, which allows persons who pose a threat to the state to be detained indefinitely without charge, was also controversial[44].

Much of Title II of the Patriot Act was initially set to expire on the last day of 2005, in accordance with the *sunset clause* written into the Act, a pre-scheduled expiry date of the legislation that occurs automatically unless an extension is voted on. Such a vote occurred in March 2006. President Bush signed it and kept most of the key elements of the title unchanged. Under Barack Obama, an extension of the act was also voted down (in 2012), and in 2015, the USA FREEDOM Act upheld most of the provisions of the expiring Patriot Act apart from Section 215, which was intended to prevent the National Security Agency from collecting information en masse from the mobile phones of Americans suspected of terrorist activity.

US Department of Homeland Security

In response to the 9/11 attacks, President Bush announced the creation of the Office of Homeland Security to coordinate homeland security efforts. On 25 November 2002, the U.S. Department of Homeland Security (DHS) was established under The Homeland Security Act of 2002 to consolidate US executive bodies related to homeland security[45]. On 1 March 2003, 22 agencies united under one department with a common mission to protect the American people, the most diverse mix of federal function

[42] The fourth amendment refers to the inviolability of persons and property. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized". See: *Constitution of the United States*.

[43] *Myths and Realities About the Patriot Act*, ACLU, 22 I 2005, https://www.aclu.org/other/myths-and-realities-about-patriot-act [accessed: 31 V 2023].

[44] Ibid.

[45] *The Homeland Security Act of 2002*, https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf [accessed: 31 V 2023].

and duties[46]. The mission of DHS, the youngest, third-largest department, includes, among others: preventing terrorism, law enforcement, ensuring land and maritime border and transport security, conducting immigration policy, crisis management, ensuring cyber security. The establishment of DHS marked a change in the American way of thinking about threats. The introduction of the term "homeland" into both the legal system and the nomenclature of the services was an expression of the rulers' focus on protecting the population not only from emergencies caused by natural factors, such as natural disasters, but also from diffuse threats from individuals or organisations[47].

Aviation security

The events of 11 September had a huge impact on civil aviation security. This included significant restrictions on the objects that can be brought on board aircraft (including a ban on knives, which were used during the Al-Qaeda attacks), a ban on access to the cockpit (more security has been introduced to make it more difficult for outsiders to enter), for which pilots underwent additional training. The changes also included improvements to security at the airports themselves[48]. After the 9/11 attacks, the Transportation Security Administration was created, and the budget as well as the number of posts in the Federal Air Marshal Service – federal air police – have been significantly increased[49].

Summary

The changes introduced after the attacks on the WTC have had far-reaching consequences in both US domestic politics and international relations. The expansion of the secret service's powers, new air security regulations

[46] *Creation of the Department of Homeland Security*, Homeland Security, https://www.dhs.gov/creation-department-homeland-security [accessed: 12 V 2023]; S. Wojciechowski, P. Osiewicz, *Zrozumieć współczesny terroryzm*..., p. 104.

[47] E. Alterman, M. Green, *The Book on Bush: How George W. (Mis)leads America*, New York 2004, p. 244.

[48] *Bezpieczeństwo i ochrona lotnictwa cywilnego* (Eng. Safety and security of civil aviation), A.K. Siadkowski, A. Tomasik (eds.), Poznań 2012, pp. 152–154.

[49] A.K. Siadkowski, *Bezpieczeństwo i ochrona w cywilnej komunikacji lotniczej na przykładzie Polski, Stanów Zjednoczonych i Izraela* (Eng. Safety and security in civil air transport on the example of Poland, the United States and Israel), Szczytno 2013, pp. 296–302.

and establishment of DHS have all contributed to improving the US' ability to prevent and respond to terrorist threats. The adopted security policy has set new standards in the fight with terrorism[50]. Nevertheless, as mentioned, these changes have also been criticised by human rights defenders and international organisations, emphasising that the introduction of these measures has to some extent violated fundamental civil rights, such as the right to privacy and civil liberties[51]. Thus, it became necessary to strike a balance between effectiveness in combating threats and protecting democratic values.

Although the changes introduced have brought many benefits in terms of security, the author believes that their long-term effects on society and the political system require further analysis. Development in technology and the evolution of counter-terrorism methods are prompting new questions about ethics, the effectiveness of prevention efforts and compliance with the associated law. It is necessary to adapt measures to the dynamically changing nature of threats, while respecting citizens' rights and international legal standards. Otherwise, the fight against terrorism may lead to the undermining of the foundations it should protect.

Bibliography

Alterman E., Green M., *The Book on Bush: How George W. (Mis)leads America*, New York 2004.

Benjamin D., Simon S., *The Age of Sacred Terror*, New York 2002.

Bezpieczeństwo i ochrona lotnictwa cywilnego (Eng. Safety and security of civil aviation), A.K. Siadkowski, A. Tomasik (eds.), Poznań 2012.

Doran M.S., *Somebody Else's Civil War*, "Foreign Affairs" 2002, vol. 81, no. 1, pp. 22–42.

Fisher L., *Presidential War Power*, Lawrence 2004.

[50] *The Lessons Learned for U.S. National Security Policy in the 20 Years Since 9/11*, CAP, 10 IX 2021, https://www.americanprogress.org/article/lessons-learned-u-s-national-securitypolicy-20-years-since-911/ [accessed: 27 I 2025].

[51] M. Carlisle, *How 9/11 Radically Expanded the Power of the U.S. Government*, Time, 11 IX 2021, https://time.com/6096903/september-11-legal-history/ [accessed: 27 I 2025].

Konstytucja Stanów Zjednoczonych Ameryki (Eng. Constitution of the United States), A. Pułło (trans. and introd.), Warszawa 2002.

Rackow S.H., *How the USA Patriot Act Will Permit Governmental Infringement upon the Privacy of Americans in the Name of "Intelligence" Investigations*, "University of Pennsylvania Law Review" 2002, vol. 150, no. 5, pp. 1651–1696. https://doi.org/10.2307/3312949.

Siadkowski A.K., *Bezpieczeństwo i ochrona w cywilnej komunikacji lotniczej na przykładzie Polski, Stanów Zjednoczonych i Izraela* (Eng. Safety and security in civil air transport on the example of Poland, the United States and Israel), Szczytno 2013.

Siegler A., *The Patriot Act's Erosion of Constitutional Rights*, "Litigation" 2006, vol. 32, no. 2, pp. 18–24.

Wojciechowski S., Osiewicz P., *Zrozumieć współczesny terroryzm* (Eng. Understanding contemporary terrorism), Warszawa 2017.

Internet sources

14 Interesting Pearl Harbor Facts, Pearl Harbor Tours, https://www.pearlharbortours.com/pearl-harbor/facts-about-pearl-harbor [accessed: 25 I 2025].

1999 – 2021 The U.S. War in Afghanistan, Council on Foreign Relations, https://www.cfr.org/timeline/us-war-afghanistan [accessed: 30 III 2023].

A Review of the FBI's Handling of Intelligence Information Prior to the September 11 Attacks, https://oig.justice.gov/sites/default/files/archive/special/0506/chapter5.htm [accessed: 10 VI 2023].

Carlisle M., *How 9/11 Radically Expanded the Power of the U.S. Government*, Time, 11 IX 2021, https://time.com/6096903/september-11-legal-history/ [accessed: 27 I 2025].

Creation of the Department of Homeland Security, Homeland Security, https://www.dhs.gov/creation-department-homeland-security [accessed: 12 V 2023].

Daalder I.H., Lindsay James M., *The Bush Revolution: The Remaking of America's Foreign Policy*, April 2003, https://www.brookings.edu/wp-content/uploads/2016/06/20030425.pdf [accessed: 25 I 2025].

Doyle Ch., *Terrorism: Section by Section Analysis of the USA PATRIOT Act*, https://www.arl.org/wp-content/uploads/2001/12/patriot-act-analysis-2001.pdf [accessed: 30 III 2023].

ECTF and FCTF, United State Secret Service, https://www.secretservice.gov/contact/ectf-fctf [accessed: 30 III 2023].

Laden O. bin, *Letter to America*, https://web.archive.org/web/20040615081002/http://observer.guardian.co.uk/worldview/story/0,11581,845725,00.html [accessed: 26 I 2025].

Myths and Realities About the Patriot Act, ACLU, 22 I 2005, https://www.aclu.org/other/myths-and-realities-about-patriot-act [accessed: 31 V 2023].

The Lessons Learned for U.S. National Security Policy in the 20 Years Since 9/11, CAP, 10 IX 2021, https://www.americanprogress.org/article/lessons-learned-u-s-national-security-policy-20-years-since-911/ [accessed: 27 I 2025].

The USA PATRIOT Act: Preserving Life and Liberty, Department of Justice, https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf [accessed: 30 III 2023].

WATCH: President George W. Bush's address to the nation after September 11, 2001 attacks, YouTube, 19 VIII 2021, https://www.youtube.com/watch?v=WA8-KEnfWbQ [accessed: 30 III 2023].

Legal acts

The Authorization for Use of Military Force, https://www.govinfo.gov/content/pkg/PLAW-107publ40/pdf/PLAW-107publ40.pdf [accessed: 30 III 2023].

The Homeland Security Act of 2002, https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf [accessed: 31 V 2023].

The USA PATRIOT Act of 2001, https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf [accessed: 30 III 2023].

Franciszek Dziadkowiec-Wędlikowski

Student majoring in national security at the Jagiellonian University in Kraków. His research interests include the United States and the functioning of special services in Poland and around the world.

Contact: franciszek.dw@gmail.com

VARIA

Terrorism – Studies, Analyses, Prevention, 2025, no. 7: 511–533

https://doi.org/10.4467/27204383TER.25.042.21819

Varia

The security and safety sector in the light of new trends

Research conclusions

Adam Tatarowski

The Technical Property Protection Development Institute TECHOM

https://orcid.org/0009-0007-5503-6819

A cross-sectional study of the security and safety sector for property and persons was carried out on behalf of the Technical Property Protection Development Institute TECHOM (hereinafter: TECHOM) in August and September 2024. They resulted in the creation, by a team of researchers from MABEA sp. z o.o.: Anna Araminowicz, Piotr Klatta, Tomasz Radochoński i Magda Sierżyńska, of the first comprehensive report entitled *Protection and Security of Property and Persons – analysis of the sector. Survey report*, which takes into account the broad legal and normative context and the specificities of the sector. It is a free report intended for general use. Its first edition was published for internal use in October 2024[1]. The second edition, expanded to include the latest statistics, was published in March 2025 on the TECHOM website[2].

[1] A. Araminowicz, P. Klatta, T. Radochoński, M. Sierżyńska, *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania* (Eng. Protection and Security of Property and Persons – analysis of the sector. Survey report), Kraków 2024, MABEA sp. z o.o., https://www.mabea.pl/wp-content/uploads/2024/11/Ochrona-i-bezpieczenstwo-mienia-i-osob-analiza-sektora.Raport-z-badania2024_do-pobrania.pdf [accessed: 28 II 2025].

[2] A. Araminowicz, P. Klatta, T. Radochoński, M. Sierżyńska, *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania. Wydanie II zaktualizowane* (Eng. Protection

The research was inspired by information provided in July 2024 by the Polish Agency for Enterprise Development (PARP) about a competition to entrust the organisation and operation of sectoral competence councils – bodies defined in Article 4c(1) point 2 of the Act on the establishment of the Polish Agency for Enterprise Development[3]. Sectoral competence councils serve to build cooperation between public administration, educational institutions and business organisations and bring together representatives of these sectors. They play important role in the labour market by supporting adult education. A sectoral competence council has been set up, among others, in the security and safety of property and persons sector (name proposed by PARP).

The idea of setting up sectoral councils arose from the trend in the EU towards a unified understanding of competences and qualifications. Already the Lisbon Convention on the Recognition of Qualifications, as an international agreement under the auspices of UNESCO and the Council of Europe, has enabled the recognition of academic qualifications in Europe and beyond[4]. Mention should also be made of Directive 2005/36/WE[5], which deals with the recognition of professional qualifications within the EU and enables professionals to practise their profession or provide services abroad. This Directive formed the basis for the introduction in 2008 of the European Qualifications Framework (EQF), which was subsequently amended in 2017[6]. According to the Recommendation of the Council of Europe on promoting automatic mutual recognition of higher and upper secondary education and training qualifications and the outcomes of learning periods abroad, the EQF is supposed to promote transparency of national education and training systems and build mutual trust. Sectoral councils according

and Security of Property and Persons – analysis of the sector. Survey report. Second updated edition), Kraków 2025, MABEA sp. z o.o., https://www.techom.com/wp-content/uploads/2025/04/Raport_MABEA_TECHOM_2025.pdf [accessed: 21 V 2025].

[3] *Act of 9 November 2000 on the establishment of the Polish Agency for Enterprise Development* (consolidated text, Journal of Laws of 2025, item 98).

[4] *Convention on the Recognition of Qualifications concerning Higher Education in the European Region, drawn up in Lisbon on 11 April 1997* (Journal of Laws of 2004, no. 233, item 2339).

[5] *Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications* (Official Journal of the EU L 255/22 of 30 IX 2005).

[6] *Council Recommendation of 26 November 2018 on promoting automatic mutual recognition of higher education and upper secondary education and training qualifications and the outcomes of learning periods abroad* (Official Journal of the EU C 444/1 of 10 XII 2018).

to the Act on the Integrated Qualifications System[7] play a fundamental role in the supervision of the Polish Qualifications Framework (i.e. the Polish implementation of the EQF) for individual sectors.

The legal basis for the operation of sectoral councils is defined by:

1) Act of on the establishment of the Polish Agency for Enterprise Development,
2) Act on the Integrated Qualifications System,
3) Act – Education Law[8].

