TERRORISM

studies
analyses
prevention

TERRORISM
PREVENTION
Centre of Excellence

CPS CENTRALNY OŚRODEK SZKOLENIA I EDUKACJI ABW

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

Translation Agencja Bezpieczeństwa Wewnętrznego

Cover design Aleksandra Bednarczyk

ISSN 2720-4383
e-ISSN 2720-6351

Articles published in the journal are peer-reviewed

Articles express the views of the authors

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

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

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

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

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

Printed in September 2022.

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

TABLE OF CONTENTS

Ladies and Gentlemen!

On 26 April 2022, the inauguration ceremony of the new scientific periodical "Terrorism - studies, analyses, prevention" (T-SAP) took place at the Central Training and Education Facility of Internal Security Agency. It was attended by representatives of analytical centres (Polish Institute of International Affairs, Centre for Eastern Studies, Western Institute), academia, state administration and uniformed services forming the anti-terrorist system of the Republic of Poland.

The meeting was opened by the Head of the Internal Security Agency, Colonel Krzysztof Wacławek, who spoke about the new publishing initiative of the Internal Security Agency. After the speakers' speeches, the participants were asked to take part in an anonymous survey. Its purpose was to obtain answers to questions on the perception of the phenomenon of terrorism and to identify the most likely directions of development of terrorist threats in the Republic of Poland. Such a survey was conducted in Poland for the first time and its results, are included in this issue of the periodical.

We plan to carry out surveys on a regular basis. We hope that the data obtained in this way will provide substantive support in the discussion on the directions and variants of the development of the anti-terrorist system in the Republic of Poland and in the construction of international initiatives in this field. Such authorial projects of a research and scientific character will therefore be constantly present in the pages of T-SAP, so that the scientific journal of the Internal Security Agency can fulfil its mission of strengthening cooperation between various communities involved in activities for anti-terrorist protection.

In the second issue of the periodical, you will find articles devoted to, among other things: the tasks of legal protection authorities in combating terrorism in Poland, the role of alert levels in the anti-terrorist system, the financing of terrorism in a historical perspective, possible scenarios for the development of terrorist threats in the context of the war in

Ukraine, as well as a case study of the perpetrator of the terrorist attacks on the Norwegian island of Utøya. It also includes a review of Tomasz Aleksandrowicz's newly published book on methods of forecasting terrorist threats.

Inviting you to read the second issue of the journal "Terrorism - studies, analyses, prevention", I hope that the materials presented in its pages will meet with your interest and will be an important contribution to the public discussion on building the resilience of the Polish society to terrorist threats.

Editor-in-Chief
Damian Szlachter, PhD

DOI: 10.4467/27204383TER.22.024.16344

ORCID: 0000-0002-6685-8769

PIOTR BURCZANIUK

Tasks and powers of criminal law enforcement authorities in combating terrorism in Poland - a legal perspective

Abstract

This paper presents the tasks and powers of the law enforcement authorities in Poland in the area of combating terrorism from a legal perspective. Despite the vast amount of literature on this subject, this topic is still interesting, in particular due to the lack of comprehensive yet concise works presenting the tasks of the abovementioned authorities from the perspective of four phases of anti-terrorist activities. These phases consist of both actions of preventive nature, coordinated by the Head of the Internal Security Agency (ABW), and actions carried out to take control of terrorist incidents, ensure response and restore the resources necessary to take control of such incidents, coordinated by the Minister of the Interior and Administration.

The problems referred to above are presented from the perspective of the Polish system of combating terrorism. This paper analyses both its institutional scope, by indicating the authorities forming part of the system, and its material scope, by characterising procedures of anti-terrorist actions according to which the competent authorities carry out their tasks.

This paper attempts to analyse these issues comprehensively and briefly. Furthermore, the considerations are supported by an empirical study of experiences accumulated since the Act of 10 June 2016 on anti-terrorist activities came into force.

Keywords:

Polish anti-terrorist legislation, the Act on anti-terrorist activities, the Internal Security Agency, the Minister of the Interior and Administration

As indicated in the legal doctrine, (...) *the group of extra-constitutional law protection bodies should include the prosecutor's office and other criminal prosecution bodies. They correspond to the criteria of a law enforcement body and find full statutory support.* (...) *The group of extra-constitutional law enforcement bodies includes numerous law enforcement bodies of ministerial, military and administrative provenience*[1]. This study analyses the tasks and powers of these bodies in the field of combating terrorism in Poland. The starting point and the axis binding these considerations is the analyses of the provisions of the Act of 10 June 2016 on anti-terrorist activities[2], which entered into force on 2 July 2016. It is in this act, as indicated in its Article 1, that the principles of conducting anti-terrorist activities and cooperation between the competent authorities in the implementation of these activities are set out, thus creating a *de jure* anti-terrorist system in Poland.

It is worth starting by emphasising that the aforementioned act materialised both the postulates of the legal doctrine and the conclusions of the analyses conducted since the beginning of the 21st century in the area of security sciences, assuming the necessity of the existence of such an act (...) *not only because the threat of terrorism in Poland is, in comparison with many European countries, significantly higher, but also because anti-terrorist activities of state authorities and other institutions have to encroach on the sphere of civil liberties and rights, which is an issue having a clear constitutional, convention (European Convention of 1950) and EU context*[3]. Moreover, it was then added that:

> (...) Poland still lacks a national document, which would define for the uniformed services and civil institutions involved in counter-terrorism, the framework and limits of actions taken, and would indicate what "state" we are aiming at and with what acceptable means, consistent with the generally accepted strategy of state action, we want to achieve it. There is also a lack of a mechanism with a clear decision-making centre, which would bring together all the necessary areas into one integrated, supra-ministerial and national counter-terrorism system[4].

---

1 F. Prusak, *Niesądowe organy ochrony prawnej* (Eng. Non-judicial legal protection bodies) Warszawa 2004, p. 83.

2 Consolidated text: Journal of Laws of 2021, item 2234, as amended.

3 L. Paprzycki, *Czy Polsce potrzebna jest ustawa antyterrorystyczna?* (Eng. Does Poland need an anti-terrorist law?), in: *Terroryzm. Materia ustawowa?* (Eng. Terrorism. Statutory matter?), K. Indecki, P. Potejko (eds.), Warszawa 2009, p. 6.

4 M. Adamczuk, P. Siejczuk, *Strategia obrony przed terroryzmem – cele i funkcje w systemie przeciwdziałania terroryzmowi* (Eng. Strategy for defence against terrorism - objectives

Despite such clearly formulated postulates and multi-stage organisational activities aimed at creating an anti-terrorist system in Poland, carried out mainly within the framework of the works of the Interministerial Team for Terrorist Threats[5], it was not until the Act of 10 June 2016 on anti-terrorist activities led to the formal establishment of this system and at the same time it precisely defined e.g. tasks and obligations of criminal law enforcement bodies in this respect. As it was indicated in the justification to the draft of this act, its basic objective was (...) *to increase the effectiveness of the Polish anti-terrorist system, thus increasing the security of all citizens of the Republic of Poland*[6]. This was to be achieved, inter alia, by strengthening the mechanisms for the coordination of activities, clarifying the tasks of individual services and bodies and the principles of cooperation between them. During legislative work, it was pointed out that existing legislation on combating terrorism is dispersed and does not provide adequate legal and organisational instruments to effectively counteract existing threats. The new regulation was intended to integrate the activities of the criminal law enforcement authorities competent in the field of counter-terrorism and to clearly outline their responsibilities for the various segments of these activities. In this way, it was to directly affect (...) *the speed and correctness of decision-making at the strategic level*[7].

The Act of 10 June 2016 on anti-terrorist activities was structurally divided into seven chapters[8], while the foundation of the solutions contained therein was based on four separate phases of undertaking anti-terrorist activities. They consist of: 1) activities preventing terrorist

and functions in the counter-terrorism system), in: *Problemy prawno-organizacyjne zwalczania terroryzmu w Polsce* (Eng. Legal and organisational problems of combating terrorism in Poland), J. Szafrański, K. Liedel (eds.), Szczytno 2011, p. 91.

5 For more on the origins of the anti-terrorist system in Poland see P. Chomentowski, *Polski system antyterrorystyczny. Prawno-organizacyjne kierunki ewolucji* (Eng. Polish anti-terrorist system. Legal and organisational directions of evolution), Warszawa 2014, pp. 81–95; M. Cichomski, I. Idzikowska-Ślęzak, *Strategic level of the Polish anti-terrorist system - 15 years of the Interministerial Team for Terrorist Threats*, "Terroryzm – studia, analizy, prewencja" 2022, no. 1, pp. 297-319.

6 Government draft law on anti-terrorist activities and amendments to some other laws, print no. 516, https://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=516 [accessed: 25 IV 2022].

7 Ibid.

8 For more on the regulatory scope of the act, see P. Burczaniuk, *Legal aspects of combating terrorism in the Polish legal system against the background of challenges shaped by European legislation*, "Terroryzm – studia, analizy, prewencja" 2022, no. 1, pp. 273-279.

events - entrusted to the Head of the Internal Security Agency; 2) preparation to take control over terrorist events by means of planned undertakings; 3) reaction in case of occurrence of such events; 4) recovery of resources intended for response to such events - entrusted to the minister in charge of internal affairs. The division into the mentioned phases emphasises the convergence of the anti-terrorist system established by this act with the system from which it de facto evolved, i.e. the crisis management system specified in the Act on crisis management of 26 April 2007[9]. In this act, the mentioned phases were treated in a non-identical manner. Two phases have been brought to the fore - activities preventing events (regulated in Chapter 2) and undertaking counter-terrorist activities (regulated in Chapter 4). The great value of this act, as Piotr Chorbot points out, is that (...) *until the enactment of this Act there had not been such an unambiguous separation of competency responsibilities in the context of counter-terrorism issues*[10].

The Act of 10 June 2016 on anti-terrorist activities, currently the most important act from the point of view of considerations concerning the tasks of criminal law enforcement bodies in the field of combating terrorism, is supplemented by sectoral regulations, especially those covered by the competence provisions of individual services and bodies. Without taking them into account, the considerations subject to this study would not be complete.

It should also be noted that, in a broad sense, the tasks and powers of criminal law enforcement bodies in the field of combating terrorism in Poland derive from the Act of 1 March 2018 on counteracting money laundering and financing of terrorism[11], establishing mechanisms for counteracting terrorism financing, as well as from regulations devoted to states of emergency, which, due to the volume limitations of this study, will not be discussed in more detail.

---

[9] Consolidated text: Journal of Laws of 2022, item 261, as amended.

[10] P. Chorbot, *Ustawa o działaniach antyterrorystycznych. Komentarz do niektórych regulacji* (Eng. the Act of 10 June 2016 on anti-terrorist activities. Commentary to some regulations), in: *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia* (Eng. Powers of special services from the perspective of contemporary threats to national security. Selected issues), P. Burczaniuk (ed.), Warszawa 2017, p. 68.

[11] Consolidated text: Journal of Laws of 2022, item 593, as amended.

Measures to prevent incidents of a terrorist nature

Special position of the Head of the ABW

Pursuant to Article 3(1) of the Act of 10 June 2016 on anti-terrorist activities, the Head of the ABW is responsible for the prevention of terrorist events. The choice by the legislator of the Head of the ABW as the coordinator of activities of criminal law enforcement bodies in the phase of prevention of terrorist events appears to be obvious, primarily in the light of the competence provisions of the Internal Security Agency, the experience of that service, as well as its organisational capabilities in that area, related mainly to the units functioning within its structure - the Counter-Terrorism Centre (CAT) and the Terrorism Prevention Centre of Exellence (TP CoE).

Referring to the competences of the ABW, it should be pointed out that, pursuant to Article 5 sec. 1 item 1 and 2 letter a of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency[12], the Agency's tasks include the identification and combating of threats to the internal security of the state and its constitutional order and the prevention of such threats, as well as the identification, detection and prevention of crimes, especially terrorism. As Magdalena Gołaszewska underlines, (...) *as an element of a threat to internal security one should undoubtedly also qualify the recognition of issues related to terrorist activity*[13]. In turn, Tomasz Batory indicates that (...) *the offence covered by art. 5 sec. 1 item 2 letter a of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency is terrorism. However, unlike in the case of espionage, this concept does not refer to a single article of the Criminal Code. It is worth noting that the Code does not use the nomenclature "terrorism", but the concept of "terrorist offence". The definition of this concept is contained in Article 115 § 20 of the Criminal Code*[14].

[12] Consolidated text: Journal of Laws of 2022, item 557, as amended.

[13] M. Gołaszewska, *Zadania ABW w zakresie zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa i jego porządek konstytucyjny* (Eng. Tasks of the ABW in combating threats to the state's internal security and constitutional order), in: *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego* (Eng. Legal aspects of the functioning of special services on the example of the Internal Security Agency), P. Burczaniuk (ed.), Warszawa 2021, p. 46.

[14] T. Batory, *Zadania ABW w zakresie rozpoznawania, zapobiegania i wykrywania przestępstw* (Eng. Tasks of the ABW in the area of identification, prevention and detection of offences), in: *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa*

The competence of the ABW expressed in this way means that among all Polish criminal law enforcement bodies, it is this service that has the broadest competence in the fight against terrorism. This is, moreover, a characteristic feature of European special services of an internal character, which as a rule are tasked with espionage and terrorism. In the context of the above, it should be noted that the legal predecessor of the ABW, namely the State Protection Office (Urząd Ochrony Państwa), since its establishment on 10 May 1990, in line with Article 2 sec. 2 item 1 and 2 of the Act of 6 April 1990 on the State Protection Office[15], had tasks in the area of identification of threats threatening, inter alia, the security of the country (which undoubtedly included terrorist threats) and counteracting them, as well as - explicitly expressed - tasks in the area of detection and prevention of crimes, inter alia terrorism.

The Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency in Article 21 sec. 1 specifies that the tasks of the ABW indicated in Article 5, including those aimed at combating terrorism, are performed by ABW officers:

1) at the level of identification and elimination of threats - operational and reconnaissance as well as analytical and information activities in order to obtain and process information vital for the protection of the state security and its constitutional order;
2) at the level of combating offences - operational and reconnaissance activities as well as investigative and prosecutorial activities aimed at recognising, detecting and preventing offences and prosecuting their perpetrators.

These powers have been presented in detail in chapter 4 of the the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency. It is worth noting that in the Act of 10 June 2016 on anti-terrorist activities the powers of the ABW in the scope of anti-terrorist activities preventing terrorist incidents have been specified. Analyses of the scope of these powers allows us to argue that in this phase of the fight against terrorism, the legislator has placed the greatest emphasis on the importance of analytical and informational as well as operational and reconnaissance activities. This should be assessed as a rational action, because in this phase,

Wewnętrznego (Eng. Legal aspects of the functioning of special services on the example of the Internal Security Agency), P. Burczaniuk (ed.), Warszawa 2021, p. 73.

[15] Journal of Laws of 1990, No. 30, item 180.

the services are mainly confronted with terrorist threats, and not with crimes (apart from preparatory or attempted criminal activities), which in turn are dominant in the next phase, associated with the occurrence of an event of a terrorist nature.

In the case of analytical and information activities, the legislator emphasised the importance of the exchange of information, its aggregation and further distribution. He has imposed tasks on the Head of the ABW in the scope of:

1) coordination of analytical and information activities undertaken by special services (in the meaning of Article 11 of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency) - Article 5 sec. 1 of the act;
2) coordination of the exchange of information provided by the Police, Border Guard, Marshal's Guard, State Protection Service, State Fire Service, General Inspector of Financial Information, National Revenue Administration, Military Police and the Government Security Centre, concerning:
   a) events of a terrorist nature (defined in Article 2 item 7 of the act as a situation suspected to have arisen as a result of a terrorist offence referred to in Article 115 § 20 of the Act of 6 June 1997 - Criminal Code, or a threat of such an offence occurring),
   b) data on persons:
      – undertaking activities for terrorist organisations or organisations connected with terrorist activities or members of such organisations,
      – wanted, conducting terrorist activity or persons suspected of committing crimes of a terrorist nature, with regard to whom in the Republic of Poland a detention order or a decision on searching with a letter of appointment has been issued, as well as persons wanted on the basis of the European arrest warrant,
      – in relation to whom there is a justified suspicion that they may carry out activities with a view to committing a terrorist offence, including persons posing a threat to the security of civil aviation,
      – participating in terrorist training or travelling to commit a terrorist offence,

by collecting, processing and analysing this information - Article 5(1) of the act. The data on the indicated persons are also subject to entry in the register kept by the Head of the ABW, pursuant to Article 6 section 1 of the act, created in compliance with the requirements concerning the protection of classified information;

3) receiving, from the special services and the entities indicated above, information serving the performance of anti-terrorist activities (defined as activities of public administration bodies consisting in the prevention of terrorist events, preparation to take control over them by means of planned undertakings, reaction in the event of occurrence of such events and removal of their consequences, including restoration of resources intended for response to them). The information has to be provided as classified in one of the incidents defined as a catalogue in a regulation issued by the minister in charge of internal affairs, in consultation with the minister in charge of public finance and the minister of national defence and after consulting the Head of the ABW[16]. The list currently includes 12 incidents grouped into two areas, i.e. incidents threatening the security of the Republic of Poland and incidents related to foreign representations of the Republic of Poland and citizens of the Republic of Poland outside its territory - Article 5, section 3 of the act;
4) collecting information from public administration authorities, owners and possessors of facilities, installations, equipment of public administration infrastructure or critical infrastructure in their possession concerning threats of a terrorist nature to the infrastructure of public administration or critical infrastructure, including threats to the functioning of energy, water and sewage systems and networks, as well as heating and telecommunication systems and networks important from the point of view of national security - Article 4, section 2 of the act;
5) free-of-charge access to data collected in public registers and records maintained both by participants in the anti-terrorist system indicated above in items 1 and 2, as well as by

[16] Currently it is the Ordinance of the Minister of the Interior and Administration of 22 July 2016 on the catalogue of terrorist incidents (Journal of Laws of 2017, item 1517 and Ordinance of the Minister of the Interior and Administration of 5 February 2019 amending the Ordinance on the catalogue of terrorist incidents, Journal of Laws of 2019, item 317).

ministers in charge of government administration departments, the Head of the Office for Foreigners, the President of the Office of Electronic Communications, the President of the Civil Aviation Authority, the President of the State Atomic Energy Agency, the Social Insurance Institution (ZUS), the President of the Agricultural Social Insurance Fund (KRUS), the Financial Supervision Authority, the Chief Geodesist of the Country, local government units, the Public Prosecutor General and organisational units subordinate to them or supervised by them - Article 11 item 1 of the act.