Moreover, in the draft amendment to the Act on crisis management[9], the sector competence council in the security and safety sector is indicated as the body issuing opinions on certificates or other documents requested by critical infrastructure (CI) operators when implementing organisational and technical solutions to ensure the security of the CI they manage and increase its resilience.

The competition application to organise and run a council in this sector, submitted by TECHOM in cooperation with the Polish Platform for Homeland Security, the Polish Association for National Security and the POLALARM National Association of Engineers and Technicians of Technical Security and Security Management (hereinafter: POLALARM), received a positive opinion from the President of PARP. This great accolade creates opportunities for action on many levels, facilitated by the specific location of sectoral competence councils in the private-public ecosystem.

The following is a synthetic presentation of the report, which takes into account a variety of data, including statistics.

Security and safety of property and persons sector – discussion of the survey results

Security and safety of property and persons sector plays a special role in ensuring the stability of the state and its importance is constantly growing in the face of new technological, regulatory and geopolitical challenges.

[7] *Act of 22 December 2015 on the Integrated Qualifications System* (Journal of Laws of 2024, item 1606).

[8] *Act of 15 December 2016 – Education Law* (consolidated text, Journal of Laws of 2024, item 737, as amended).

[9] Draft Act amending the Act on crisis management and certain other acts, https://legislacja.rcl.gov.pl/docs//2/12386961/13069020/13069024/dokument711601.pdf [accessed: 4 IV 2025].

Today's threats require new legislative and organisational solutions, more effective security methods and – above all – qualified personnel capable of countering both traditional and new forms of threats, including cybercrime or hybrid threats.

The authors of the report focused on three key aspects of the sector:

1. Structure and regulations – analysis of the legal and normative context, taking into account the specific characteristics of the sector.
2. Competency needs – identification of skill gaps in the workforce and recommendations for training and skills validation.
3. New challenges and technologies – discussion of geopolitical, legislative and technological trends that will shape the future of the sector.

The research carried out was aimed at comprehensively diagnosing the current situation in the sector, identifying of the most important problems and directions for development that will allow security services to be better adapted to contemporary realities.

Research methodology and scope of analysis

The research on the security and safety of property and persons sector was conducted in August and September 2024. The objectives of this research were:

- analysis of the socio-economic and institutional-legal environment of the security and safety of property and persons sector,
- analysis of the educational and training offer for the needs of the sector,
- analysis of trends influencing the labour market and competence needs in the sector,
- identification of competence needs in the sector,
- identification of challenges facing the sector in the context of actions aimed at ensuring personnel with competences adequate to the needs of the labour market in the sector[10].

The research included both existing data analysis, a qualitative study and a survey research.

[10] A. Araminowicz, P. Klatta, T. Radochoński, M. Sierżyńska, *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania* (Eng. Protection and Security of Property and Persons – analysis of the sector. Survey report), Kraków 2024..., p. 8.

As part of the analysis of the existing data, the following were taken into account:

- legal acts regulating activities in the sector,
- statistical data,
- reports and analyses concerning the sector,
- scientific articles,
- articles in printed and electronic media and press releases,
- information posted on the websites of entities (e.g. institutions regulating the sector, sector organisations, universities),
- information posted on sector portals[11].

The qualitative study was an important complement to the analysis of the existing data and allowed the specifics of the sector to be recognised. It was carried out in the form of two focus group interviews and an expert panel. A total of 29 people took part in the survey, including respected experts from public administration (market regulators), professional associations and chambers, universities, specialised continuing education institutions, as well as representatives of entrepreneurs, both those who operate in the sector (security agencies, companies designing and installing security systems) and those who procure security services (inter alia in the areas of CI, trade, logistics).

The questionnaire survey was conducted using the CAWI (Computer-Assisted Web Interview) method on a group of 46 respondents representing, among others, companies providing security services, principals and users of security services, professional organisations, educational institutions, public administration[12].

Based on the data collected, scenarios were drew up for the development of the sector, taking into account the impact of new regulations, technological developments and the changing needs of the labour market. The research methodology allowed for a multidimensional analysis of the sector and the integration of regulatory, business and educational perspectives.

Characteristics of the sector

The sector of security and safety of property and persons started to develop intensively in Poland after the political transformation in 1989. It very

[11] Ibid., p. 9.

[12] Ibid., p. 11.

quickly gained great importance in the free market economy. The first piece of legislation that made it possible to operate in the sector was the Act on economic activity[13]. It regulated the need to obtain a licence for services in the area of security of persons and property, as well as detective services. The foundation of the sector's operation is the Act on the protection of persons and property[14]. For almost a decade the sector functioned without proper regulation, which generated numerous legal ambiguities. Today, it is subject to a number of additional regulations, but a significant proportion of security services operate outside the legal framework, as there are no requirements for service providers operating outside the framework set by the Act on the protection of persons and property. This sector-specific phenomenon has practical implications for the entire security services market. It poses both strictly legislative and bottom-up challenges, resulting from dynamic market changes and growing expectations of security personnel. It requires them to adapt to new technologies and acquire specialised competences, including security management, performing complex tasks in risk-based structures or crisis management. In view of the growing role of CI protection, security agencies and other companies at the core of the sector have to meet increasingly demanding standards, which is not only a regulatory challenge, but also educational and competence verification challenge.

The definition of the sector for the purposes of the report – in accordance with PARP guidelines – was based on Polish Classification of Activities (PKD) codes. Selected subclasses are presented in the Table 1[15].

[13] *Act of 23 December 1988 on economic activity* (Journal of Laws of 1988, no. 41, item 324, as amended).

[14] *Act of 22 August 1997 on the protection of persons and property* (Journal of Laws of 2025, item 532).

[15] All tables and graphs in this article are taken from the publication: A. Araminowicz, P. Klatta, T. Radochoński, M. Sierżyńska, *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania*, Kraków 2024... (editor's note).

Table 1. Description of selected subclasses of the Polish Classification of Activities 2007.

Subclass	Subclass includes
74.90.Z – Other professional, scientific and technical activities not elsewhere classified	• business intermediation, i.e. organising procurement or sales for small and medium-sized businesses, excluding real estate intermediation, brokering the purchase or sale of patents, valuation activities, excluding real estate valuation and valuation for insurance companies (antiques, jewellery, etc.), inspection of transport documents, information on freight rates, weather forecasting activities, • **safety advisory services**, • activities of agronomists and agricultural economists, environmental consultancy, other technical consultancy, consultancy other than architectural or engineering consultancy and management consultancy, costing activities, activities of agents or agencies acting on behalf of individuals for the purpose of engaging in film, theatre and other artistic or sporting activities, publishing of books, musical recordings, play scripts, artistic works and photographs by publishers, producers, etc.
80.10.Z – Other professional, scientific and technical activities not elsewhere classified	• carrying out security and patrolling activities, security activities related to the transport of money, securities or other valuables, • security activities in armoured car transport, • personal protection service activities, • lie detector service activities, • fingerprinting and identification service activities, • other security activities, excluding the operation of security systems
80.20.Z – Security activities, excluding security systems service activities	• security activities relating to the operation and monitoring of electronic security systems, such as burglar or fire alarms, including their installation and maintenance, • installation, repair, conversion and adjustment of mechanical or electronic locking devices, safes and vaults in connection with subsequent monitoring. Units carrying out this activity may also sell the above equipment, i.e. electronic security systems, mechanical or electronic locking devices, safes and vaults
80.30.Z – Security systems service activities	• investigative and detective activities, • the activities of private investigators, irrespective of the type of client or the purpose of the investigation

The descriptions of PKDs correspond to the way the security system for CI is understood. Within the framework of the National Critical Infrastructure Protection Program (NPOIK), there is a so-called six-pack

describing the security system for CI. Measures taken to ensure security include:

1) providing physical security, including technical measures to support physical protection,
2) providing technical security, including fire protection,
3) providing personal security,
4) providing information and communication security,
5) providing legal security,
6) business continuity and recovery plans[16].

The structure of the sector is highly diversified. Micro, small and medium-sized companies providing physical security services dominate, but companies specialising in technical security systems are playing an increasingly important role (the use of new technologies based on artificial intelligence is also gaining popularity). Large security corporations, most of which are international in scope, are also important.

According to data from the REGON register (as at June 2024), there were 7595 entities registered in the sector, declaring their activities within the scope of PKD 80 division – Investigation and security activities[17]. Table 2 presents the number of these entities between 2015 and 2024, by the number of people employed in the entity.

Table 2. Number of entities in 2015–2024 declaring to conduct investigation and security activities, by number of employees (based on data from REGON register).

As at	0–9	10–49	50–249	250+	total
31.12.2015	4 822	734	288	112	5 956
31.12.2016	5 259	732	275	116	6 382
31.12.2017	5 482	741	265	115	6 603
31.12.2018	5 546	697	247	113	6 603

[16] *National Critical Infrastructure Protection Program*, Government Centre for Security (RCB), 2023. The text of the program is available at: https://www.gov.pl/web/rcb/narodowyprogram-ochrony-infrastruktury-krytycznej.

[17] A. Araminowicz, P. Klatta, T. Radochoński, M. Sierżyńska, *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania*, Kraków 2024..., p. 51.

As at	0–9	10–49	50–249	250+	total
31.12.2019	5 656	663	247	112	6 678
31.12.2020	5 913	637	240	112	6 902
31.12.2021	6 173	620	234	109	7 136
31.12.2022	6 410	606	228	107	7 351
31.12.2023	6 529	583	228	105	7 445
30.06.2024	6 690	578	223	104	7 595

Chart 1 shows the distribution of entities declaring to carry out investigation and security activities, taking into account the subclasses of the PKD 80 division.

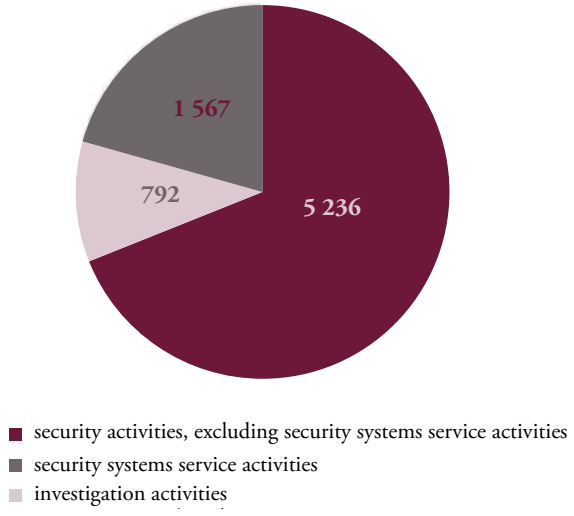


Chart 1. Number of entities declaring activities in the security and safety sector in 2024, by subclass of PKD 80 division (based on data from the REGON register).

According to data from Statistics Poland (GUS) on employment within the PKD 80 division, the sector employs 117 743 employees (as at 31 March

2024)[18]. A decline in employment in the sector between 2021–2024 is evident (Chart 2). This may be a consequence of the COVID-19 pandemic, the full-scale Russian invasion on Ukraine, as well as new trends expressed in the shift away from direct physical protection to technical security.

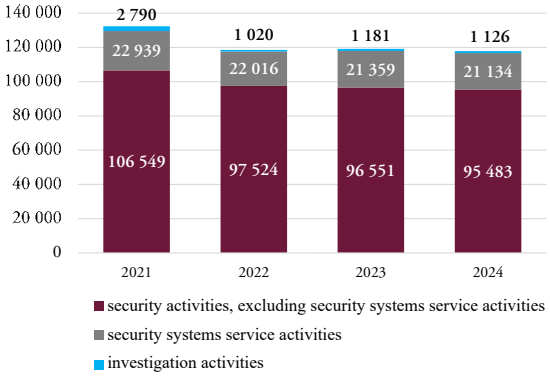


Chart 2. Number of people employed in the security and safety sector in 2021–2024, including a division into subclasses of PKD 80 division (based on Statistics Poland data).

The value of the market for the protection and security of property and persons in 2023 was estimated at approx. PLN 16 billion, the largest part of which – more than PLN 11,7 billion – was made up of revenue from security activities, excluding the operation of security systems (PKD 80.10.Z division)[19].

Entitlements and qualifications

Much of professional activity in the security and safety of property and persons sector is subject to outdated regulations that are out of step with modern realities and are largely concessionary in nature – in practice omitting the competence acquisition stage. They also do not take into account the real validation of competences.

[18] Ibid., p. 59.

[19] Ibid., p. 46.

The basic legal act that regulates this subject is the Act on the protection of persons and property. The issue of admission to the possession of weapons is in turn regulated by the Act on weapons and ammunition[20].

Table 3 presents the number of persons enrolled on the lists of qualified sector employees between 2015 and 2023, who are qualified in accordance with the Act on the protection of persons and property.

Table 3. Number of people on the lists of qualified sector personnel between 2015 and 2023 (based on the Police HQ data).

State at the day	List of persons on the list of qualified physical security officers	List of persons on the list of qualified technical security personnel
31.12.2015	90 059	17 405
31.12.2016	91 230	18 066
31.12.2017	92 943	18 633
31.12.2018	95 238	19 212
31.12.2019	95 413	19 644
31.12.2020	99 235	20 137
31.12.2021	103 323	20 801
31.12.2022	108 261	21 338
31.12.2023	112 459	22 039

A very good example showing the obsolescence of the mentioned regulations in the context of the acquisition and validation of competences and/or qualifications is the way of obtaining entry into the list of qualified technical security personnel described in Article 27 of the Act on the protection of persons and property. Apart from the formal conditions (age, medical examination, Police opinion) there are practically no requirements in terms of competences/qualifications. It is sufficient if the person concerned, in accordance with Article 27(2) point 4, (...) *has at least a vocational technical education with a specialisation in electronics, electricity, communications, mechanics, information technology or has completed a course for a technical*

[20] *Act of 21 May 1999 on weapons and ammunition* (consolidated text, Journal of Laws of 2024, item 485).

security officer or has been apprenticed to the aforementioned professions under the provisions of the Act of 22 March 1989 on crafts (Journal of Laws of 2020, item 2159). There are no other provisions at the statutory level that clarify this. A person who obtains such an entry shall be entitled to:

- perform the activities referred to in Art. 3 point 2 of the Act on the protection of persons and property, i.e.:
  a) *installation of electronic devices and alarm systems signalling threats to protected persons and property, as well as operation, maintenance and repair in the places where they are installed,*
  b) *installation of mechanical security devices and means, as well as their operation, maintenance, repair and emergency opening in places where they are installed;*
- carry out the activities referred to in Article 27(4) of the mentioned Act, i.e.:

1) *development of a protection plan to the extent specified in Art. 3 point 2,*
2) *organising and managing teams of technical security personnel.*

The activities referred to in the mentioned Article 3 point 2 of the Act on the protection of persons and property do not include the design of security systems – a de facto unregulated aspect. Any person, even one who has no professional training – given the current statutory provisions – can carry out the design of technical security systems.

The approach to the formulation of competence and qualification requirements for service providers carrying out the activities of design, installation and maintenance of technical security systems[21] is also regulated by military normative requirements, but their impact on the overall market is limited. These regulations do not have sufficient force to translate them into uniform requirements in the civilian sector. Similarly, Annex 1 of the 2023 NPOIK[22] only mentions the means of acquiring and validating competence in this field. The document stresses the relevance of delivering technical security officer courses in a specialised continuing education institution operating within the educational system, and refers to the PN-EN 16763 standard *Services for fire safety systems and security systems*. However,

[21] *Instruction on the protection of military facilities and escorted property – DU-3.14.3(A) (Szt. Gen. 1705/2023)* – (classified document).

[22] *Standards for ensuring the proper functioning of critical infrastructure – best practices and recommendations*, Annex 1 to the National Critical Infrastructure Protection Program, Government Centre for Security (RCB), 2023. The text of the Annex is available at: https://www.gov.pl/web/rcb-en/national-critical-infrastructure-protection-program.

it should be emphasised that the NPOIK only serves as a recommendation, and in Polish tender practice the most important criterion for the selection of service providers is the lowest price. As a result, the competence and qualifications of contractors are often overlooked unless they are explicitly defined in the law. According to the authors of the report:

> (...) the powers set out in the Act on the protection of persons and property apply to two groups of persons – physical protection employees and technical security employees. However, representatives of the sector draw attention to the need to take into account the contemporary understanding of the processes involved in providing safety and security and to adapt the provisions concerning the competences of employees to the current organisational solutions and technologies used.
>
> They also emphasise the need to revise and clarify the rules on the authorisations required to carry out activities in the provision of security and the protection of persons and property in terms of how the various authorisations are obtained. The rules should, on the one hand, ensure reliable verification of the requirements laid down by the rules and, on the other hand, not unduly restrict access and ensure an inflow of workers with the necessary authorisations into the sector.
>
> An analysis of the issues related to the entitlements of practitioners could also be one of the important elements in the discussion related to the identification of typical professional processes and tasks in the sector. This would clarify the scope of the sector and identify points of contact with other sectors (e.g. with the health sector for activities falling within the field of emergency response activities).
>
> In view of the ongoing changes in the range of activities carried out in the sector, it is also important to discuss the identification among them of those the performance of which requires the possession of competences defined by law. With regard to the others, formal confirmation of possession of competences useful for their performance could be voluntary and constitute good practice. Solutions available under the Integrated Qualifications System, in the form of free market or sectoral qualifications, could be used for this. It would be worth considering collaboration between representatives of different stakeholder groups to monitor the sector's needs in this regard, so that entitlements and qualifications in the sector constitute a coherent and transparent system[23].

[23] A. Araminowicz, P. Klatta, T. Radochoński, M. Sierżyńska, *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania,* Kraków 2024..., p. 82.

Education for the sector

The report analyses in detail the sector's education system, formal and non-formal education, and identifies key skills gaps and market needs.

Formal education refers to both vocational education and higher education. Vocational education includes preparation for work in the sector in occupations such as personal and property security technician and occupational health and safety technician. Community colleges offering these courses operate throughout the country and the skills of graduates are confirmed by professional examinations in the qualifications BPO.02 (Protection of persons and property) and BPO.01 (Management of safety in the working environment).

Vocational examinations have varying pass rates. For example, in the summer session of 2023, 62.70% of candidates passed the whole examination for the BPO.02 qualification (of whom 469 people took the written part, passing 90.62%, and 516 people took the practical part, passing 63.37%)[24]. In the BPO.01 qualification the result was lower and amounted to 40.03% (2087 candidates took the written part and passed 91.42%, 2794 candidates took the practical part and passed 37.62%)[25]. The data indicate clear difficulties in passing the practical part of the examinations, which may suggest insufficient preparation of graduates for real professional challenges.

Higher education in the area of security includes such majors as national security, internal security, criminology or administration and internal security. Universities offer a large choice of specialisations, but academic diplomas are not sufficient to obtain entry to the list of qualified physical security officers – they only confirm theoretical preparation. Universities for the uniformed services also play an important role in the sector, preparing, among others, future state officers.

In addition to formal education, courses and training are an important part of training in the security sector. These include:

- courses giving the basis for entry into the list of qualified physical security officers, including theoretical and practical preparation in the field of shooting, intervention techniques and law;
- courses for technical security officer (there are no precise requirements in the Act on the protection of persons and property concerning their scope and standards);

[24] Ibid., p. 86.

[25] Ibid., p. 87.

– obligatory training courses for qualified physical security officers – every 5 years, amounting to 40 hours.

According to representatives of the sector, the system of courses imposed by the Act on the protection of persons and property is not fulfilling its role and should be changed. There is a lack of standardisation in terms of training programmes, ways of validating competences. In addition, appropriate requirements should be placed on training establishments. Moreover, representatives of the sector stated that some courses do not provide real skills and their participants treat them only as a formality aimed at obtaining the relevant certificate. For example, courses organised by continuing education establishments operating within the structures of security agencies – in the author's opinion, are difficult, in such a case, to provide reliable training and validation of competences. Due to increasing labour costs, companies are investing less and less in the development of their employees, which leads to a decrease in the quality of security services.

The results of the survey show that the sector needs more practical and tailored training for today's threats, covering technology as well as legal aspects and security management. Without systemic changes and a proper focus on quality control of courses and training institutions, the sector may have an increasing problem with qualified staff, which will affect the quality and effectiveness of the security services provided.

Trends affecting the sector

The security and safety of property and persons sector faces a number of challenges due to the rapidly changing socio-political, technological and economic environment. These include:

– outflow of Ukrainian security personnel and increased demand for the protection of strategic facilities related to Russia's full-scale invasion of Ukraine;
– strengthening of security management and upgrading of sector personnel competencies resulting from hybrid warfare involving cyber attacks, CI sabotage and disinformation activities;
– changing working patterns after the COVID-19 pandemic – return to stationary and hybrid working, translating into an increase in demand for office and retail security;
– climate change forcing the adaptation of security procedures and technology to extreme weather conditions and natural disasters;

- technological advances transforming the industry through automation, the use of artificial intelligence, unmanned systems and modern surveillance tools, changing the requirements for security personnel;
- implementation of the CER Directive[26] forcing an increase in the standards of CI protection, leading to the need for certification of services, people and organisational and technical solutions;
- rising operating costs, including an increase in the minimum wage. This is causing security agencies to reduce the number of physical security personnel and direct the business towards the implementation of technical security systems;
- reducing physical security in some sectors due to the high level of security in Poland (one of the highest in Europe), the increase in shop crime, however, indicates the need to rethink security strategies;
- sustainability and green transformation, which are forcing the industry to comply with ESG (Environmental, Social and Corporate Governance) standards, which includes optimising energy consumption, ecological approach to equipment and reporting on environmental performance.

All these factors will shape the security sector in the coming years. In addition, they require flexibility and innovative approaches to security management.

Competence needs

The results of the analysis of existing data, trends and qualitative and quantitative research have identified the main competency areas needed to provide quality services in the security and safety sector. These include knowledge and skills in:

1. Security management.
   Effective security management requires the ability to plan, analyse threats, assess risks and integrate physical protection with technical security systems and cyber security aspects. Knowledge of modern security management methods, effective

[26] *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* (Official Journal of the EU L 333/164 of 27.12.2022).

crisis communication and the ability to manage dynamic and unpredictable threats are essential.

2. Technological advances.
   The growing role of technology in the sector requires competence in the operation and implementation of advanced security systems, including solutions based on artificial intelligence, automation, with the inclusion of modern surveillance tools. The developing unmanned and anti-drone systems are also an important element. It is relevant that both technical specialists and physical security personnel are able to use modern solutions effectively.
3. Evolution of current threats and the emergence of new ones.
   The changing geopolitical situation, the development of hybrid warfare, terrorist threats and extreme weather events make it necessary to constantly update knowledge on potential threats. Workers in the sector should be able to identify and analyse new threats and implement effective prevention and response strategies.
4. Performance of physical security tasks, including knowledge of procedures and practical skills.
   Physical security personnel must be able to: apply self-defence techniques, use weapons, interact in teams, recognise and neutralise threats. It is also important to adapt operational procedures to changing threats and to provide an appropriate level of training for individuals with varying work experience.
5. Knowledge of the law and the ability to apply it.
   Legislative changes require sector staff to update their knowledge of regulations. Knowledge of the law is essential for the proper performance of their duties, in particular with regard to interventions, the protection of CI and the application of security procedures in accordance with applicable standards or norms.
6. Green transformation and the need to align operations with environmental regulation.
   Sustainability and ESG regulations are forcing companies in the sector to implement green solutions such as optimising energy consumption, reducing their carbon footprint and managing resources responsibility. Employees in the sector should have knowledge of environmental regulations and the ability to implement them in their daily operations.

Interdisciplinarity is becoming a key requirement in the sector, meaning that employees need to combine knowledge of management, law, technology, cyber security and other areas. Increasing the competence of those responsible for procuring security services is equally important, as the ability to formulate requirements and procurement specifications has a huge impact on the quality of services in the industry. One participant in the qualitative study stated that (...) *security has become strongly interdisciplinary. The boundary of how far security experts in different scientific disciplines should go is blurring*[27].

Respondents who took part in the survey were asked to rate each area of competence on a scale of 1 (not very important) to 5 (crucial). The relevance rating is the arithmetic average of the answers given. The most relevant competence area, according to survey participants, is knowledge and skills related to the evolution of current threats and the emergence of new threats. Areas such as security management or knowledge of physical protection procedures and practical skills also received high relevance ratings. Competences related to green transformation are the least relevant according to respondents, which may be due to low awareness of the impact of ESG regulations on the sector (Chart 3).

Chart 3. Assessment of competence relevance.

In the next question, respondents were asked to rate the degree of competence shortage on a scale from 1 (not lacking) to 5 (very lacking).

[27] A. Araminowicz, P. Klatta, T. Radochoński, M. Sierżyńska, *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania*, Kraków 2024..., p. 132.

Evaluation of the degree is the arithmetic average of the answers given. The greatest shortage of competencies is found in areas related to the evolution of threats and the emergence of new threats, competences related to technological progress and competences related to technological security management (Chart 4).

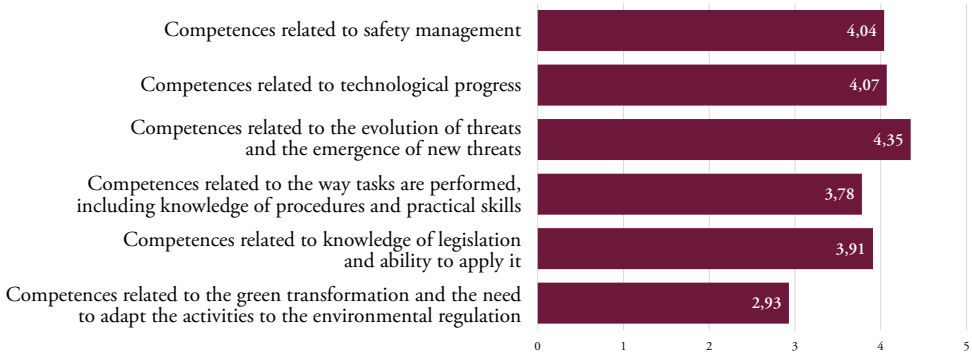


Chart 4. Assessment of the degree of competence gap.

The research carried out confirms that the development of competences in the security and safety of property and persons sector is essential, especially in the context of dynamic technological changes, the evolution of threats and new legal regulations. Particularly important areas requiring training support are competences related to the evolution of threats and the emergence of new threats, to technological advances, and to security management. Competency gaps in these areas pose a major challenge and affect the efficiency and effectiveness of security systems.

The research further indicates that the greatest shortfalls relate to the ability to analyse and counter new threats, including cyber attacks, disinformation and acts of sabotage. Upgrading skills to integrate physical protection with technical safeguards and to operate modern security systems is also important.

Competences related to knowledge of the law and the ability to apply them, which allow for effective and lawful action in crisis situations, are also an important direction of development. In view of the increasing regulatory requirements, especially resulting from the implementation of the CER Directive, training should also include procedures for the protection of CI.

It will also be important to introduce training on green transformation, including aligning operations with environmental regulations and ESG reporting, although respondents rated this topic as the least important. In addition, the security sector often has individuals with very different competences working together, highlighting the need to unify standards and improve practical skills in physical protection, such as the use of weapons, intervention techniques or team cooperation.