Importantly, the act on the one hand establishes the Head of the ABW as the authority authorised to receive and aggregate information, and on the other hand makes him the source of its distribution. Information is provided:

1) pursuant to Article 7 of the act - for the needs of the most important state bodies. The Head of the ABW is obliged to immediately forward information which may be crucial for the prevention of terrorist events to the President of the Republic of Poland, the Prime Minister, the minister in charge of internal affairs, the Minister of National Defence, the minister in charge of foreign affairs, the Minister Coordinator of Special Services, if appointed[17];
2) pursuant to Article 6 sec. 2 of the act - for the needs of other special services and the mentioned participants of the anti-terrorist system (the Police, Border Guard, the Marshal's Guard, the State Protection Service, the State Fire Service, the General Inspector of Financial Information, the National Revenue Administration,

[17] The scope of normative provisions covering, in Article 7 of the act, "information which may be of significant importance for the prevention of terrorist events" and prescribing the adequate application of Article 18 of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency differs significantly from the scope of normative provisions of Article 6 sec. 3 of the act, which refers to "information serving the implementation of anti-terrorist measures". Given the specific scope of application of Article 7, which covers the most important state bodies, this argues for its interpretation and application in a wide range, covering, inter alia, information covered by certain prohibitions. Considerations concerning the correlation of Article 18 and Article 39 par. 3 of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency, undertaken in: P. Burczaniuk, *Zadania Szefa ABW w zakresie obowiązków infor= macyjnych* (Eng. Tasks of the Head of the ABW with regard to information obligations), in: *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego* (Eng. Legal aspects of the functioning of special services on the example of the Internal Security Agency), P. Burczaniuk (ed.), Warszawa 2021, pp. 17–39.

the Military Police and the Government Centre for Security), as well as other public administration bodies, within the scope of their competence. This information (also in the form of current analyses of the state of the threat of a terrorist event)
   a) for the implementation of anti-terrorist activities, classified in line with the catalogue of terrorist incidents,
   b) included in the list of persons;
3) pursuant to Article 4, section 1 of the act - to public administration bodies, owners and holders of objects, installations, devices of public administration infrastructure or critical infrastructure. This is information necessary to prevent the occurrence of an event of a terrorist nature threatening public administration infrastructure or critical infrastructure, life or health of people, property of significant size, national heritage or the environment, to remove such a threat or to minimise it.

It should be added that, pursuant to Article 4 sec. 3 of the act, in the event of obtaining information on a possible terrorist incident threatening the public administration infrastructure or critical infrastructure, human life or health, property of considerable size, national heritage or the environment, the Head of the ABW has the right to issue instructions to the authorities and entities indicated above in item 3 (excluding the most important persons in the country) in order to counteract such threats, remove them or minimise them. The bodies and entities are obliged to inform the Head of ABW about the actions taken in this respect. The above-mentioned authority of the Head of the ABW was implemented into the anti-terrorist system from the crisis management system, namely in Article 12a of the aforementioned Act of 26 April 2007 on crisis management, in effect from September 2009[18] until the Act of 10 June 2016 on anti-terrorist activities enters into force.

In the case of operational and reconnaissance activities, pursuant to Article 8 of the act, the Head of the ABW was entrusted with their coordination within the subject scope, when these activities are undertaken by special services, the Police, the Border Guard, the National Revenue Administration and the Military Police, and within the subject scope, when they relate to events of a terrorist nature. The only statutory specification

[18] Added by the Act of 17 July 2009 amending the Act on crisis management (Journal of Laws of 2009, No. 131, item 1076).

of this task is the power granted to the Head of the ABW to issue recommendations to the aforementioned entities with a view to eliminating or minimising the terrorist threat. As Michał Gabriel-Węglowski points out, (...) *a question arises as to the binding character of these recommendations.* (...) *However, the leading role of the Internal Security Agency in counteracting a terrorist threat, resulting from this act, supports the assumption that the issued recommendations always require implementation by the remaining services*[19]. Moreover, from the very coordinating function performed by the Head of the ABW, a conclusion may be drawn about the obligation of the listed entities to inform him about the intention and conduct of operational and reconnaissance activities with regard to terrorist events. The lack of such information would make it functionally impossible for the Head of the ABW to fulfil the coordination task assigned to him, including issuing the discussed recommendations. By the way, it is worth noting that, as part of the solutions concerning operational and reconnaissance activities, the act has given the Head of the ABW two new powers:

1) conducting surveillance activities with regard to foreigners[20] - Article 9 of the act;
2) accessing images of events recorded by image-recording devices placed in public facilities, along public roads and other public places and receiving, free of charge, a copy of the recorded image - Article 11, item 2 of the act.

Moreover, the Act of 10 June 2016 on anti-terrorist activities introduced many comprehensive amendments to the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency, the aim of which was to enhance the state's capability to prevent terrorist threats, and which constitute the sphere of basic responsibility of the ABW, including, inter alia, the power to:

1) secret cooperation with the ABW of a perpetrator of a crime of espionage or a suspect of a crime of a terrorist nature - Article 22b of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency;

[19] M. Gabriel-Węglowski, *Działania antyterrorystyczne. Komentarz* (Eng. Anti-terrorist activities. A commentary), Article 8, Warszawa 2018, https://sip.lex.pl/#/commentary/-587754148/551588/gabriel-weglowski-michal-dzialania-antyterrorystyczne-komentarz?cm=URELATIONS [accessed: 28 IV 2022].

[20] Detailed considerations concerning this power remain outside the thematic scope of this study. See in more detail: M. Gabriel-Węglowski, *Działania antyterrorystyczne. Komentarz*...

2) assess the security of IT systems in order to prevent and counteract terrorist incidents and to combat them - Article 32a of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency;
3) provide, at the request of the Head of the ABW, information on the construction, functioning and principles of operation of ICT systems in the event of obtaining information on the occurrence of an event of a terrorist nature involving these systems - Article 32b of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency;
4) block by the ABW the availability in the ICT system of specific IT data or ICT services connected with an event of a terrorist nature - Article 32c of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency.

As it follows from the above, the act on anti-terrorist activities made the Head of the ABW responsible for the prevention of terrorist events and provided him with two basic powers to perform this task in the form of a coordinating function over analytical, informational and operational-reconnaissance activities undertaken in this area. As it has already been pointed out, the legislator's choice of the Head of the ABW to perform this task was an obvious one, also due to his over-30-years' experience (taking into account the period of functioning of the UOP), which is currently used mainly by the two already mentioned organisational units of the ABW, i.e. the CAT and the TP CoE.

The Counter-Terrorism Centre is responsible for coordinating the activities of entities responsible for counter-terrorist protection in Poland. Hence, it seems that not only officers of the ABW, but also representatives of other participants in the anti-terrorist system of Poland are on duty at the CAT. Article 14 of the Act of 10 June 2016 on anti-terrorist activities and executive acts issued on its basis create an organisational system, on which, in practical terms, the operations of the CAT and the coordinating role of the Head of the ABW are based. It boils down to the possibility of delegating representatives of other special services, as well as the Police, the Border Guard, the Marshal's Guard, the State Protection Service, the State Fire Service, the General Inspector of Financial Information, the National Revenue Administration, the Military Police and the Government Centre for Security to serve or work in the ABW. These persons perform (...) *tasks within the competence of the institution which they*

represent[21]. The choice of these entities by the legislator is not accidental, as they undoubtedly constitute elements of the anti-terrorist system of the Republic of Poland, in which each of them, within the scope of its competence and taking into account the coordinating role of the Head of the ABW, performs tasks aimed at counteracting terrorism.

The importance of other services

Counter-terrorist tasks, in the scope similar to those of the ABW, have been entrusted to the Foreign Intelligence Agency which, pursuant to Article 6 sec. 1 item 5 and 7a of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency, identifies, inter alia, international terrorism and extremism as well as identifies, prevents and counteracts terrorist incidents against citizens or property of the Republic of Poland outside its borders, with the exception of terrorist incidents against the personnel or property of the Armed Forces of the Republic of Poland, however it performs these tasks outside the borders of the Republic of Poland.

Counter-terrorist tasks are also performed by other special services, including the Military Counterintelligence Service. In accordance with Article 5 sec. 1 item 2a of the Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service[22], the Military Counterintelligence Service identifies, detects and prevents events and offences of a terrorist nature endangering the security of the state's defence potential, the Armed Forces of the Republic of Poland and organisational units of the Ministry of Defence. In turn, the Military Intelligence Service, similarly to the Foreign Intelligence Agency, pursuant to Article 6, section 1, item 2, letter b and item 3a of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency, deals with the identification of threats of international terrorism and counteracting them as well as the identification of terrorist incidents against the personnel and property of the Armed Forces of the Republic of Poland outside the borders of the state, counteracting and preventing these incidents and combating their effects.

[21] Service of the Republic of Poland gov.pl, Counter-Terrorism Centre (CAT ABW), https://www.gov.pl/web/mswia/abw [accessed: 27 IV 2022].

[22] Consolidated text: Journal of Laws of 2022, item 502, as amended.

For the functioning of the anti-terrorist system in Poland the tasks in the field of counter-terrorism assigned to the Police, which - as emphasised in the legal doctrine[23] - in the phase of prevention of terrorist events are not directly mentioned in the Act of 6 April 1990 on the Police[24]. However, they can be deduced from the wording of Article 1(2)(1)-(3) of this act, which indicates that the basic tasks of the Police include:

1) protection of human life and health and property against unlawful attempts infringing these goods;
2) protection of public safety and order, including ensuring calm in public places and in means of public transport and communication, in road traffic and on waters intended for common use;
3) initiating and organising activities aimed at preventing the commission of offences and misdemeanours as well as criminogenic phenomena and cooperating in this respect with state and local government bodies and social organisations.

In the system in question the legislator assigned an important place also to the Border Guard whose counter-terrorist tasks, similarly as in the case of the Police, are not expressed directly, but functionally result from the role this formation plays in protecting the state border, controlling border traffic and preventing and counteracting illegal migration (Article 1 sec. 1 of the Act of 12 October 1990 on the Border Guard[25]). Pursuant to Article 1(2)(5d) of the act, the Border Guard is obliged to cooperate with other authorities and services in identifying and counteracting threats of terrorism.