It is also recommended to increase the awareness of those responsible for procuring security services and to train them in the formulation of quality requirements for security services. Effective training programmes should be tailored to the specificities of the sector and take into account the interdisciplinary competence by combining knowledge from the areas of management, technology, law and physical protection.

The assessment of training needs is shown in Chart 5. Respondents could indicate up to three areas. The most frequently indicated competences were those related to safety management (34 indications), competences related to the evolution of threats and the emergence of new threats (33 indications) and competences related to technological progress (28 indications).

Chart 5. Assessment of training needs.

In order to effectively fill competence gaps, detailed development and standardisation of requirements for specific competence areas are needed. It is worth considering the implementation of a sectoral qualification framework, which could be addressed by a sectoral competence council, and the development of training programmes to upskill the workforce and adapt the sector to new challenges.

Further analysis should take into account both national and foreign solutions for competency formation in the security and safety sector, which will enable the development of effective tools to support the growth of the sector.

Summary

The security and safety of property and persons sector is facing the need to adapt to dynamic changes, comprehensively described in the report. This requires not only the implementation of new organisational solutions, but also a systemic approach to cooperation, education and regulation. The challenge is to strengthen cooperation between industry organisations (national and international), entrepreneurs, educational institutions and public administration. Given the difficult history of the industry and the negative influence exerted on it by some industry organisations, this element is particularly relevant from the perspective of the competence council's activities. Taking into account different perspectives in the development of standards and regulations can contribute to a more effective response to emerging risks and to improving the quality of services provided. In this context, it is important to draw on the experience of foreign professional organisations and to actively participate in the shaping of European competence standards in the security sector.

Legislative and organisational changes play a significant role in shaping the future of the sector. Many of the existing regulations are out of step with modern realities, resulting in difficulties in the interpretation of the regulations and their practical application, such as inconsistent competence requirements for qualified technical security personnel. It is therefore important to make the regulations more coherent and up-to-date so that they meet the real requirements of the market. The introduction of transparent regulations on professional entitlements in the security sector would both improve the quality of services provided and facilitate access to the profession for competent persons. A thorough amendment of the Act on the protection of persons and property, with the participation of a competence council, is a good direction. In the coming years, the impact of the amended Act on crisis management, which implements the CER Directive, will be important. Specific requirements for CI operators are to be expected – standardisation will cover the competences

of not only the operators' staff, but also the external service providers and the organisational and technical solutions that the operators will be required to use. In the long term, it will be necessary to standardise requirements across the sector, with a particular focus on the competences and qualifications of the sector's staff.

Improving the image of employees in the sector is also one of the important challenges. Currently, working in security is often associated with low demands and few opportunities for development, which reduces the supply of qualified staff. Building a positive image of the sector as an area offering stable employment, professional development and the opportunity to perform socially relevant tasks is necessary to attract new employees and increase the prestige of the profession[28].

Ensuring high-quality training and paying more attention to the practical part in education should also be an integral part of professionalising the industry. The current education systems and compulsory further education courses do not always fulfil their function, and many companies cut back on spending on employee development for financial and formal reasons.

The introduction of more effective quality control mechanisms for training and training institutions, as well as closer cooperation between universities and employers, could significantly improve the preparation of candidates for the sector. Adapting the educational offer of modern technologies and changing risks is key.

The Integrated Qualifications System (IQS) is relevant and its importance will increase in the coming years. Although there are many regulated qualifications in the sector, none of them have been included in the IQS so far. Such a move would increase the transparency of professional requirements and make them easier to compare. There is a need to review existing qualifications and adapt them to the contemporary needs of the sector.

Further exploration of competences required in the sector and the identification of tools supporting professional development of employees should also respond to these challenges. The creation of a sectoral qualifications framework and clarification of competency

[28] It is worth mentioning that POLALARM has been pushing for the recognition of the technical security profession as a profession of public trust for many years – through the partnership in the competence council, the implementation of such ideas will become possible.

standards for individual job roles would allow for better management of career paths in the sector. In addition, an analysis of existing solutions used in other sectors and countries could provide valuable insights into effective training methods and skills validation.

The sectoral competence council for the security and safety of property and persons sector is a tool to respond effectively to the challenges described in the report. The Council will work towards the professionalisation of the sector by integrating experts, entrepreneurs, representatives of the public administration and education. Its overarching goal will be to adapt the qualifications and competences of the sector's employees to dynamically changing realities in a broad context. The Council will bring together a group of distinguished experts with professional knowledge and experience, whose task will be to develop systemic solutions to improve the quality of security and safety services. Through cooperation with public institutions and industry organisations, it will not only monitor the needs of the market, but also initiate legislative, certification and educational activities. Sectoral competence councils operating in other areas of the economy have been effective in contributing to the harmonisation of competence and qualification standards. We intend to achieve the same effect in the security sector.

Adam Tatarowski

Chairman of the Competence Council for the Protection and Security of Property and Persons at the Polish Agency for Enterprise Development. Expert of the Government Centre for Security in the field of standardisation and conformity assessment of organisational and technical solutions used in ensuring the security of critical infrastructure. President of the Technical Property Protection Development Institute TECHOM – a specialised certification body and a continuing education institution operating within the educational system.

President of the All-Poland Association of Engineers and Technicians of Technical Security and Security Management 'POLALARM'. Member of the Standardisation Council at the Polish Committee for Standardisation.

Contact: tatarowski@techom.com

Terrorism – Studies, Analyses, Prevention, 2025, no. 7: 535–560

https://doi.org/10.4467/27204383TER.25.043.21820

Varia

The positioning of the GROM Military Unit in the national security system

Łukasz Niemczyk

Independent author

https://orcid.org/0009-0009-5759-7841

The purpose of this study is to signal the difficulties in the effective use of Special Forces units on the territory of Poland and abroad to support entities of the non-military system (organisational units subordinated to the minister responsible for internal affairs and supervised by the Minister Coordinator of Special Services or the Minister of Foreign Affairs) in the dynamically changing security environment of the state, in connection with both external and internal threats.

The statutory term the Armed Forces of the Republic of Poland (hereinafter: the Polish Armed Forces) began to function in general legislation since 9 December 1991, i.e. from the entry into force of the Act amending the Act on the universal duty to defend the Polish People's Republic and certain other acts[1]. In the amendment, the expression "Polish People's Republic" has been replaced by the expression "Republic of Poland", which is of particular significance in the change of the content

[1] *Act of 25 October 1991, amending the Act on the universal duty to defend the Polish People's Republic and certain other acts* (Journal of Laws of 1991, no. 113, item 491).

of Article 3(1) of the amended Act on the universal duty to defend the Polish People's Republic (Republic of Poland)[2], in accordance with which the sovereignty and independence of the Polish Nation as well as its security and peace are guarded by the Armed Forces of the Polish People's Republic (Republic of Poland). It can therefore be indicated that the Polish Armed Forces have existed since 1991. The GROM Military Unit was established by Organisational Order no. 004 of 13 August 1990 of the Minister of the Interior with a date of its final formation until 31 March 1991. It functioned within the Ministry of the Interior on the material, technical and financial provision of the commander of the Vistula Units of the Ministry of the Interior. Interestingly, the then Head of the GROM Military Unit – in accordance with § 3(1) of the aforementioned order – was a member of the Inter-Ministerial Anti-Terrorist Team.

Special Forces as a type of the Polish Armed Forces is a relatively young formation. It was introduced into the legal order, together with the Special Forces Command and the Commander of Special Forces[3], as of 4 July 2007 by virtue of Article 1 point 1 of the Act amending the Act on universal duty to defend the Republic of Poland and amending certain other acts[4]. The Minister of National Defence – by execusion of the statutory delegation set out in Article 13a(6) of the Act on universal duty to defend the Republic of Poland[5] – defined the requirements for the Special Forces by Order no. Z-8/MON of the Minister of National Defence of 15 February 2008[6]. Due to the nature of this study, only documents and data constituting publicly available and open information will be provided.

The Special Forces, despite the fact that they consist of highly specialised formations, especially the GROM Military Unit, the Commandos

---

[2] *Act of 21 November 1967 on the universal duty to defend the Polish People's Republic* (Journal of Laws of 1988, no. 30, item 207, as amended).

[3] Article 1 point 2 of the *Act of 24 May 2007 amending the Act on universal duty to defend the Republic of Poland and amending certain other acts*, which introduced the regulations in question in a new Article 13a(4) and (5) of the *Act of 21 November 1967 on universal duty to defend the Republic of Poland*.

[4] *Act of 24 May 2007 amending the Act on universal duty to defend the Republic of Poland and amending certain other acts* (Journal of Laws of 2007, no. 107, item 732).

[5] *Act of 21 November 1967 on universal duty to defend the Republic of Poland* (Journal of Laws of 2004, no. 241, item 2416, as amended).

[6] *Ordinance No. Z-8/MON of the Minister of National Defence of 15 February 2008 on the detailed scope of activities, organisational structure and the headquarters of the Special Forces Command* (Journal of Laws of Ministry of National Defence of 2008, no. 7, item 71).

and the Formoza Military Units, have been subordinated to the same system regulations identical to those of conventional military units. Over the course of several years, the Special Forces have gained and then lost independence. Along with the introduction of the Special Forces as a new type of the Polish Armed Forces, the Special Forces Command was established under the aforementioned Act of 24 May 2007. Subsequently, the reform of the leadership and command system carried out, among others, under the Act amending the Act on the office of the Minister of National Defence and certain other acts[7], abolished, as of 1 January 2014, the commands of the branches of forces (including the Special Forces Command). It left only the Operational Command of Branches of the Armed Forces and established the Armed Forces General Command. Thus, despite the existence of a de facto separate type of military such the Special Forces, they ceased to function independently and began to operate within the framework of all-military regulations, which is slowly being reversed.

Legal basis for the use of the GROM Military Unit in the country

There are two key provisions in the Constitution of the Republic of Poland[8] relating to the use of the Polish Armed Forces in the country: Article 26(1) and Article 5. The former defines the tasks of Polish Armed Forces and states that they serve to protect the independence of the state and the integrity of its territory and to ensure the security and inviolability of its borders. The latter provision complements the former and indicates that the Republic of Poland, among other things, ensures the security of citizens (protects them from external and internal threats). The statutory implementation of the constitutional regulations is the provision of Article 11(3) of the Act on defence of the homeland[9], according to which the Polish Armed Forces may participate in combating natural disasters and elimination of their effects, anti-terrorist actions, actions in the field

[7] *Act of 21 June 2013 amending the Act on the office of the Minister of National Defence and certain other acts* (Journal of Laws of 2013, item 852).

[8] *Constitution of the Republic of Poland of 2 April 1997* (Consolidated text of Journal of Laws of 1997, no.78, item 483, as amended).

[9] *Act of 11 March 2022 on defence of the homeland* (Consolidated text of Journal of Laws of 2024, item 248, as amended).

of property protection, search actions, actions to save or protect human health and life, protection and defence of cyberspace, clearing areas of explosives and hazardous materials of military origin and their disposal, as well as in the implementation of tasks in the field of crisis management. The legislator has developed these activities into a military operation conducted on the territory of the Republic of Poland in peacetime, introduced by Article 8 point 1 of the Act amending certain acts in order to improve the functioning of the Polish Armed Forces, the Police and the Border Guard in the event of a threat to state security[10]. This regulation entered into force on 31 August 2024. Such an operation consists of:

a) an organised activity of the Polish Armed Forces conducted for the purpose of ensuring the external security of the state, which is not a training or exercise,
b) the action of foreign troops within the framework of military reinforcement of the Polish Armed Forces or troops of the States Parties to the North Atlantic Treaty, as referred to in Article 3a(1) of the Act on the principles of stay of foreign troops on the territory of the Republic of Poland[11], the principles of their movement through this territory and the principles of providing assistance to allied troops and international organisations.

This action is taken if the circumstances require immediate action, in particular in situations of threat to the state border, critical infrastructure (hereinafter: CI) facilities, security of people or property of significant size, including when the forces and means of services subordinate to the minister responsible for internal affairs internal or supervised by him may prove inadequate due to the nature of the threat.

One may ask whether this type of action is related to the response of the Polish Armed Forces to threats of a terrorist nature, since the legislator does not refer here to any extent to anti-terrorist or counter-terrorist actions or CI as defined in Article 2 points 1, 2 and 4 of the Act on anti-terrorist

[10] *Act of 26 July 2024 amending certain acts in order to improve the functioning of the Armed Forces of the Republic of Poland, the Police and the Border Guard in the event of a threat to state security* (Journal of Laws of 2024, item 1248).

[11] *Act of 23 September 1999 on the principles of stay of foreign troops on the territory of the Republic of Poland, the principles of their movement through this territory and the principles of providing assistance to allied troops and international organisations* (Consolidated text of the Journal of Laws of 2024, item 1770).

activities (hereinafter: AT Act)[12]. This type of action, however, relates to supporting or even replacing the services responsible for preparing to take control of terrorist incidents by means of planned undertakings, responding to the occurrence of such incidents and restoring the resources intended for responding to such incidents (Article 3(2)).

In attempting to answer the question posed, it is necessary to recall the essential regulations concerning the tasks of the Special Forces. Firstly, Order no. 30/MON of 4 November 2013[13] was issued (pursuant to Article 12(1) point 1 and (2) of the Act on public finances[14]), in which the military units constituting the Special Forces and their tasks are openly indicated. According to the content of § 8 of Annex no. 2 to the mentioned order, the basic task of the GROM Military Unit is to carry out the full spectrum of special operations and physical counter-terrorist operations in the national, allied and coalition system in the land and maritime environment of the highest risk and strategic importance, including hostage release operations and conducting anti-terrorist operations during peace, crisis and war. Secondly, it should be emphasised that there is no clear and internally consisted system of the use of the Polish Armed Forces, including the GROM Military Unit, on the territory of the country in situations of terrorist threat. Despite the fact that the threat is one, the legislator has introduced as many as six solutions contained in as many acts, containing different modes of subsidiary use of the Polish Armed Forces, at the request of different entities, with different regulation of the use of weapons, armament and means of direct coercion and different forms of directing these actions.

The Act of 6 April 1990 on the Police

Branches and subdivisions of the Polish Armed Forces may be used to assist Police branches and subdivisions if the use of Police branches or subdivisions proves or may prove insufficient in the event of threat to public safety or public disturbance, in particular by causing:

[12] *Act of 10 June 2016 on anti-terrorist activities* (Consolidated text of the Journal of Laws of 2024, item 92, as amended).

[13] *Order no. 30/MON of 4 November 2013 on granting statutes to Special Forces Units* (Journal of Laws of the Ministry of National Defence of 2013, item 292).

[14] *Act of 27 August 2009 on public finances* (Journal of Laws of 2013, item 885 and 938).

1) public danger to life, health or freedom of citizens,
2) direct threat to property of significant volume,
3) direct threat to facilities or devices important for the country's safety and defence, on the seats of principal authorities, principal and central state administration authorities or the judiciary, on facilities of economy and national culture and on diplomatic missions and consular offices of foreign countries or international organisations, as well as facilities supervised by armed protection unit established pursuant to separate provisions,
4) **the threat of a criminal offence of a terrorist nature liable to result in danger to the life or health of participants of cultural, sporting or religious events, including gatherings or mass events**[15].

The Act of 12 October 1990 on the Border Guard

Branches and subdivisions of the Polish Armed Forces may be used to assist the Border Guard, if the use of forces of the Border Guard proves insufficient or is justified by the degree of threat. They may be used in the event of a threat to public security or disturbance of public order within the territorial range of the border crossing point and in the border area, in particular:

1) direct threat of an attack on the inviolability of the state border or its accomplishment,
2) introduction of direct public danger to life, health or freedom of citizens,
3) direct threat of an attack on facilities or equipment used by the Border Guard,
4) **the threat or commission of a criminal offence of a terrorist nature against the facilities or equipment referred to in point 3 or which may result in danger to human life**[16].

In addition, the provision of Article 11c(1) of the Act on Border Guard provides for the use of troops and subdivisions of the Polish Armed Forces in the form of independently conducted counteraction when required by

[15] Article 18 of the *Act of 6 April 1990 on the Police* (Journal of Laws of 2024, item 145, as amended). The emphasis in the text comes from the author (editor's note).

[16] Article 11b of the *Act of 12 October 1990 on the Border Guard* (Journal of Laws of 2024, item 915, as amended).

reasons of state security, ensuring the inviolability of the state border or a threat to public security in the territorial range of the border crossing and in the border zone or in the Polish maritime areas, if the Border Guard is not in a position to effectively counteract a threat or the commission of an offence or this is justified by the type of threat.

The Act of 3 July 2002 – Aviation Law

An unmanned aircraft may be destroyed, rendered inoperative or its flight may be overtaken when:

1) the course of operation or operation of the unmanned aircraft:
   a) endangers or is likely to endanger the life or health of a person,
   b) poses or is likely to pose a threat to protected objects, equipment or areas,
   c) disrupts or is likely to disrupt the course of a mass event or endangers the safety of its participants,
   d) **creates or is likely to create a reasonable suspicion that it may be used as a means of a terrorist attack**,
   e) poses or is likely to pose a risk to the safety of air traffic, the aircraft or the life or health of the crew or passengers on board,
   f) hinders or is likely to hinder air traffic or causes or is likely to cause its interruption or restriction;
2) an unmanned aircraft, contrary to a prohibition, performs an operation in a geographical zone established over:
   a) protected objects of the Polish Armed Forces and organisational units subordinated or subservient to the Minister of National Defence or supervised by the Minister of National Defence,
   b) facilities, equipment or areas essential for the security or defence of the state, public safety or the inviolability of the state border.

Among others, soldiers of the Military Police (points 1 and 2) and the Polish Armed Forces (points 1 letters a,b, d–f and 2) are authorised to destroy or immobilise an unmanned aircraft or take control of its flight[17].

[17] Article 156ze of the *Act of 3 July 2002 – Aviation Law* (Consolidated text of Journal of Laws of 2025, item 31, as amended).

The Act of 26 April 2007 on crisis management

If, in a crisis situation, the use of other forces and resources is impossible or may prove insufficient, unless other provisions state otherwise, the Minister of National Defence, at the request of voivode, may place at his/her disposal troops or subdivisions of the Polish Armed Forces, together with directing them to perform crisis management tasks, in accordance with the voivodeship crisis management plan. The tasks referred to above include:

1) participation in the monitoring of threats,
2) carrying out tasks related to the assessment of the consequences of phenomena occurring in the area of danger,
3) performing search and rescue tasks,
4) evacuation of the affected population and property,
5) performance of tasks aimed at preparation of conditions for temporary stay of evacuated population in designated places,
6) participation in the protection of property left in the area of danger occurrence,
7) isolating the danger area or the place where rescue action is to be carried out,
8) carrying out protection, rescue and evacuation works at endangered buildings and monuments,
9) carrying out works requiring the use of specialised technical equipment or explosives owned by the Polish Armed Forces,
10) removal of hazardous materials and their disposal, with the use of forces and means equipped by the Polish Armed Forces,
11) elimination of chemical contamination and biological contamination and infections,
12) elimination of radioactive contamination,
13) performing tasks related to the repair and reconstruction of technical infrastructure,
14) participation in ensuring the possibility of transport routes,
15) providing medical assistance and performing sanitary, hygienic and anti-epidemic tasks[18].

[18] Article 25 of the *Act of 26 April 2007 on crisis management* (Consolidated text of Journal of Laws of 2023, item 122, as amended).

Photo 1. Soldiers of the Grom Military Unit during the training on counter-terrorist tactics in the Warsaw metro.

Source: own materials of the Grom Military Unit.

Act of 4 September 2008 on the protection of shipping and seaports

In the event when the forces and resources of the Police and the Border Guard are insufficient or may prove tobe insufficient, the Minister of National Defence, on the proposal of the minister responsible for internal affairs, may decide on the application of necessary measures by the Polish Armed Forces in order to prevent, reduce or remove a serious and imminent danger created by the use of a ship or floating object as a means of a terrorist attack. This applies to the danger threatening:

1) ships, port and harbour facilities and associated infrastructure,
2) the Baltic Pipe interconnector constituting the connection of the transmission systems of the Republic of Poland and the Kingdom of Denmark along with the infrastructure necessary for its operation within the maritime areas of the Republic of Poland,
3) facilities, equipment and installations included in the infrastructure providing access to ports of fundamental importance for the national economy,
4) the use in the exclusive economic zone of artificial islands, all kinds of structures and equipment intended for the exploration or exploitation of resources, as well as other projects for the economic research and exploitation of the exclusive economic

zone, in particular for energy purposes, including offshore wind farms within the meaning of Article 3 point 3 of the Act on promoting electricity generation in offshore wind farms[19] and sets of equipment for the output of power within the meaning of Article 3 point 13 of the aforementioned Act, as well as submarine electricity and fibre-optic networks or pipelines and related infrastructure,

5) the liquefied natural gas regasification terminal in Świnoujście.

The Polish Armed Forces in the Polish maritime areas may take the necessary measures, up to and including the sinking of that ship or floating object[20].

Photo 2. Counter-terrorist operations tactics exercises in internal port areas.

Source: own materials of the Grom Military Unit.

The act of 10 June 2016 on anti-terrorist activities

In the case of the introduction of the third or fourth alert level pursuant to Article 16(1) of the AT Act, if the use of police divisions and subdivisions proves insufficient or may prove insufficient, troops and subdivisions

[19] *Act of 17 December 2020 on promoting generation electricity in offshore wind farms* (Consolidated text of Journal of Laws of 2025, item 498).

[20] Article 27 of the *Act of 4 September 2008 on the protection of shipping and seaports* (Consolidated text of Journal of Laws of 2024, item 597).

of the Polish Armed Forces may be used to assist the police divisions and subdivisions, in accordance with their specialised preparation, the equipment and armament they possess and the needs that arise[21]. Soldiers may be part of the counter-terrorist group referred to in Article 23(4) of the AT Act.

In order to fully answer the question concerning the response of the Polish Armed Forces to threats of a terrorist nature, it is necessary to clarify the tasks of counter-terrorism by the Special Forces. The provision of Article 3 of the AT Act established a kind of division of responsibility for anti-terrorist and counter-terrorist activities. Paragraph 1 refers to the responsibility of the Head of the Internal Security Agency (ABW), while paragraph 2 refers to the responsibility of the minister responsible for internal affairs (currently the Minister of the Interior and Administration).

Tasks related to counter-terrorism stem directly from the wording of Article 1(2) point 3a on the Police, delegating to the Police the conduct of counter-terrorist activities within the meaning of the AT Act.

To a certain extent, anti-terrorism issues are also included in the sphere of activities of the Border Guard, in accordance with the Act on the Border Guard. This is related to the main tasks of this service with regard to border traffic control, combating illegal migration and the supervision of the entry and residence of foreigners on the territory of Poland, as well as the prosecution of related crimes (Article 1(2) points 1–2a, point 4 letter (a), (c) and (e), points 5–5b) and with the obligation to cooperate with other bodies and services with regard to identifying and counteracting terrorist threats (Article 1(1) point 5d).

As mentioned, the Act on defence of the homeland in Article 11(3) indicates the tasks in which the Polish Armed Forces may participate. Since this law does not specify how they carry out the counter-terrorist activities in question, it would be appropriate to clarify their specific tasks. This is also a good starting point for enabling the establishment and development of cooperation of selected military units – primarily the Special Forces – with bodies whose tasks include: preventing terrorist incidents, preparing to take control of them by means of planned undertakings, responding to the occurrence of such incidents and removing their consequences, including the restoration of resources intended for responding to them. This would therefore be a cooperation primarily with the ABW.

[21] Article 22 of the *Act on anti-terrorist activities*.

This would allow a holistic whole-of-government approach (WGA) to state security, which would enhance the capabilities of both partners. The ABW would benefit from the use of logistics capabilities, equipment, forces and resources at the disposal of the Special Forces – if only in terms of chemical, biological, radiological, and nuclear (CBRN) threats, drones, communications integration, counter-terrorism and counter-insurgency expertise in terms of CI protection, and the Special Forces would gain access to threat information. This will enable the ABW and the Special Forces to better prepare, according to one of the principles, "for the war that will be, not that was". Furthermore, since – according to the AT Act – the counter-terrorist group includes, among others, officers of the ABW and soldiers of the Polish Armed Forces (Article 23(4)), one may ask why this law does not allow the Polish Armed Forces to cooperate directly with this service in counter-terrorist activities.

A similar inconsistency on the part of the legislator is evident in the entrusting of the Military Police (ŻW), within the meaning of the AT Act, only with the conduct of anti-terrorist activities in areas or facilities belonging to organisational units and entities subordinate to the Minister of National Defence or supervised by him or administered by these organisational units and entities (Article 4(1) point 3a of the Act on the Military Police and Military Law Enforcement Bodies)[22]. In view of the fact that the Act on the Military Police, in the provision indicating the way in which the tasks of the Military Police are carried out, apart from operational and reconnaissance activities, does not contain a provision indicating another way of carrying out the mentioned counter-terrorist activities, one has to wonder whether the tasks of the Military Police include counter-terrorist activities (Article 4(2)). Such tasks are also not provided for in the Regulation of the Council of Ministers of 2 July 2018[23], despite the fact that Article 14(1) and (2) of the Act in question does not take into account the cooperation of this formation with, inter alia, the Police and the ABW. The answer is contained in two provisions of the AT Act. The first

[22] *Act of 24 August 2001 on the Military Police and Military Law Enforcement Bodies* (Consolidated text of Journal of Laws of 2025, item 12, as amended).

[23] *Regulation of the Council of Ministers of 2 July 2018 on the cooperation of the Military Police with authorities entitled to perform operational and reconnaissance activities, to conduct investigations in cases of offences, as well as with authorities entitled to exercise the powers of a public prosecutor, and with authorities entitled to impose fines by way of a penalty ticket in cases of offences* (Journal of Laws of 2018, item 1334).

of these, Article 18 point 2, entrusts the leadership of anti-terrorist actions – undertaken by the competent services or bodies within the framework of their statutory tasks at the scene of a terrorist incident – to a soldier of the Military Police designated by the Minister of National Defence and, in urgent cases, by the Commander-in-Chief of the Military Police. This applies to incidents of a terrorist nature in areas or facilities belonging to organisational units and entities subordinate to the Minister of National Defence or supervised by him or administered by these organisational units and entities. The second provision, i.e. Article 23(4), specifies that special use of weapons may be made by officers of the Police, the Border Guard, the ABW, soldiers of the Military Police or the Polish Armed Forces who are part of a group performing counter-terrorist actions (hereinafter: counter-terrorist group). It would be reasonable to supplement the pragmatic Act on the Military Police with a provision analogous to that contained in the Act on the Police, where in Article 1(2) point 3a the legislator indicated that the basic tasks of the Police include, among others, carrying out counter-terrorist activities within the meaning of the AT Act. In addition, it is worth considering the possibility of providing support to the Military Police in counter-terrorist activities carried out within its local jurisdiction (in areas or facilities belonging to organisational units and entities subordinate to the Minister of National Defence or supervised by him or administered by these organisational units and entities) by the Central Counter-Terrorism Unit of the Police 'BOA' or by the Special Forces, which is not provided for in the Regulation of the Minister of National Defence of 24 July 2012[24].