The State Protection Service is also an important element of the anti-terrorist system in Poland, despite - as in the case of the Police and the Border Guard - the lack of explicitly expressed statutory competence, due to its general competence which boils down to the protection of persons and objects and the recognition and prevention of crimes directed against them (Article 2(1) of the Act of 8 December 2017 on the State Protection Service[26]). A similar role in this system is played by the Marshal's Guard, which

[23] Cf. M. Gabriel-Węglowski, *Działania antyterrorystyczne. Komentarz*...

[24] Consolidated text: Journal of Laws of 2021, item 1882, as amended.

[25] Consolidated text: Journal of Laws of 2022, item 1061, as amended.

[26] Consolidated text: Journal of Laws of 2021, item 575, as amended.

performs tasks with regard to the protection of the Sejm and the Senate (Article 1(1) of the Act of 26 January 2018 on the Marshal's Guard[27]).

Actions under the responsibility of the Minister of Interior and Administration

As mentioned earlier, pursuant to Article 3(2) of the act on anti-terrorist activities, the minister in charge of internal affairs is responsible for three out of four phases of undertaking anti-terrorist activities, i.e. preparation for taking control over terrorist events by means of planned undertakings, response in the event of occurrence of such events and restoration of resources intended for responding to such events.

In the legal doctrine it is indicated that (...) *one of the most significant solutions of the Act of 10 June 2016 on anti-terrorist activities, from the perspective of preparing to take control over events of a terrorist nature and responding in the event of the occurrence of such events, was the transfer of the institution of alert levels and CRP alert levels to the act*[28]. In turn, the foundation of the response phase became the solutions included in chapter 4 of the act, devoted to actions on the scene of a terrorist event, including counter-terrorist actions. The most important for this chapter Article 18 determines the manner of designation of the leader of counter-terrorist activities on the scene of a terrorist incident, undertaken by competent services or authorities within the framework of their statutory tasks. In principle, the person in charge is appointed by the Commander-in-Chief of the Police. In the event that such an event occurs on areas or in facilities belonging to the Minister of National Defence, supervised or administered by him, the in-charge is appointed by that Minister. In eight

[27] Consolidated text: Journal of Laws of 2019, item 1940, as amended.

[28] See in more detail: M. Cichomski, M. Horoszko, I. Idzikowska, *Przygotowanie do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym oraz reagowanie w przypadku wystąpienia takich zdarzeń w świetle rozwiązania ustawy o działaniach antyterrorystycznych – w kontekście zadań resortu spraw wewnętrznych* (Eng. Preparing to take control over terrorist events and reacting in case of such events in the light of the solution of the act on anti-terrorist activities - in the context of the tasks of the ministry of internal affairs), in: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem* (Eng. Polish Act on anti-terrorist activities - a response to the threat of contemporary terrorism), W. Zubrzycki, K. Jałoszyński, A. Babiński (eds.), Szczytno 2016, p. 283.

points contained in Article 20 sec. 1 of the act the powers of the person in charge of counter-terrorist operations were defined.

It is clear from the presented regulations that the coordination tasks in these three phases entrusted to the Minister of the Interior and Administration may be performed by him through entities subordinate to him or supervised by him, the list of which is specified in the Ordinance of the Prime Minister of 18 November 2019 on the detailed scope of activities of the Minister of the Interior and Administration[29]. They include: Commander-in-Chief of the Police, Commander-in-Chief of the Border Guard, Commander-in-Chief of the State Fire Service, Commander-in-Chief of the State Protection Service, Head of the National Civil Defence, Head of the Office for Foreigners, Inspector of Internal Supervision (and the Director of the Pension Fund of the Ministry of Internal Affairs and Administration, who does not participate in the anti-terrorist system due to the scope of his tasks).

In this context it should be pointed out that by means of the Act of 10 June 2016 on anti-terrorist activities the legislator amended the competence acts of the indicated services and strengthened their powers necessary to perform these tasks[30]. Undoubtedly, the Police remain the most important service in this respect. In accordance with Article 1, section 2, item 3a of the Act of 6 April 1990 on the Police one of the basic tasks of this uniformed formation is to carry out counter-terrorist activities within the meaning of the Act of 10 June 2016 on anti-terrorist activities. By the way, it should be mentioned that on 5 April 2019 a counter-terrorist service was separated in the composition of the Police[31], at the same time specifying it in Article 5c of the Act of 6 April 1990 on the Police. According to this regulation, the counter-terrorist service of the Police consists of the Central Counter-Terrorist Subdivision of the Police (BOA) and independent counter-terrorist subdivisions of the Police, which are

[29] Journal of Laws of 2019, item 2264.

[30] Amendments were introduced in: Act of 6 April 1990 on the Police, Act of 12 October 1990 on the Border Guard, Act of 24 August 1991 on fire protection (i.e. Journal of Laws of 2021, item 869, as amended – with regard to the organisation of the national rescue and firefighting system), Act of 16 March 2001 on the Government Protection Bureau (amendments were consolidated in the Act of 8 December 2017 on the State Protection Service).

[31] Act of 9 November 2018 amending the Act on the Police and certain other acts (Journal of Laws of 2019, item 15). Previously, counter-terrorist subdivisions were part of the Police (from the entry into force of the Police Act on 10 May 1990 until 12 October 1995).

responsible for conducting counter-terrorist activities and supporting the activities of the organisational units of the Police in conditions of special threat or requiring the use of specialised forces and means and specialised tactics of operation. In view of the discussed importance of the Police for the performance of tasks in the scope of directing anti-terrorist actions on the site of a terrorist incident it is worth adding that the Act of 10 June 2016 on anti-terrorist activities has provided for the possibility of using for assistance of the Police divisions and subdivisions of the Armed Forces of the Republic of Poland in the event of introducing the third or fourth alert level and only in a situation where the use of the Police divisions and subdivisions proves to be insufficient or may turn out to be insufficient. Not without significance in this context is the entitlement, provided for in Article 23 of the act, to the special use of weapons during counter-terrorist operations. It constitutes a derogation from the principles of using firearms regulated in the Act of 24 May 2013 on means of direct coercion and firearms[32], consisting in its use against a person carrying out an attack or taking or holding a hostage, which may result in death or a direct threat to the life or health of that person.

The Act of 10 June 2016 on anti-terrorist activities regulated separately the issue of coordination of the actions of services and bodies in the event of a terrorist incident outside the borders of the Republic of Poland. It was entrusted to the minister in charge of foreign affairs, in cooperation with the Minister Coordinator of Special Services, and if the incident was directed against the personnel or property of the Polish Armed Forces, then to the Minister of National Defence, in cooperation with the minister in charge of foreign affairs (Article 19 of the act). The act also allowed conducting anti-terrorist activities on the principles specified therein outside the borders of the Republic of Poland, in the waters of the Polish SAR area of responsibility, pursuant to the International Convention on Maritime Search and Rescue, drawn up in Hamburg on 27 April 1979[33].

[32] Consolidated text: Journal of Laws of 2022, item 1416.

[33] Journal of Laws of 1988, No. 27, item 184.

Prosecution and preparatory proceedings

An important element of the solutions provided for in the Act of 10 June 2016 on anti-terrorist activities are special provisions concerning preparatory proceedings. As Wojciech Olsztyn points out, (...) *so far all procedural activities have been conducted in line with the principles of the Criminal Code and the Code of Criminal Procedure*[34]. A change in this respect was introduced by regulations included in chapter V of the Act of 10 June 2016 on anti-terrorist activities. Pursuant to Article 25 of the act, in the case of a suspicion or attempt to commit or preparation of an offence of a terrorist nature, in order to detect or detain or forcibly bring in a suspected person, as well as in order to find items which may constitute evidence in the case or which may be seized in criminal proceedings, the public prosecutor may issue a decision to search premises and other places located in the area indicated in the decision or to detain a suspected person, if there are reasonable grounds to suspect that the suspected person or the said items are located in that area. Such a search and detention may be carried out at any time of day.

Preparatory proceedings conducted in connection with the suspected commission of an offence of a terrorist nature have been considerably improved by the power under Article 26 of the act, which makes it possible to draw up a decision to present charges on the basis of information obtained as a result of operational and reconnaissance activities. Moreover, in this case, the court, upon the prosecutor's motion, may apply temporary arrest for a period not exceeding 14 days, and the sole prerequisite for the application of this temporary arrest is the probability of committing, attempting or preparing to commit an offence of a terrorist nature.

The Act of 10 June 2016 on anti-terrorist activities significantly amended the regulations of the Criminal Code, introducing, inter alia, the punishable stage of preparation to commit crimes against peace, humanity and war crimes defined in: Article 117 of the Criminal Code (initiation or conduct of an attacking war), Article 118 of the Criminal

[34] W. Olsztyn, *Nowe rozwiązania w obszarze działań operacyjno-rozpoznawczych oraz procesowych wynikające z ustawy o działaniach antyterrorystycznych* (Eng. New solutions in the area of operational, reconnaissance and procedural activities resulting from the Act of 10 June 2016 on anti-terrorist activities), in: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem* (Eng. Polish Act of 10 June 2016 on anti-terrorist activities - a response to the threat of contemporary terrorism), W. Zubrzycki, K. Jałoszyński, A. Babiński (eds.), Szczytno 2016, p. 329.

Code (genocide), Article 118a of the Criminal Code (participation in a mass attack against a group of people), Article 120 of the Criminal Code (use of means of mass extermination), Article 122 of the Criminal Code (conducting hostilities in a manner inconsistent with international law), Article 123 of the Criminal Code (war crimes against prisoners of war or civilians), Article 124 of the Criminal Code (other violations of international law during the conduct of hostilities) and Article 125 of the Criminal Code (damaging or appropriating cultural property), and by adding in Articles 259a and 259b new types of criminal acts concerning the conduct of foreign fighters.