This is a legitimate proposal because, as can be seen from the content of Resolution No. 252 of the Council of Ministers of 9 December 2014 on *the National Anti-Terrorist Programme for the years 2015–2019*[25], which, it is worth noting, was adopted before the enactment of the AT Act, (...) ***a branch of the Armed Forces particularly predisposed to support anti-terrorist actions are the Special Forces, which have capabilities, capacities, training and equipment increasing the potential of the aforementioned services in responding to threats of a terrorist nature. The Polish Armed***

[24] *Regulation of the Minister of National Defence of 24 July 2012 on the scope and mode of cooperation of the Military Police with the Military Counterintelligence Service, the Military Intelligence Service, military law enforcement bodies and with commanders of military units and commanders (commandants) of garrisons* (Journal of Laws of 2012, item 880).

[25] *Resolution no. 252 of the Council of Ministers of 9 December 2014 on "the National Anti-Terrorist Programme for the years 2015-2019"* (M.P. of 2014, item 1218).

Forces also participate in stabilisation missions, peacekeeping missions and international anti-terrorist coalitions. Unfortunately, this document was not amended after 2019 and the entire programme was expired.

The 2020 National Security Strategy, on the other hand, indicated that it is necessary (...) ***to develop the operational capabilities of the Polish Armed Forces, in particular the Special Forces, to combat threats, including those of a hybrid nature*** [,] ***and counter-terrorist activities, in all states of emergency and state of national defence readiness***[26]. Similar provisions appear in *the National Security Strategy Recommendations* of 4 July 2024: (...) ***the state's ability to counter hybrid threats is an important element of building the state's resilience and should include, due to its unique nature, inter alia, the development of the operational capabilities of the Polish Armed Forces, in particular the Special Forces – for counter-terrorist operations in all states of national defence readiness*** (...)[27].

Unfortunately, the indicated documents have not been translated into specific solutions that could significantly improve the use of the Special Forces, especially the GROM Military Unit, which is discussed in more detail later in the text.

Tasks of the GROM Military Unit

The operations carried out by Special Forces are wide-ranging. The tasks of individual Special Forces units are listed in the already mentioned Order No. 30/MON:

1) the GROM Military Unit – **implementation of the full spectrum of special operations and physical counter-terrorism operations in the national, allied and coalition system in land and maritime environments of highest risk and strategic importance, including hostage release operations and conducting counter-terrorist operations, during peace, crisis and war**,
2) the Commandos Military Unit – implementation of the full spectrum of special operations in the national, allied and coalition

[26] *The National Security Strategy of the Republic of Poland of 2020*, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf, p. 19 [accessed: 23 I 2025].

[27] *The National Security Strategy Recommendations*, 4 VII 2024, https://www.prezydent.pl/storage/file/core_files/2024/7/4/7fa9f08052b51758d6ed4e9a11a9d32d/REKOMENDACJE%20SBNRP%204%20lipca%202024.pdf, p. 28 [accessed: 23 I 2025].

system in the land environment, including inland waters, to achieve objectives of operational and strategic importance in times of peace, crisis and war,

3) the Formoza Military Unit – implementation of the full spectrum of maritime special operations in national, allied and coalition system to achieve objectives of operational and strategic importance. The unit retains the capability to support the maritime component in a combined operation and to support hostage release operations in a maritime environment.

Photo 3. Counter-terrorist operations tactics exercises in aircraft.

Source: own materials of the Grom Military Unit.

Significantly, the entire cycle of recruitment, training, planning and procurement is subordinated to maintaining and enhancing the capability to conduct the above-mentioned actions and operations. Thus, the Polish Armed Forces have military units dedicated to anti-terrorist operations, including counter-terrorist, of which, in the author's opinion, the most versatile and specialised in physical counter-terrorism is the GROM Military Unit.

The GROM Military Unit maintains forces and resources to support the structures of the Ministry of the Interior and Administration and constitutes an effective tool to ensure the internal security of the country

within the framework of the tasks of the Polish Armed Forces[28], which include:

- support of the forces and resources of the Police and the Border Guard by, inter alia, providing transport of task elements during operations in support of the protection of the land border and territorial waters, day and night and in all weather conditions,
- support of RENEGADE operations (in particular M-RENEGADE) by, inter alia, maintaining forces and means in high readiness for action at all times,
- securing the country's CI by, inter alia, conducting aerial reconnaissance of threatened areas,
- support of the forces of the Ministry of the Interior during the security of large mass events and VIP visits, inter alia, by maintaining constant readiness of task elements within the framework of AT duty, as well as by increasing the mobility and reducing the response time of dedicated forces and resources, in a situation of a threat of a terrorist event,
- supporting the non-kinetic crisis management system, for example, by evacuating victims from disaster areas,
- conducting search and rescue operations in an environment beyond the capabilities of civilian services.

The GROM Military Unit, in accordance with the *Crisis Management Plan of the Ministry of National Defence*[29], maintains forces and resources in readiness to assist the Police in conducting counter-terrorist operations. The Police unit designated for this type of operation is the Central Counter Terrorism Unit of the Police 'BOA'.

As noted in the literature on counter-terrorism, the GROM Military Unit (...) *occupies a very important place in the crisis response system. It should be*

[28] *Order no. Z-3/KT of the Commander of the Special Forces Component of 20 January 2023 on the use of the "Plan for the Use of Forces and Means of the Commander of the Special Forces Component in Crisis Situations" in the Special Forces Component Command and subordinate units of the Special Forces Component* (classified document).

[29] *"Crisis Management Plan of the National Defence sector" approved by the Minister of National Defence on 16 August 2022*; *Order no. Z-9 of the General Commander of the Armed Forces of 10 January 2023 on the implementation of the "Plan for the use of forces and means of the General Commander of the Armed Forces in crisis situations" in the Armed Forces General Command and the organisational units subordinate to the Armed Forces General Commander*; *Order no. Z-3/KT of the Commander of the Special Forces Component of 20 January 2023 on the use...*

emphasised that it is the only unit capable of performing tasks related to physical counter-terrorism in all its manifestations, (...) *it is a versatile unit, capable of performing tasks of varying degrees of difficulty in all regions of the world*[30].

Prospects for the development of the Special Forces, including the GROM Military Unit

The issue of the development of the Special Forces, including the GROM Military Unit, can be considered on two levels. The first one concerns separate legislation for the Special Forces or their selected units. As indicated in the literature, such a solution has been planned before. As part of the work on the legal basis of the GROM Military Unit in the state structures, it was proposed that the rules of its operation should be regulated by an act of statutory rank. The draft act regulating the principles of operation of this special unit was developed by a group of lawyers specialising in internal security[31]. However, the proposal was rejected by the Ministry of Defence. The unit became part of its structure on 1 October 1999. Since the subordination of the GROM Military Unit to the Special Forces Command, later to the Special Forces Component Command (subordinate to the Armed Forces General Command), the concept of a separate regulation for this formation has not had any support among military and political decision-makers. Currently – in the author's opinion – such a complete exclusion of the GROM Military Unit from subordination to military structures and its transfer to the direct disposal of a political body (e.g. the Minister of National Defence) does not find any practical or functional justification. However, it is undoubtedly necessary to improve and accelerate the procedures for the use of the Special Forces units in widely understood crisis situations and to make these procedures to some extent secret.

[30] *Zagadnienia fizycznej walki z zagrożeniami terrorystycznymi – aspekty prawne i organizacyjne* (Eng. Issues in the physical fight against terrorist threats – legal and organisational aspects), K. Jałoszyński (ed.), Warszawa 2010, p. 264.

[31] H. Królikowski, *Wojskowa formacja specjalna GROM im. Cichociemnych Spadochroniarzy Armii Krajowej 1990–2000* (Eng. Military special formation GROM named after Cichociemni Paratroopers of the Home Army 1990–2000), Gdańsk 2001, pp. 110–111.

Photo 4. CBRN threat prevention exercises.

Source: own materials of the Grom Military Unit.

The second level of development is the creation of a body directly subordinated to the Minister of National Defence (through the Secretary of State or Undersecretary of State or the Chief of the General Staff of the Polish Armed Forces) or within the Government Centre for Security or within the structures of the Minister's Cabinet – the member of the Council of Ministers responsible for coordinating of special services (e.g. under the name of the High Risk Operations Bureau). The task of this body would be to coordinate within the Ministry of National Defence or inter-ministerially the exchange of information between the Ministry of National Defence, the Special Forces, the special services, as well as to quickly, effectively and secretly earmark a component of the Polish Armed Forces with the leading role of the Special Forces (especially the GROM Military Unit) to create task forces with the participation of the special services. This is justified insofar as, in accordance with Article 19(1) and (2) of the AT Act, the minister responsible for foreign affairs, in cooperation with the Minister Coordinator of Special Services,

if appointed, coordinates the actions of the relevant services and authorities in the event of a terrorist incident outside the borders of the Republic of Poland against citizens or property of the Republic of Poland, excluding terrorist incidents outside the borders of the Republic of Poland against personnel or property of the Polish Armed Forces. Such a dichotomous division has not worked and appears ineffective, as demonstrated by the operation to evacuate Polish citizens from the Islamic Republic of Afghanistan[32]. In this case, military action was taken (a military operation both in terms of its nature and the forces and means used) in the case of a threat to non-soldiers, citizens of the Republic of Poland and citizens of other countries. Such a solution has been planned in similar circumstances in other threat areas where civilian Polish citizens were or are present. This operation proves the necessity to develop legal solutions concerning the cooperation of the Special Forces and the Foreign Intelligence Agency (hereinafter: AW). A seed of such solutions exists in Article 10(2a) of the Act on the Military Counterintelligence Service (hereinafter: SKW) and the Military Intelligence Service (hereinafter: SWW)[33]. According to this provision, in the performance of their tasks, these services cooperate with the General Staff of the Polish Armed Forces and other organisational units of the Ministry of National Defence, as well as the General Commander of the Armed Forces, the Operational Commander of the Armed Forces, the Commander of the Territorial Defence Forces, the Chief of the Inspectorate for the Armed Forces Support, commanders of military garrisons and military units. In the purpose for this cooperation, in particular to ensure the security and proper implementation of the tasks of the SWW outside the country's borders, task forces may be created in the SWW, consisting of officers of this service, professional soldiers assigned to official positions in the SWW and soldiers serving in troops or subdivisions of the Polish Armed Forces.

Taking into account the nature of potential threats to the state's security related to terrorist activity and the analysis of potential directions of their development, it should be emphasised that efficient and discrete (the so-called *law pro*) cooperation of the Special Forces,

[32] *Polish soldiers completed mission in Afghanistan*, the Ministry of National Defence, 27 VIII 2021, https://www.gov.pl/web/obrona-narodowa/polscy-zolnierze-zakonczyli-misje-w-afganistanie [accessed: 23 I 2025].

[33] *Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service* (Consolidated text of Journal of Laws of 2024, item 1405, as amended).

especially the GROM Military Unit, with special services, the Police and the Border Guard is necessary for ensuring the country's security at a high level. The most desirable form of development of the Special Forces is the creation of a legal framework in individual acts regulating the functioning of special services, on the basis of which the Special Forces, and especially the GROM Military Unit, will be able to efficiently support bodies responsible for the internal security of the state. In the case of the need to use the Special Forces outside the country, there is also a need to modify the current mode. Currently, the operation of the Polish Armed Forces abroad is decided by the President of Poland. However, the interaction of the task forces of the special services and the Special Forces will be subject to multi-level control in the form of the Minister of National Defence, the Minister Coordinator and the Prime Minister. Bearing in mind the need for speed, the sparse composition of the task force and, above all, the operations security, the President may be informed of it but does not necessarily have to decide, as such a task force would operate under the direction of the service concerned (in this case the AW). It is also important to improve and make the process secretive. To this end, a number of issues need to be regulated, including pseudonymisation[34] and planning and financial autonomy of the Special Forces, i.e. the creation of a separate special operations fund to pay for logistics costs, as well as, the creation of the Special Forces task groups with the special services, and the possibility of shifting ADCOM (Administrative Command) or OPCOM (Operational Command) subordination to shorten the decision-making path.

Countering hybrid threats and counter-terrorist activities require effective coordination of the use of the services responsible for these tasks, according to the whole-of-government (WAG) principle. This requires:

a) rapid transmission of information,
b) rapid decision-making,
c) rapid activation and use of adequate forces and resources.

With regard to the speed of the flow of information and decision-making, it should be pointed out that the recent amendments to the service pragmatics of the Police, the Border Guard and the AT Act introduced under the Act amending certain acts in order to improve the operations

[34] Using operational numbers or nicknames to make it difficult to identify formations or personal data of soldiers.

of the Polish Armed Forces, the Police and the Border Guard in the event of a threat to state security, made it possible to transmit a request or decision on the use of the Polish Armed Forces by authorised bodies orally, by telephone, by means of electronic communication within the meaning of Article 2 point 5 of the Act on the provision of services by electronic means[35] or by other means of communication. The content of the request or decision and the relevant motives for such settlement of the case shall be recorded in writing in paper form (Article 1 point 2 letter (b), Article 2 point 1 letter (b), Article 7 point 2 letter (a)). Such a solution has previously been postulated by the Special Forces on several occasions and can be assessed as positive. Practice will show whether it will be properly used.

De lege ferenda proposals and comments

The next part of the text will present proposals on the principles of the functioning of the Special Forces for consideration by experts in the field of state security, especially the operation of the special services.

According to the current legal order, the Special Forces do not have the possibility of direct interaction with the AW, the ABW or the State Protection Service (SOP). There seems to be a willingness to cooperate at the tactical and operational levels, but there is a lack of legal solutions of a statutory rank, which is necessary in the case of transferring classified information or the use of means of direct coercion or firearms, as well as – to a limited extent – supporting or protecting special services in carrying out operational and reconnaissance activities (e.g. by collecting biometric data for the needs of these services) or protective measures (SOP). The creation of tools analogous to those in the case of the SWW or the SKW could be considered (Article 10 or Article 4 of the Act on the SKW and the SWW), i.e. task forces consisting of the AW, the ABW or the SOP officers, professional soldiers appointed to official positions in these services and soldiers serving in troops or subdivisions of the Polish Armed Forces (due to the specificity of the tasks of these services, the participation of the Special Forces soldiers only could be considered in this situation).