Summary

The above text systematises and discusses the tasks and powers of criminal law enforcement authorities in the field of combating terrorism in Poland, analysing them also from the perspective of more than six years of experience with the functioning of the Act of 10 June 2016 on anti--terrorist activities. It can be concluded that the aforementioned law has fulfilled its purpose, as it has organised the tasks and unified the activities of criminal law enforcement bodies, while providing them with modern tools to fulfil these tasks. The quality of this law is evidenced by the positive substantive assessment, among others, expressed in 2018 by Jukka Savolainen, Director of Resilience at the European Centre of Excellence for Countering Hybrid Threats in Helsinki. He considered that the act is an excellent example in terms of legislative solutions that can serve as model solutions and make an important contribution to the development of national legislation of EU and NATO countries in the context of "legal resilience" to hybrid threats[35]. Equally positive was the practical verification of the solutions contained in this law - many of its solutions concerning anti-terrorist actions at the scene of a terrorist incident were not applied in practice.

However, given that the fight against terrorism can never be considered a closed topic, the analyses of the modus operandi of the perpetrators of terrorist actions should constantly follow the analyses of the needs for

[35] Cf. S. Żaryn, *Polska antyterrorystycznym wzorem* (Eng. Poland as an anti-terrorist model), wGospodarce, 28 XII 2018, https://wgospodarce.pl/opinie/58189-polska-antyterrorystycznym-wzorem [accessed: 29 IV 2022].

legal changes, undertaken both at the level of individual countries, and above all within the international community faced with identical threats. In this context, a number of legislative postulates can be put forward, which come from the experience of the application of the *A*ct of 10 June 2016 on anti-terrorist activities.

Firstly, since the moment of its creation, attention has been drawn to the imbalance in the content of the solutions it covers in relation to the individual phases of undertaking anti-terrorist activities. As indicated earlier, the legislator put the main substantive emphasis on the solutions covered by the phase of activities aimed at preventing terrorist events (in respect of which the provisions of the act fill nearly half of its content, i.e. 12 out of 26). It is worth considering whether the remaining range of solutions covering the three remaining phases of activities, i.e. preparation to take control over terrorist events by means of planned undertakings, response in the event of the occurrence of such events, restoration of resources intended for response to such events, constitutes a comprehensive instrumentarium, which in practice will make it possible to manage the response to terrorist events. This issue requires - as it seems - detailed analyses, which should be undertaken primarily by the ministry of internal affairs responsible for it. However, the effectiveness of the actions of the first phase, coordinated by the Head of the ABW, often makes these considerations theoretical, as practical experience can only come from exercises, including the very important NATO Crisis Management Exercise (CMX).

Secondly, despite the broad regulation of activities undertaken in the first phase of counter-terrorist activities, the issue of cooperation in operational and reconnaissance activities undertaken by various services, both special services and those of a police nature, requires possible clarification - mainly due to the lack of statutory definitions. This applies in particular to the legitimacy of clarifying the principles and manner of performing the coordinating role by the Head of the ABW, taking into account the tasks in the area of supervision and control of the activities of services and the coordination of their activities entrusted to the Prime Minister and the Minister Coordinator of Special Services.

Thirdly, in the near future the most important challenge to be faced by domestic and European legislators will undoubtedly be the need to adapt anti-terrorist regulations to the changing paradigm of threats to state (international community) security. The emergence of threats considered

collectively as asymmetrical (hybrid) threats, in which both another state and a non-state entity may be the source of the threat, and the range of unconventional actions applied leads to the blurring of the definition of classic crimes, mainly such as terrorism, espionage or aggression war, requires - in order to counteract them properly - significant modifications. Changes will have to be introduced both at the level of substantive penal regulation, procedural regulation, and, perhaps most importantly, at the level of the system of legal protection bodies, headed by the competence regulations (tasks and powers) of the special services. This issue should become the subject of separate, more extensive considerations.

Bibliography

Burczaniuk P., *Legal aspects of combating terrorism in the Polish legal system against the background of challenges shaped by European legislation*, "Terroryzm – studia, analizy, prewencja" 2022, no. 1, pp. 273-279.

Chomentowski P., *Polski system antyterrorystyczny. Prawno-organizacyjne kierunki ewolucji* (Eng. Polish anti-terrorist system. Legal and organisational directions of evolution), Warszawa 2014.

Cichomski M., Idzikowska-Ślęzak I., *Strategic level of the Polish anti-terrorist system - 15 years of the Interministerial Team for Terrorist Threats*, "Terroryzm – studia, analizy, prewencja" 2022, no. 1, pp. 297-319.

Gabriel-Węglowski M., *Działania antyterrorystyczne. Komentarz* (Eng. Anti-terrorist activities. A commentary), Warszawa 2018, Lex/el.

Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem (Eng. Polish Act of 10 June 2016 on anti-terrorist activities - responding to the threats posed by modern terrorism), W. Zubrzycki, K. Jałoszyński, A. Babiński (eds.), Szczytno 2016.

Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego (Eng. Legal aspects of the functioning of special services on the example of the Internal Security Agency), P. Burczaniuk (ed.), Warszawa 2021.

Problemy prawno-organizacyjne zwalczania terroryzmu w Polsce (Eng. Legal and organisational problems of combating terrorism in Poland), J. Szafrański, K. Liedel (eds.), Szczytno 2011.

Prusak F., *Niesądowe organy ochrony prawnej* (Eng. Non-judicial legal protection bodies), Warszawa 2004.

Terroryzm. Materia ustawowa? (Eng. Terrorism. Statutory matter?), K. Indecki, P. Potejko (eds.), Warszawa 2009.

Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia (Eng. Powers of special services from the perspective of contemporary threats to national security. Selected issues), P. Burczaniuk (ed.), Warszawa 2017.

Internet sources

Żaryn S., *Polska antyterrorystycznym wzorem* (Eng. Poland as an anti-terrorist model), wGospodarce, 28 XII 2018, https://wgospodarce.pl/opinie/58189-polska-antyterrorystycznym-wzorem [accessed: 29 IV 2022].

Legal acts

International Convention on Maritime Search and Rescue, Hamburg, 27 April 1979 (Journal of Laws of 1988, No. 27 item 184).

Act of 9 November 2018 amending the Act on the Police and certain other acts (Journal of Laws of 2019, item 15).

Act of 1 March 2018 on counteracting money laundering and financing of terrorism (i.e. Journal of Laws of 2022, item 593, as amended).

Act of 26 January 2018 on the Marshal's Guard (i.e. Journal of Laws of 2019, item 1940, as amended).

Act of 8 December 2017 on the State Protection Service (i.e. Journal of Laws of 2021, item 575, as amended).

Act of 10 June 2016 on anti-terrorist activities (i.e. Journal of Laws of 2021, item 2234, as amended).

Act of 24 May 2013 on direct coercive measures and firearms (i.e. Journal of Laws of 2022, item 1416).

Act of 17 July 2009 amending the Act on crisis management (Journal of Laws of 2009, No. 131, item 1076).

Act of 26 April 2007 on crisis management (i.e. Journal of Laws of 2022, item 261, as amended).

Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service (i.e. Journal of Laws of 2022, item 502, as amended).

Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency (i.e. Journal of Laws of 2022, item 557).

Act of 6 June 1997 - Criminal Code (i.e. Journal of Laws of 2022, item 1138).

Act of 24 August 1991 on fire protection (i.e. Journal of Laws of 2021, item 869, as amended).

Act of 12 October 1990 on the Border Guard (i.e. Journal of Laws of 2022, item 1061, as amended).

Act of 6 April 1990 on the Police (i.e. Journal of Laws of 2021, item 1882, as amended).

Act of 6 April 1990 on the State Protection Office (Journal of Laws of 1990, No. 30, item 180).

Ordinance of the Prime Minister of 18 November 2019 on the detailed scope of activities of the Minister of the Interior and Administration (Journal of Laws of 2019, item 2264).

Ordinance of the Minister of the Interior and Administration of 5 February 2019 amending the Ordinance on the catalogue of terrorist incidents, (Journal of Laws of 2019, item 317).

Ordinance of the Minister of the Interior and Administration of 22 July 2016 on the catalogue of terrorist incidents (Journal of Laws of 2017, item 1517).

DOI: 10.4467/27204383TER.22.025.16345

ORCID: 0000-0003-3707-7856
ORCID: 0000-0002-2012-4954

MARIUSZ CICHOMSKI
ILONA IDZIKOWSKA-ŚLĘZAK

Alert levels - practical and legal dimensions of their use

Abstract

Alert levels - as a legal institution currently standardised in Chapter 3 of the Act of 10 June 2016 on anti-terrorist activities, having its origins still in the Act of 26 April 2007 on crisis management - can significantly affect both public administration bodies and many entities and, in certain cases, the general public when applied. Seven years of functioning of the alert levels in the current formula allows an attempt to describe them and make a several-faceted assessment.

The article discusses alert levels on two dimensions, i.e. the actual use of this legal institution, especially the answer to the questions whether and in which cases they are managed, and the adequacy of legal solutions from the perspective of the assumed objectives, taking into account both the practical dimension of the use of alert levels and the structural correctness.

Keywords:

alert levels,
CRP alert levels,
Act on anti-terrorist activities,
terrorism,
terrorist threats

Legal basis and essence of alert levels

From a historical perspective, it should be mentioned that alert levels are not a legal institution that has only been in force in Poland since 2016, i.e. since they were introduced into the Polish legal order by universally applicable law, i.e. the Act of 10 June 2016 on anti-terrorist activities[1].

[1] Consolidated text: Journal of Laws of 2021, item 2234, as amended.

For the first time, alert levels in the context of terrorist threats were introduced to Poland by Order No. 74 of the Prime Minister of 12 October 2011 on the list of undertakings and procedures of the crisis management system[2], which was replaced shortly before the entry into force of the Act on anti-terrorist activities by Order No. 18 of the Prime Minister of 2 March 2016 on the list of undertakings and procedures of the crisis management system[3]. Both of these orders were issued on the basis of Article 7 of the Act of 26 April 2007 on crisis management[4]. They introduced a list of undertakings and procedures of the crisis management system, taking into account undertakings and procedures resulting from the Emergency Response System of the North Atlantic Treaty Organisation (NATO)[5] and defined the bodies responsible for their activation. In addition to the aforementioned list of undertakings resulting from Poland's membership of NATO, it also included alert levels, and since the entry into force of Order No. 18 of 2 March 2016 - also alert levels for threats in Poland's cyberspace, called 'CRP alert levels'.

It should be noted, however, that it was not until the Act on anti-terrorist activities that the system for determining CRP alert levels and alert levels was intruduced which would be universally applicable and thus have the valour of effectiveness beyond the authorities, services and institutions also for other organisational units and the public, since (...) *the previous system, applicable on the basis of Ordinance No. 18 of the Prime Minister of 2 March 2016 on the list of undertakings and procedures of the crisis management system covered only the government administration*[6].

This system was largely transposed from the provisions contained in Annex No. 1 of the aforementioned Order No. 18 of 2 March 2016, which were in force at the time of the entry into force of the Act on anti-terrorist

[2] Unpublished (editor's note).

[3] For the text of the Ordinance see https://www.stawiguda.pl/userfiles/OC/Komunikaty_zew/Zarz%C4%85dzenie%20nr%2018%20Prezesa%20Rady%20Ministr%C3%B3w%20z%20dnia%202%20marca%202016%20r.pdf.

[4] Consolidated text: Journal of Laws of 2022, item 261, as amended.

[5] NATO Crisis Response System Manual.

[6] P. Chorbot, *Ustawa o działaniach antyterrorystycznych. Komentarz do niektórych regulacji* (Eng. The Act on anti-terrorist activities. Commentary on some regulations), in: *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia* (Eng. The powers of the special services from the perspective of contemporary threats to national security. Selected issues), P. Burczaniuk (ed.), Warszawa 2017, p. 71.

activities. The justification for making the change in question was that the alert levels apply not only to government bodies, but also to other organisational units and citizens, and it was therefore considered insufficient to regulate them at the level of the Ordinance. At the same time, the introduction of a system of alert levels at the level of a generally binding act made it possible to extend the catalogue of entities obliged to take relevant actions (previously limited to government administration bodies)[7]. In the commentary to the Act on anti-terrorist activities, it was additionally pointed out that specific colours were assigned to particular levels of threat[8]. *In Poland, colour coding was also used in the past; however, the Act on anti-terrorist activities does not introduce such a classification*[9].

It should also be emphasised, following the explanatory memorandum to the draft Act on anti-terrorist activities, that the system of alert levels is independent of the possibility of introducing states of emergency provided for in:

– The Act of 29 August 2002 on martial law and the powers of the Commander-in-Chief of the Armed Forces and the principles of his subordination to the constitutional bodies of the Republic of Poland[10] - in relation to the threat of terrorism or actions in cyberspace as a premise for the introduction of martial law and the use of the Armed Forces of the Republic of Poland;

---

[7] Explanatory memorandum to the draft Act on anti-terrorist activities, https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=516 [accessed: 2 VII 2022]; cf.: M. Cichomski, M. Horoszko, I. Idzikowska, *Przygotowanie do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym oraz reagowanie w przypadku wystąpienia takich zdarzeń w świetle rozwiązań ustawy o działaniach antyterrorystycznych – w kontekście zadań resortu spraw wewnętrznych* (Eng. Preparing to take control of terrorist incidents and responding in the event of such incidents in the light of the solutions of the Act on anti-terrorist activities - in the context of the tasks of the Ministry of Internal Affairs), in: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem* (Eng. Polish Act on anti-terrorist activities - a response to the threat of modern terrorism), W. Zubrzycki, K. Jałoszyński, A. Babiński (eds.), Szczytno 2016, pp. 283–287.

[8] Cf.: *Kolory, stopnie i terminologia NATO. Jak odczytać alerty terrorystyczne* (Eng. NATO colours, levels and terminology. How to interpret terrorist alerts), TVP Info, 23 III 2016, https://www.tvp.info/24554977/kolory-stopnie-i-terminologia-nato-jak-odczytac-alerty-terrorystyczne [accessed: 7 XII 2018].

[9] P. Łabuz, T. Safjański, W. Zubrzycki, *Ustawa o działaniach antyterrorystycznych. Komentarz* (Eng. The Act on anti-terrorist activities. Commentary), Warszawa 2019, access through the Legal Information System Legalis, sip.legalis.pl [accessed: 20 VII 2022].

[10] Consolidated text: Journal of Laws of 2017, item 1932, as amended.

– The Act of 18 April 2002 on the state of natural disaster[11] - with regard to a terrorist threat or an event in cyberspace as premises for the introduction of the state of natural disaster and use of the Armed Forces of the Republic of Poland;
– The Act of 21 June 2002 on a state of emergency[12] - in relation to a terrorist threat or an event in cyberspace as a premise for the introduction of a state of emergency and the use of the Armed Forces of the Republic of Poland.

In preparing the solutions of the Act on anti-terrorist activities concerning the system of alert levels, it was assumed that if these instruments were used and proved to be insufficient in preventing or responding to threats, this would constitute a rationale for the introduction of an appropriate state of emergency. Accordingly, provisions relating to terrorist threats were left in the aforementioned laws[13]. This seems obvious both from the perspective of the constitutional foundations of the acts concerning states of emergency (Article 228 of the Constitution of the Republic of Poland of 2 April 1997[14]) and the premises for the introduction of particular states of emergency (especially the state of emergency, which, in accordance with Article 230 of the Constitution of the Republic of Poland, may be introduced in the event of a threat to the constitutional system of the state, security of citizens or public order).

The construction of states of emergency in the light of the regulations of the Act on anti-terrorist activities may be considered on several levels, including:

– subject matter - in this respect, alarm levels sensu stricto and CRP alarm levels can be distinguished,
– threat level - on a four-grade scale,
– local - refers to alert levels applicable on the territory of Poland, including the whole territory or specific areas, and outside its borders, but within Polish jurisdiction.

In the case of the first tier, under Article 15 of the Act on anti-terrorist activities, two types of alert levels can be distinguished: (1) alert levels sensu stricto (a term introduced for the purposes of this study) and (2) CRP

[11] Consolidated text: Journal of Laws of 2017, item 1897.

[12] Consolidated text: Journal of Laws of 2017, item 1928.

[13] Explanatory memorandum to the draft Act on anti-terrorist activities...

[14] Journal of Laws of 1997, No. 78, item 483, as amended.

alert levels, introduced in the case of a threat of a terrorist event concerning ICT systems of public administration bodies or ICT systems constituting critical infrastructure.

Separation of the categories: "alert levels sensu stricto" is due to the fact that the legislator uses the term "alert levels" in two circumstances: (1) in order to define the particular levels that may be introduced in the event of a threat of the occurrence of all categories of terrorist events, and (2) the occurrence of such an event in addition to cyber events - Article 15(1) of the Act on anti-terrorist activities. The legislator also uses this term as a general term applied to the entirety of this legal institution (both alert levels sensu stricto and CRP alert levels), which is reflected, inter alia, in the title of Chapter 3 of the Act on anti-terrorist activities - *Alert levels*, thus treating collectively all types of alert levels, including CRP alert levels (one may then speak of alert levels *sensu largo*).

When considering alert levels in the context of the degree of threat of a terrorist event, the legislator modelled the terminology on that used within the NATO emergency response system and introduced a four-stage scale of alert levels - similar in the case of alert levels sensu stricto and CRP alert levels. In the case of alert levels sensu stricto, he distinguished:

– first alert level - ALFA level,
– second alert level - BRAVO level,
– third alert level - CHARLIE level,
– fourth alert level - DELTA level.

For CRP alert levels, respectively:

– first CRP alert level - ALFA-CRP level,
– second CRP alert level - BRAVO-CRP level,
– third CRP alert level - CHARLIE-CRP level,
– fourth CRP alert level - DELTA-CRP level.

The analogy of the adopted systematics is also indicated by the rationale for the introduction of each of the two categories of alert levels, i.e. alert levels sensu stricto and CRP alert levels, defined jointly for both categories, depending on the intensity of the threat and the detail and reliability of the information about it.

Both the first alert level and the first CRP alert level can be introduced in a situation where information has been obtained about the possibility of a terrorist event, but both the nature of this potential threat and its extent are difficult to predict.

Subsequent alert levels and CRP alert levels are introduced as the detail and reliability of the available information increases, as well as the resulting likelihood of a terrorist event.

BRAVO alert level and BRAVO-CRP alert level are applicable in the case of an increased and predictable threat, when the specific target of an attack is still not identified. On the other hand, the possibility to introduce the CHARLIE and CHARLIE-CRP alert levels was made by the legislator conditional on the occurrence of several prerequisites jointly or separately, the first of which was the actual occurrence of an event confirming the likely target of an attack of a terrorist nature, provided that this attack simultaneously undermines security or public order or the security of the Republic of Poland, or the security of another state or international organisation, but at the same time affects the Republic of Poland and becomes a potential threat to it. In addition, the legislator provided for the possibility of introducing a third alert level (both sensu stricto and CRP alert level) in the event that information on a planned terrorist event on the territory of the Republic of Poland is reliable and confirmed. As the third premise, it indicated that the information obtained is credible and confirmed and concerns a planned terrorist event, (...) *the effects of which may affect Polish citizens residing abroad or Polish institutions or Polish infrastructure located outside the borders of the Republic of Poland*[15].