[35] *Act of 18 July 2002 on the provision of services by electronic means* (Consolidated text of Journal of Laws of 2024, item 1513).

The current provisions of Article 10 of the Act on the ABW and the AW[36] or Article 4 and Article 19(1) of the AT Act do not provide sufficient grounds for real cooperation between the Special Forces with the ABW and the AW, including the use of weapons or means of direct coercion even for the protection of CI, CBRN security (protection against proliferation of weapons of mass destruction) or action beyond the borders of the state. Similarly, according to Article 38 of the Act on the SOP[37], no provision is made for the possibility of support of this formation by the Polish Armed Forces, in particular the Special Forces, and especially the GROM Military Unit. In the case of persons of special status, their protection on the ground in the country and, above all, outside its borders, e.g. in the area of armed conflict, it seems to be an area requiring consideration and correction by the legislator. All the more so, as discussed, Article 11 of the Act on defence of the homeland provides for the possibility of using the GROM Military Unit (as an element of the Polish Armed Forces) for anti-terrorist activities (specific primarily for the ABW, in accordance with Article 3(1) in conjunction with Article 2 point 1 of the AT Act) and crisis management, and thus, inter alia, for the protection of CI (Article 2 in conjunction with Article 3 points 1 and 2 of the Act on crisis management). It is also worth considering the participation of experts from the GROM Military Unit in the deliberations of working groups and teams operating in the crisis management system. The proposed solution will undoubtedly benefit the Special Forces, as demonstrated by operations outside the country's borders, inter alia, in the Islamic Republic of Afghanistan. After analysing these operations, the experts assessed that (...) *the necessary skills to use their own sources of information were subsequently acquired, including through the acquisition of appropriate equipment and better cooperation with the relevant services*[38].

A complementary element should be the addition of Special Forces to the chain of bodies with which the Head of the ABW coordinates analytical and information activities and exchanges information, in particular those

[36] *Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency* (Consolidated text of Journal of Laws of 2024, item 812, as amended).

[37] *Act of 8 December 2017 on the State Protection Service* (Consolidated text of Journal of Laws of 2025, item 34, as amended).

[38] T. Sapierzyński, *Operacje bojowe JW GROM w pierwszej dekadzie XXI wieku* (Eng. The GROM Military Unit combat operations in the first decade of the 21st century), "Bezpieczeństwo. Teoria i Praktyka" 2020, no. 2, p. 164. https://doi.org/10.34697/2451-0718-btip-2020-2-009.

relating to events and threats of a terrorist nature (Article 5(1) of the AT Act), as well as making it clear in organisational documents that the Special Forces are the reconnaissance service of the Polish Armed Forces, as referred to in Article 11 of the Act on the ABW and the AW.

As mentioned, the support of the 'BOA' by the GROM Military Unit can take place both under the Police Act (Article 18) and the AT Act (Article 22). In the first case, the cooperation (decision of the authorised body) can be initiated without the introduced alert levels referred to in Article 15(1) of the AT Act, but with restrictions on the use of firearms[39]. In the second case, the use of the GROM Military Unit to support counter-terrorist operations conducted by the 'BOA' can only take place after the introduction of the third (CHARLIE) or fourth (DELTA) alert level (Article 22(1) of the AT Act). The two procedures are carried out on two different legal bases. Therefore, for example, the support of the Police by the GROM Military Unit during a Polish Army Day or a mass event related to the visit of a person with a special status from another country (which without the third or fourth alert level can only take place under the Police Act), it cannot continue as a counter-terrorist group activity within the meaning of Article 23(4) of the AT Act (this also applies to the authority for the special use of weapons referred to in Article 23(1) of that Act) immediately after the introduction of the third or fourth alert level. This is due to the fact that the original decision of the Minister of National Defence (Article 18(5)) or the provision of the President of the RP (Article 18(3)) issued under the Act on the Police, as already stated, are issued on a different legal basis.

Similarly, the issue of the special use of weapons (Article 23(1) of the AT Act) needs to be reviewed, as it only applies to firearms. Today, it is already known that an unmanned aerial vehicle (UAV) with a suspended explosive charge may also be used if this is necessary to counter a direct, unlawful, violent attack on a person's life or health or to free a hostage, and the use of firearms in a manner causing the least possible harm proves insufficient and it is not possible to counter such an attack or to free the hostage by other means. In the circumstances indicated, the effect of this special use of a weapon may be death or an imminent threat to the life or health of the person making the attack.

[39] Lack of possibility to use weapons in a special way, as referred to in Article 23 of the AT act.

In this regard, due to the dynamic development of UAV technology, the provisions of the Act – Aviation Law and ministerial regulations should be adapted so that the Special Forces can use UAVs, including loitering munitions commonly referred to as kamikaze drones, as weapons[40], in the course of both real-world operations and training, without having to treat their damage or destruction as an aviation accident or incident or damage to property. In addition, the process of acquiring UAV flight authorisations for military pilots to counter hybrid threats and perform counter-terrorist or CI resilience-building activities should be deformalised.

Another issue has also recently emerged, namely the conduct of a counter-terrorist operation to free hostages during a full-scale armed conflict. In principle, there is no controversy regarding its legal basis, the difficulty arises in the selection of the tools (means) used for this purpose. According to Article 8 of the Rome Statute of the International Criminal Court[41], war crimes mean serious violations of the Geneva Conventions of 1949[42] and other serious violations of the laws and customs of international law applicable to armed conflicts of an international character. These include the use of bullets which expand or flatten in the human body, such as bullets with a hard envelope which does not entirely cover the core or is pierced with incisions (Article 8(2) letters (a) and (b) (xix) of the Rome Statute of the International Criminal Court). In counter-terrorist operations, such ammunition, i.e. hollow-point bullets, is advisable because of their anti-ricochet properties (safety for bystanders) and their knock-down power (increasing the likelihood of eliminating the threat with a small number of shots). These bullets have several advantages that make them an excellent for self-defence:

- are safer for bystanders than full metal jacketed bullets,
- are less likely to ricochet and hit bystanders because they are less likely to bounce off hard surfaces and hit unintended targets,
- are less likely to kill bystanders if fired at the wrong angle,

[40] SOFCOM Doctrine and Lessons Learned 26.11.2024 – The New Frontier of Warfare: Unmanned Systems and Countermeasures (NATO UNCLASSIFIED document, but it has not been submitted for publication, the document can only be used by the institutions indicated in it).

[41] *Rome Statute of the International Criminal Court of 17 July 1998* (Journal of Laws of 2003, item 708, as amended).

[42] *Conventions for the Protection of War Victims signed at Geneva on 12 August 1949* (Journal of Laws of 1956, item 171, as amended).

- they expand on impact, creating a larger wound channel, thus increasing the incapacitation rate[43].

This type of ammunition is also used in Poland for counter-terrorist operations within the country during peacetime[44]. This is a topic for discussion in terms of conducting effective, and therefore hostage-safe Hostage Rescue operations in analogous conditions to what happened in Gaza[45], although using means that are questionable from the point of view of international humanitarian law, i.e. hollow-point ammunition.

Summary

The presented issues are the result of experiences related to the functioning of the Special Forces and the GROM Military Unit gained during real-life operations and trainings with various national and foreign formations. The author hopes that the thoughts contained in the text will help initiate an expert discussion on the role of Special Forces' units in supporting the so-called non-military system. It should be emphasised that the aim is to increase the statutory capabilities of the constituent services and formations, not to replace them or duplicate their tasks by the Special Forces. In the author's opinion, the enhancement of these capabilities is necessary for peacetime and non-war crisis operations. This is especially true for securing CI and ensuring the security of the most important persons in the state in situations of hybrid threats. At the same time, attention should be paid to the legal security of soldiers and officers. They should feel that when they are carrying out tasks ordered by their superiors, the state and clear legal regulations are behind them and that they are able to select forces and means the most appropriate to the threat.

[43] *Amunicja typu Hollow Point a konwencja genewska* (Eng. Hollow Point Ammunition and the Geneva Convention), Centrum Praw Człowieka, 9 VIII 2022, https://ofpc.pl/amunicja-typu-hollow-point-a-konwencja-genewska/ [accessed: 23 I 2025].

[44] J. Sabak, *Milion pocisków antyrykoszetowych dla JW GROM* (Eng. One million anti-ricochet missiles for the GROM Military Unit), Defence24, 15 V 2015, https://defence24.pl/geopolityka/milion-pociskow-antyrykoszetowych-dla-jw-grom [accessed: 23 I 2025].

[45] P. Celej, *Elitarna izraelska jednostka Jamam w akcji: Kulisy uwolnienia zakładników przez Siły Obronne Izraela* (Eng. Israel's elite Jamam unit in action: Behind the scenes of the release of hostages by the Israel Defence Forces), Gazeta Prawna, 8 VI 2024, https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/9522754,elitarna-izraelska-jednostka-jamam-w-akcji-kulisy-uwolnienia-zakladni.html [accessed: 23 I 2025].

Legal counsel and professional soldier. He deals with the subject of Special Forces, and in particular with legal solutions concerning the use of such formations for cooperation in non-military system, and also with streamlining procedures concerning the use of Armed Forces in the territory of the country and abroad. Lecturer, among others, at the University of Technology and Economics in Warsaw and at the National School of Judiciary and Public Prosecution.

Contact: l.niemczyk@ron.mil.pl

Terrorism – Studies, Analyses, Prevention, 2025, no. 7: 561–570

https://doi.org/10.4467/27204383TER.25.044.21821

Varia

35th anniversary of the GROM Military Unit. The role of special units in times of hybrid threats

The high dynamics of political, economic and technological changes taking place in the modern world mean that in order to act effectively, one must be proactive and constantly seek new solutions. The military sphere, which uses modern tools, for example, in the form of swarms of autonomous unmanned systems, 3D printing or artificial intelligence, and constantly adapts tactics, techniques and procedures, is no exception to this respect.

– In the GROM Military Unit, we constantly analyse changes taking place in the world and security architecture in order to anticipate threats and challenges that the future may bring, and to know whether our current capabilities will allow us to meet them – emphasises **Col. Grzegorz Krawczyk**, Deputy Commander of the GROM Military Unit. In July 2025, the elite Special Forces unit will celebrate its 35th anniversary.

Damian Szlachter: The GROM Military Unit was formed in 1990 and will celebrate its 35th anniversary this year. Please tell us what changes it has undergone during this time and whether any commemorative events are planned.

Col. Grzegorz Krawczyk: during its 35 years of existence, GROM has been reorganised several times. From a unit capable of performing counter-terrorist tasks, it has become a unit capable of independently conducting – within the national and allied system – complex special operations, requiring the involvement of professionals from various fields, such as: CBRNE, JTAC, K9, EOD[1], analysts and reconnaissance or targeting specialists supporting the combat element. Our ability to redeploy task elements has also changed and GROM can now autonomously deploy operators by land, water and air. However, the biggest transformation has been in the command capability. We have moved from a unit administration model to a model of commanding GROM task forces and assigned combat teams, both national and coalition, during special operations conducted in a crisis, below the threshold of war and kinetic special operations during war. The changes are the result of experience gained in various circumstances and areas, mainly in the performance of tasks outside the country, thanks to participation in national and foreign military exercises and those involving non-military formations. Training with the best special forces units in the world, i.e. the British 22 SAS Regiment, the US CAG, Navy SEAL or 10th SFG, is particularly valuable. We also constantly analyse the changes that are taking place in the world and the security architecture in order to anticipate what threats and challenges the future may bring and to know whether our current capabilities will be able to meet them.

As part of the celebrations of the GROM Military Unit, a closed conference will be held on the challenges facing special forces in relation to the geopolitical situation in the world – the current one and the one we may face in the future. There will be national and international experts as speakers. Our aim is to show the broadest possible view of the topics discussed, which is why we have invited representatives from the military and civilian spheres to participate

[1] CBRNE (chemical, biological, radiological, nuclear, and explosives), JTAC (joint terminal attack controller), K9 – term for combat dogs, EOD (explosive ordnance disposal) – acronym for pyrotechnics (editor's note).

in the meeting. Confirmed speakers include Gen. Austin S. Miller (retired), former commander of CAG and US JSOC Command, and Peter W. Singer, a 21st century warfare specialist. A book on the history of GROM should be published by July. Its co-authors are professional historians associated with the Warsaw Rising Museum, and work on it has taken more than seven years. We have taken care to ensure that the study has an accessible form for the reader. I believe that it will be a very valuable item in the library of every GROM sympathiser and beyond.

In the last dozen years, GROM has intensively supported the development of Poland's counter-terrorist system, including by providing comments on amended legislation, organising training, participating in counter-terrorist exercises, sharing combat experience from areas of armed conflict, supporting the protection of VIPs and diplomatic missions or building the resilience of critical infrastructure facilities to sabotage activities. I have been following this multifaceted activity for a long time and admire it for its professionalism and commitment. How do you manage to combine so many different projects and activities within one unit?

The creation of the GROM Military Unit in the 1990s was guided by one objective – to have a professional unit with the capability to respond to terrorist threats arising from the global situation at the time. Initially, GROM's participation in military operations outside the country was not envisaged, although it did carry out such operations, whether in Haiti or the Balkans. The subordination of the unit to the Ministry of the Interior meant that it could be quickly directed to carry out counter-terrorist tasks at home, but the possibilities for its use in missions abroad were limited. In 1999, GROM was transferred from the structures of the Ministry of the Interior to the Ministry of National Defence. This was to allow a more efficient use of its potential outside the country and a much better provision of the unit's logistical needs. However, the subordination to the Ministry of National Defence did not change GROM's basic tasks, i.e. readiness to conduct hostage release and counter-terrorism operations.

Although the unit was "plugged in" to the national crisis management system, ready to support counter-terrorist activities carried out either by the Border Guard or the Police, it lacked an efficient overarching system to manage these forces in crisis situations. After 2014, the security situation in our region has changed radically. Analysing the geopolitical situation and bearing in mind the experience of our British partners, as well as the legislation in force in Poland, we concluded that we need to be more proactive at the level of internal security. In 2017, we began intensive work on a concept to increase our effectiveness in this sphere, and included not only terrorist threats but also hybrid threats, which did not receive as much attention as they do now. At that time, however, the latter area was not understood in our military environment, as the possibility of such threats was not anticipated. The concept we developed encompassed a number of areas, including support for the training process of counter-terrorist sub-units drawn from the non-military system, participation in exercises and training on the subject, legal analyses for the effective use of the unit in counter-terrorist operations and recommendations for legal changes. We also sought to enhance our ability to respond more quickly to a crisis. This was reflected in the shortening of the time that elapsed from decision to take action, which further enhanced the ability to maintain an appropriate level of secrecy for special operations and the ability to rapidly redeploy forces to any location in Poland. Thanks to this initiative, an Aviation Team equipped with S-70i Black Hawk helicopters was established at GROM.

Today, more and more advanced technologies are being used in terrorist attacks – swarms of unmanned vehicles, 3D printing, artificial intelligence, satellite internet. How is GROM improving its resources and tactics to meet new challenges and be effective?

Yes, it is true, the security environment has changed a lot, as have the tools to attack. This is one of the consequences of the conflict in Ukraine. Wars have always accelerated the adaptation of different types of technology for military purposes. This was the case, for example, with dynamite, which was originally intended for civilian mining work and a while later found its use in military operations. 3D printers, which were initially used for fun or to make various

things for civilian use, have now become a tool for producing weapons and their components. There is exponential growth in this matter and practically every fortnight, maybe every month, improved or completely new solutions appear. From the beginning, GROM's organisational culture has emphasised creativity and the constant search for the best tools, techniques, tactics and procedures to get the job done. We have built-in mechanisms to support this. Much is contributed in this respect by our multinational cooperation and exchange of experience with foreign partners. It is a process of continuous information gathering and analysis. The next level is self-initiative – we look for solutions to problems, while trying to think outside the box. We also have our own 3D printing workshop and innovation department, where our ideas are embodied and then tested by end users. It is a 360° process, which means that we are in a permanent cycle of observation, analysis, implementation and adaptation to the VUCA world[2]. It would still be worth thinking about the possibility of cooperating or using GROM to support all Polish special services in order to work out optimal solutions, taking into account the experiences of various foreign organisations.

What does the war in Ukraine teach you about the role of special units in contemporary armed conflict? What changes are your partners from NATO countries making in relation to it?

The war in Ukraine is a huge source of information in many aspects of contemporary conflict. It is the first war in the 21st century where it can be assumed that two what we would call militarily equivalent states are fighting each other, and operations are being conducted in almost all domains, i.e. land, sea, air and cyberspace. An analysis of the three years of this war allows many positive, but also negative, conclusions to be drawn about the use of special forces units. Since 2014, NATO has made many efforts to organise Ukrainian special forces along Western lines. After almost eight years of strenuous training, it was possible to establish a special forces command and to certify Ukrainian special units according to Alliance standards. However, the beginning of the war revealed the problem of a complete misunderstanding of the role and tasks of special forces by all-military

[2] VUCA (volality, uncertainly, complexity, ambiguity) – (editor's note).

commanders. Wrong decisions on the use of this type of military resulted in almost all their potential being lost in a few months. And this is the first lesson, for us the most important one. Having analysed the Polish military environment, as a special unit command we are not sure that we would not share a similar fate in wartime. This is our sore point, as we are aware of how much effort and time it costs to select and then train a special forces unit operator (basic training is a minimum of 12 months) and how demanding the process of rebuilding such capabilities is. Therefore, treating special forces as better-trained infantry and assigning them to tasks such as "cleaning" the trenches is a straightforward way to lose these capabilities and have a serious problem recreating them at an appropriate level in the short term. When analysing the course of a conflict, both we and our NATO partners project potential tasks for us during special operations. We can distinguish three phases of a future conflict. The first is likely to be a hybrid action, perhaps terrorist, to disorganise the functioning of critical infrastructure and the state. Here, the role of special operations as a support element to the non-military system in preventing and combating such threats is quite evident. The duration of this phase can be either short but intense or long in order to exhaust forces. The second phase is a dynamic kinetic clash in which tactical manoeuvre will be a key factor. Special operations can be of a different nature in this phase – ranging from the classic task of searching for and destroying high-value and high-reward targets, e.g. air defence systems, ballistic missiles, logistical supplies, operational command and communications systems, to counterinsurgency operations and military support of conventional troops. The latter would consist not of fighting within the ranks of general military subdivisions, but more of advising battalion-level commanders to bring together the entire multi-domain battlefield capability, but with such an element specific to special forces. This view is being considered by many NATO special forces units. The third phase is frontline stabilisation, where static fighting will take place, which is what we are now seeing in Ukraine. The centre of gravity of the special forces tasks can be shifted in this case to the creation and management of resistance movements in areas occupied by the enemy and to striking at the political and economic interests of the aggressor state, both in its hinterland and in third countries where it has such interests. These are lessons from the operational level, very important

for us to create in military and political decision-makers a picture of the correct conduct of special operations in times of crisis and war.

In the area of tactics, techniques and procedures, there are even more conclusions. Someone quite aptly described Russian's ongoing war with Ukraine as a combination of Star Wars and World War I. The widespread use of drones of all kinds has meant that it is no longer possible to fight the way we used to. The drone now functions as binoculars, a rifle and a grenade, but has much greater range than these combat attributes. The use of flying, floating or land-based drones is being explored both theoretically and practically. Some capabilities are already implemented, others are still being worked on. Drones are not a game changer simply because they can destroy military equipment and neutralise the enemy. More relevant is the cost-effect relationship. Drones are relatively low cost and compared to classic precision weapons, i.e. HIMARS or JASSM, equally effective. Their production is less demanding and can be carried out on a mass scale in adventitious ground or in the proverbial garage.

Another important piece of the puzzle is the merging of the worlds of special services and special forces. This can be observed in Ukraine, where both HUR military intelligence and SBU counterintelligence have their combat elements and effectively conduct military special operations. This is why it is important, among other things, for us to participate in special operations conducted by top-level central institutions in order to reduce the potential and operational-strategic capabilities of the adversary on a war-wide scale, not only along the front line. And such action for the benefit of these institutions should be considered the main task for GROM. In the Polish legal area, Special Forces can form task forces with the Military Counterintelligence Service and the Military Intelligence Service, while the possibility of direct cooperation with the Foreign Intelligence Agency (AW), the Internal Security Agency (ABW) and the State Protection Service (SOP) is hindered.

I would like to draw attention to one aspect. One should not delude oneself that the future conflict will be the same as the one across the eastern border of the EU, and try to copy certain solutions one hundred percent. From discussions with our Ukrainian partners, it is clear that warfare is dynamic and techniques, tactics and procedures become outdated very quickly. This sometimes results in changes to tools and procedures even occurring on

a two-week cycle, as I mentioned earlier. This is why it is so important to collect information from the battlefield, analyse it and draw correct conclusions, and then quickly make decisions on what to implement and to what extent.

What in the context of anti-terrorist and counter-terrorist activities, should we reconsider and change at the systemic level in Poland so that law enforcement and military special units can cooperate without hindrance and use their potential in the event of the recognition of terrorist threats and the introduction of a third or fourth alert level?

One could say that at first glance everything works and there is nothing to discuss. After all, we have the Act on anti-terrorist activities, which covers various terrorist incidents and how to respond to them. However when one goes into the details and takes into account the experiences from inter-ministerial exercises, for example the annual Kaper tactical and special exercises, the case is not so optimistic. Above all, there are legal grounds to think about. Although there is a provision in the aforementioned act for the use of Special Forces, the regulations concerning the third or fourth alert level may significantly delay the support of subdivisions of the non-military system (mainly counter-terrorist subdivisions of the Police) by Special Forces. It must be remembered that terrorist attacks are highly dynamic and time is crucial in responding to them, and the statutory provisions mean that it is not possible to act preventively, only reactively. Another problem is that the law does not provide for the management at governmental level of a crisis related to a terrorist action (as in the British model). This is ceded to the ministerial level (abroad, the Ministry of Foreign Affairs is responsible for this) or even to the service level (counter-terrorist actions being the responsibility of the Police). This makes it difficult to use all the resources needed to solve the crisis, as it is often necessary to involve forces subordinate to different ministries. Operating at sea may, for example, require the participation of units subordinate to the Ministry of the Interior, the Ministry of Defence, the Ministry of Foreign Affairs (in the case of territorial waters of a third country), the Ministry of Infrastructure or the Minister Coordinator of Special Services. Another problem is inconsistent legislation. There are laws whose provisions do not

correspond to those in the Anti-terrorism Act. An example is the Act on the Protection of shipping and sea ports, in which the leading role is assigned to the Ministry of Defence. A legal dilemma arises as to which act is superior in such situations. The government body managing the crisis could have a casting vote in this case, as the Prime Minister would be at the head of such a group. Such a solution has been adopted in the UK. Another element worth thinking about is to rehearse, in the form of war games, various potential event scenarios. It needs to be tested whether the system of decision-making and force generation adopted is effective and allows for a sufficiently rapid response appropriate to the dynamics of such a crisis. Who should be involved in such war games? In my opinion, to start with, those who are obliged under current laws to solve the terrorist crisis. Well-run war games based on different scenarios would, in my opinion, provide answers to many questions and dilemmas, and would give arguments for legal and organisational changes. Before the law would be changed, the game could also be implemented in a model target group to ascertain whether the proposed changes are effective and to familiarise the government crisis management group with the procedures for action.

An important element of the Polish anti-terrorist system, which took shape after 11 September 2001, was informal cooperation. Its architects emphasised integrating the activities of state institutions and bodies, building mutual respect and trust. Today, there is a different generation at the helm of the various links of the counter-terrorist community in the Republic of Poland, and we see rivalry between different services and units. Divisions were, are and will be there, but the point is to build security beyond them. How do we maintain the unity of nearly 30 operational and tactical level entities?

Very interesting and difficult question. There is no denying it – there are people with strong characters, alpha personalities serving in the force institutions that deal with the broader security of the state, and this certainly presents a challenge in terms of building security across divisions. At the command of the GROM Military Unit, we always emphasise that it is not about who is the best and who will do the job. The most important thing is that we all have a common

goal, which is to provide a safe environment for the development of the country and a sense of security for Polish citizens, both those inside and outside the country. If we all understand this, it will be good, and if we are guided by it in action, it will be very good. We must also remember that our capacity to respond is, on the one hand, fragmented, and on the other hand, sufficient. What I mean by this is that, for example, the Polish Armed Forces have greater potential in the area of aircraft or maritime capabilities, and the Police and the Border Guard can activate their formations more quickly in the event of an immediate need for such force generation. In turn, the special services, i.e. ABW, AW, SKW and SWW, have the knowledge and capabilities to carry out operations. It is economically unjustifiable to develop and maintain capabilities that have already been developed in another ministry, but close and multifaceted cooperation as well as a comprehensive and well-coordinated approach to emerging threats with competences and dependencies defined, are necessary. Another important element in building security is continuous, mutual inter-ministerial education – whether in the form of conferences and working meetings or exercises. Firstly, this will allow you to make and maintain contacts, i.e. networking, and secondly to keep you up to date with who and what you have. This always raises the question of who should organise this. Ministries, commands or individuals? Let me answer simply – anyone who cares about security. At GROM we teach not to be passive and not to wait for someone to do something for us, but to take responsibility and look for solutions if we see that the system does not yet recognise the problem. Hence the emphasis on creativity that I mentioned earlier.

The last and perhaps most controversial proposal is to organise exercises in the form of so-called stress testing, or overload testing. Their scenario is designed to continually subject practitioners to extreme situations. This leads to the system being overloaded and failing. We know from experience that such failures are like a bucket of cold water. It has positive effects and it fosters creative solutions when the practitioners encounter a similar situations in the future.

He was talking: Damian Szlachter

studies
analyses
prevention

TERRORISM

special edition

Terrorist and sabotage threats to critical infrastructure

The issue includes:

- **The use of critical infrastructure in hybrid conflicts**
Case studies of attacks on CI. Building CI resilience using the example of CER and NIS 2 Directives.

- **Hybrid threats in Europe**
Russian operations in EU countries in the light of the analyses of European Centre of Excellence for Countering Hybrid Threats – Hybrid CoE.

- **The importance of the Baltic Sea for the energy security of the countries of the Baltic region**
Threats to CI facilities in the Baltic Sea and port infrastructure. Opportunities for counteraction.

- **Ukrainian infrastructure as a target of hybrid and conventional war**
Russian operations against Ukraine's CI. Tactics, weapons, resilience and defence – lessons from the Ukrainian experience.

- **EU cyberspace as a domain of hybrid activities**
Current threats in European cyberspace from state-sponsored, hacktivist and cybercriminal groups.

- **Protection of critical infrastructure from unmanned aerial vehicles**
Assessment of unmanned aerial vehicles detection and neutralisation systems. Legal changes

For more, see:
https://abw.gov.pl/pub/terrorism-studies-analyses-pre/15,Intro.html

The issue was prepared under the aegis of the Internal Security Agency and the Government Centre for Security as part of the Polish Presidency of the Council of the EU.

RCB