The prerequisites for the introduction of the fourth level (characterised by the legislator jointly in relation to the levels sensu stricto and the CRP levels), similarly to the introduction of the third level, which may occur jointly or separately, are:

- the occurrence of an event of a terrorist nature, whereby, as in the case of the introduction of the third alert level, the event undermines security or public order or the security of the Republic of Poland, or the security of another state or international organisation and at the same time poses a threat to the Republic of Poland;
- information indicating an advanced stage of preparations for an event of a terrorist nature on the territory of the Republic of Poland;
- information indicating an advanced stage of preparations for an event of a terrorist nature which is to be directed against Polish citizens residing abroad or against Polish institutions, or against Polish infrastructure located outside the Republic of Poland, which

[15] Act on anti-terrorist activities, Article 15(5)(3).

at the same time testifies to the imminence of the occurrence of such an event.

For practical reasons, the legislator provided for the possibility of introducing levels both higher and lower than those previously introduced, with the omission of intermediate levels. Importantly - the Act also includes the possibility to introduce the categories of alert levels sensu stricto and CRP alert levels separately or jointly, while the level defined for one category does not in any way determine the level defined for the other, e.g. in 2022, the second alert level sensu stricto, i.e. BRAVO alert level, and the third CHARLIE-CRP alert level are maintained simultaneously.

In view of the possibility of local conditioning of the scope of validity of a given level, which will be discussed further when discussing the third of the above-mentioned levels of consideration of alert levels, the legislator also provided for the possibility of simultaneous validity of different alert levels in a given area and indicated in Article 15(10) of the Act on anti-terrorist activities that in this type of situation the tasks provided for a higher level should be performed.

Bearing in mind the relationship of alert levels to additional obligations on the part of public institutions and, in some cases, to restrictions on civil liberties, the Act emphasises that both alert levels sensu stricto and CRP alert levels shall be revoked (...) *as soon as the threat or consequences of the event giving rise to their introduction have been minimised*[16]. Another intention of the legislator can be discerned here - the alert levels are not intended to serve as a general and current description of the level of terrorist threat in Poland, and should only be introduced in the event of a more or less concrete threat (or in the event of a terrorist event) and revoked as urgently as possible after its cessation (unless a derogatory norm is contained in the order on the introduction of the alert level itself). Accordingly, a 'zero level' construct has not been introduced. Instead, the validity of the alert level itself is intended to oblige certain entities to take actions that are above standard and appropriate to the threat. For example - on the basis of a general assessment of the geopolitical situation in Central and Eastern Europe, it is possible to conclude that the level of terrorist threat in Poland is medium, not negligible or low, and at the same time not to introduce the alert level.

[16] Ibid., Article 15(10).

Turning to the third level of consideration of the alert levels, it should be noted that Article 16(1) provides for the possibility of an area-based limitation of the place where the introduced alert levels will apply, and in this case, too, the legislator did not limit this possibility only to alert levels sensu stricto, but allowed its use to CRP alert levels. In practice, CRP alert levels have so far been ordered only on the territory of the whole country (however, it cannot be ruled out that information about a possible threat could concern, for example, the ICT systems of a specific authority, as a result of which it would be unjustified to introduce a CRP alert level on the territory of the whole country). The Act provides for the possibility of introducing both categories of alert levels:

- on the entire territory of the Republic of Poland,
- on the area of one or several territorial divisions of the country,
- on the area defined in a manner other than by reference to the units of territorial division of the country,
- for specific buildings of organisational units of public administration, prosecutor's office, courts or other objects of infrastructure of public administration or critical infrastructure[17].

The indicated provision also contains the possibility of introducing the alert level understood stricto or the CRP alert level also in the case when (...) *the consequences of an event of a terrorist nature may affect Polish citizens residing abroad of the Republic of Poland or Polish institutions or Polish infrastructure located outside the borders of the Republic of Poland other than foreign posts of the Republic of Poland within the meaning of the Foreign Service Act of 21 January 2021*[18] (i.e. Journal of Laws of 2022, item 1076, as amended – editor's note).

In turn, Article 16(2) of the Act provides for the possibility of introducing the aforementioned categories of alert levels:

- for certain foreign missions of the Republic of Poland within the meaning of the Foreign Service Act ,
- in relation to information and communication systems of the minister in charge of foreign affairs.

The procedure for the introduction of alert levels remains differentiated, but not due to these two subject categories of level

[17] Ibid., Article 16(1)(1-4).

[18] Ibid., Article 16(1)(5).

distinction (alert levels sensu stricto and CRP alert levels), but depending on the scope of their territorial validity.

The body introducing the alert levels by means of an ordinance - in a variant which, for the purposes of the article, can be described as basic - is the Prime Minister. In the situations catalogued in Article 16(1), and therefore relating primarily to the national territory, before issuing such an order he shall consult the minister responsible for internal affairs and the Head of the Internal Security Agency - bodies responsible for internal security. Their designation is a logical consequence of Article 3 of the Act on anti-terrorist activities, according to which the Head of the ABW is responsible for the prevention of terrorist incidents, and the minister in charge of internal affairs is responsible for preparing to take control of terrorist incidents by means of planned undertakings, responding in the event of the occurrence of such incidents and restoring the resources intended for responding to such incidents.

In the situations described in Article 16(2), i.e. in the case of the introduction of alert levels in foreign posts of the Republic of Poland or with regard to ICT systems under the responsibility of the minister in charge of foreign affairs (i.e. - as may be assumed - in both cases outside the country's borders, but in the areas of Polish jurisdiction), the entities giving opinions are the minister in charge of foreign affairs and the Head of the Foreign Intelligence Agency.

This solution - in line with the scope of competence of the individual opinion-forming bodies - also has a direct bearing on the variant that we may call the special variant of introducing the alert levels, i.e. in an urgent situation. In the special variant, the alert level, by way of an ordinance, is introduced - respectively, in the areas specified in Article 16, section 1 and in the case specified in the aforementioned Article 16, section 1, item 5 - by the minister in charge of internal affairs after consultation with the Head of the Internal Security Agency, and with regard to foreign posts of the Republic of Poland and information and communication systems - by the minister in charge of foreign affairs after consultation with the Head of the Foreign Intelligence Agency.

In both special variants, depending on the area of validity of the alert levels, the body introducing the alert level shall immediately notify the Prime Minister.

The Prime Minister shall immediately communicate information on the introduction of the alert level, as well as information on the change or

cancellation of the alert level, to the President of the Republic of Poland and to the Marshals of both Houses of Parliament.

At this point, it is worth noting that, prior to the transfer of the alert level system to common law, in the aforementioned orders - No. 74 of 12 October 2011 and No. 18 of 2 March 2016. - the authority that was authorised to introduce the alert was determined by the area of the alert.

While under the current legislation such an authority is the Prime Minister, and in exceptional situations the minister in charge of internal affairs or the minister in charge of foreign affairs, the aforementioned orders provided for the possibility of the introduction of alert levels by the Prime Minister only in a situation where the entire territory of the country or several provinces were affected. In other cases, the right to introduce the alert level was vested in:

- ministers or heads of central offices - in relation to all or selected heads of subordinate, subordinate and supervised organisational units, formations and offices,
- voivodes - in relation to areas, objects and devices according to local jurisdiction, on the area of the whole or part of a voivodeship[19].

In addition, Order No. 18 of the Prime Minister of 2 March 2016 provides for the possibility of introducing an alert level in Polish diplomatic representations and consular offices by a decision of the minister in charge of foreign affairs.

On the grounds of the Act on anti-terrorist activities, due to the universally applicable nature of the alert levels, the legislator decided to limit the competence in terms of the possibility to introduce them and to centralise the powers.

As already mentioned, the introduction of the alert level sensu stricto or the CRP alert level is the basis for the implementation by public institutions, i.e. bodies of public administration and heads of services and institutions competent in matters of security and crisis management, of specific undertakings with the primary aim of minimising the threat. The legislator, taking into account the above-described procedural differences resulting from the competences of individual authorities, depending on the territorial area where the alert level is introduced,

[19] Cf: Annex 5 to Order No. 74 of the Prime Minister of 12 October 2011 and Annex 1 to Order No. 18 of the Prime Minister of 2 March 2016.

provided for separate executive acts regulating the scope of undertakings carried out in individual alert levels sensu stricto and CRP alert levels.

In the case of the mode of introducing the alert level referred to in Article 16, paragraph 1, the Prime Minister is authorised to issue a relevant regulation, and in the case of the mode resulting from Article 16, paragraph 2 - the minister in charge of foreign affairs. In the first case, the executive act refers subjectively to the undertakings carried out within the scope of statutory competence by public administration bodies and managers of services and institutions competent in matters of security and crisis management, and in the second case only to the managers of foreign posts of the Republic of Poland. In both situations, the guidelines for the issuance of executive acts are: minimising the consequences of events of a terrorist nature and ensuring the efficiency of information flow.

At the level of the Act, attention has also been drawn to the fact that, in addition to the above-mentioned acts, public administration bodies and heads of services and institutions competent in matters of security and crisis management are also obliged to carry out other undertakings which either result directly from their statutory competences or from crisis management undertakings and procedures - if these have been provided for a given alert level and have not been specified in the above-mentioned executive acts.

At the level of the Act on anti-terrorist activities itself, additional competences and duties of individual authorities are also provided for, depending on the alert levels introduced.

In the aforementioned Chapter 3, entitled *Alert levels*, Article 17 provides for the establishment of the so-called coordination staff, whose statutorily defined tasks include recommending the change or cancellation of the alert level and recommending the forms and scope of cooperation of the services and authorities constituting the staff and participating in its work. The staff is composed of representatives appointed by the special services and by the Police, the Border Guard, the Marshal's Guard, the State Protection Service, the State Fire Service, the General Inspector of Financial Information, the National Revenue Administration, the Military Police and the Government Security Centre, i.e. entities participating in the exchange of information on terrorist incidents coordinated by the Head of the ABW under Article 5(1) of the Act on anti-terrorist activities. In turn, to participate in the works of the staff, the Head of the ABW may appoint, optionally, depending on the type of event which was the basis for the introduction

of the alert level, representatives of other public administration bodies and the Public Prosecutor General. The appointment of a coordination staff is an obligation of the Head of the ABW in the case of the introduction of any of the alert levels - regardless of whether it is an alert level sensu stricto or a CRP alert level, and at which level (ALFA, BRAVO, CHARLIE, DELTA) it is set. While this obligation applies only to the levels introduced in the mode referred to in Article 16(1) of the Act on anti-terrorist activities, i.e. on the territory of the country. There is no analogous obligation imposed on the Head of the AW participating in the procedure of issuing alert levels in the mode referred to in Article 16(2) of that Act.

On the introduction of a specific alert level sensu stricto, but no longer on the CRP alert level, in further provisions depends:

– **the introduction of a ban on the holding of assemblies or mass events (Article 21 of the Act)** - as a competence of the minister in charge of internal affairs, acting on his/her own initiative or on the motion of the Head of the ABW or the Commander-in-Chief of the Police, in the case of the introduction of the third or fourth alert level. The prohibition territorially refers to the area covered by the alert level, and temporally - to the time for which the alert level was ordered. The rationale for its introduction is the need to protect human life and health or public safety. It is also incumbent on the minister responsible for internal affairs to inform the Marshal of the Sejm and the Marshal of the Senate, who in turn transmit this information to MPs and senators respectively. The prohibition results in the issuing of a decision by the municipal authority to prohibit the assembly or to dissolve it, respectively, in the modes specified in the Act of 24 July 2015 - Law on assemblies[20] or the introduction by the governor, by means of an administrative decision, of a prohibition to hold a mass event or its interruption, in accordance with the provisions of the Act of 20 March 2009 on the security of mass events[21]. These decisions apply to all assemblies and mass events during the alert level and in the area of its validity in the part covered by the local jurisdiction of the public administration body concerned, and are subject to the appeals specified in

[20] Consolidated text: Journal of Laws of 2022, item 1389.

[21] Consolidated text: Journal of Laws of 2022, item 1466.

the aforementioned Acts - the Law on assemblies and the Act on security of mass events;

– **the use of branches or subdivisions of the Armed Forces of the Republic of Poland to assist the branches and subdivisions of the Police (Article 22 of the Act)** - as the competence of the Minister of National Defence acting on the motion of the minister in charge of internal affairs, in the event of the introduction of the third or fourth alert level. The procedure specified in Article 22 of the Act on anti-terrorist activities is a simplification and, at the same time, an improvement of the procedures in relation to the procedure provided for in the provisions of Article 18 of the Act of 6 April 1990 on the Police[22] thanks to the preparation of the Armed Forces of the Republic of Poland for their use, i.e. commencement of planning, acquisition of information and cooperation with public administration bodies, immediately after the introduction of the third or fourth alert level and prior to the issuance of the decision by the Minister of National Defence. Due to the special category of threats of terrorist events, including the number of victims, which is difficult to estimate, and the unpredictable course and consequences of such events - in the situation of a high probability of the occurrence or occurrence of a terrorist event, which we are dealing with in the third and fourth alert level - the legislator provided for the possibility of using and employing means of direct coercion and firearms. They may be used in counter-terrorist operations by branches and subdivisions of the Special Forces supporting the Police in the manner provided for in the Act of 11 March 2022 on the defence of the homeland[23], subject to the admissibility of the use of firearms in cases specified in Article 23(1) of the Act on counter-terrorist operations. This means, in practice, that soldiers of the Special Forces will be able to use means of direct coercion and firearms within the scope of their statutory competence, i.e. (...) within the scope of protecting the independence of the state, the indivisibility of its territory and ensuring the security and inviolability of its borders (...) in a manner adequate to the threat and within the limits of the principles defined in ratified international

[22] Consolidated text: Journal of Laws of 2021, item 1882, as amended.

[23] Journal of Laws of 2022, item 655, as amended.

agreements binding the Republic of Poland and in international customary law[24];

– **checking the security of objects in the area covered by the alert level (Article 12 of the Act)** - as an obligation of the Police or the Military Police, respectively, in the event of the introduction of a second or higher alert level. The Police have been obliged by the Act to check the security of critical infrastructure facilities, while the Military Police have been obliged to check facilities belonging to organisational cells and units subordinate to the Minister of National Defence or supervised by him, or administered by these organisational cells and units. The obligation is also linked with an additional competence of the Head of the Internal Security Agency, who, in agreement with the minister in charge of internal affairs, may issue a recommendation to the Police to specifically secure individual facilities, taking into account the type of threat of a terrorist event.

Turning from the statutory regulations to the undertakings set out in the aforementioned executive acts, reference should first be made to the Ordinance of the Prime Minister of 25 July 2016 on the scope of undertakings to be carried out in individual alert levels and CRP alert levels[25]. The Ordinance indicates, in accordance with the statutory delegation, that its main addressees are public administration bodies and heads of services and institutions competent in matters of security and crisis management. However, § 1(2) additionally points out that these entities shall carry out undertakings within the framework of individual alert levels and CRP alert levels (...) *in cooperation with the owners, sole holders and dependent holders of critical infrastructure facilities with regard to the protection of these facilities*. Pursuant to § 2(2) of this Regulation, for the purposes of such cooperation, the above-mentioned owners, self-owners and dependent holders of critical infrastructure are even obliged to take into account the detailed scope of undertakings laid down in the Regulation. From the perspective of legislative correctness, this solution may raise doubts as to its compliance with the content of the statutory

[24] Act on the Police, Article 11(4).

[25] Journal of Laws of 2016, item 1101. Amendments were introduced in: Notice from the Prime Minister of 27 July 2016 on the correction of errors (Journal of Laws of 2016, item 1116) and Ordinance of the Prime Minister of 4 March 2022 amending the Ordinance on the scope of undertakings to be carried out in individual alert levels and CRP alert levels (Journal of Laws of 2022, item 538).

mandate, and the above-mentioned obligation imposed on entities not explicitly mentioned in the delegation should rather constitute a statutory norm.

The detailed scope of undertakings was defined in an annex to the regulation in question, while independently of it, in § 3 of the regulation, it was indicated that the public administration bodies and heads of services and institutions competent in matters of security and crisis management will define (...) *the procedures for the implementation of undertakings under individual alert levels and CRP alert levels, including task modules for each level, containing, in particular, the list of tasks to be performed*[26] (it seems that this provision, as imposing certain additional obligations, should be transferred to the statutory ground in the future).

Paragraph 4 of the regulation contains the information obligation imposed on the addressees of the regulation towards the Government Centre for Security. According to the ordinance, upon receiving information on the introduction of an alert level or CRP alert level, public administration bodies and heads of services and institutions competent in matters of security and crisis management shall immediately confirm to the Government Centre for Security the receipt of information on the introduction of an alert level or CRP alert level. They shall also transmit a report on the status of the implementation of the tasks resulting from the introduced level within no more than 12 hours from the commencement of the level. While, from a functional perspective, this provision does not raise any objections and closes the procedure related to the introduction, cancellation and modification of the alert levels and informing the entities competent to take the necessary actions about this fact, from a legal and legislative perspective, it should find precise support in the substantive provisions of the Act, and the possible mode of transmission of information should be included in the authorisation to issue this executive act.

The scope of undertakings contained in the aforementioned annex has been defined separately both for each of the four alert levels sensu stricto and for each CRP alert level, while for each successive level, starting from ALFA and ALFA-CRP alert levels, it has been indicated that, in the event of its introduction, the tasks listed for the lower levels of a given category

[26] An example of this type of procedure is Order No. 16 of the Minister of the Interior and Administration of 2 July 2019 on the implementation of tasks related to the opinion, introduction, change or cancellation of alert levels or CRP alert levels (unpublished).

(either alert levels sensu stricto or CRP alert levels) should be performed and the performance of these tasks should be continued or verified.

A similar structure is also provided for in the Regulation of the Minister of Foreign Affairs of 7 June 2022 on the detailed scope of undertakings carried out by managers of foreign posts of the Republic of Poland in particular alert levels or CRP alert levels[27]. The detailed scope of undertakings provided for in the above-mentioned regulations for particular alert levels is presented in the tables below.

Table 1. Scope of undertakings provided for in the regulations for alarm levels sensu stricto.

Alert level sensu stricto	Tasks of public administration bodies and heads of services and institutions responsible for security and crisis management[a]	Tasks of heads of foreign posts[b]
ALFA	1) conducting, with the use of the Police, Border Guard or Military Police, increased control of large population centres which may potentially become a target of a terrorist event, including mass events and public gatherings; 2) conducting, as part of the implementation of the tasks of facility administrators, increased control of public buildings and other facilities that could potentially become a target of a terrorist event; 3) recommending to subordinate personnel to inform the relevant services in the event of noticing: unknown vehicles on the premises of public institutions or other important facilities, abandoned packages and luggage or any other signs of unusual activity;	1) informing members of staff at the foreign post and their family members of the introduction of the first alert level (ALFA level); 2) informing members of staff at the foreign post of the need for increased vigilance in the event of suspicious behaviour by persons and the search for suspicious objects; 3) introducing permanent 24-hour standby duty for members of staff at the foreign post; 4) launching a procedure for increased checks on vehicles and persons entering the premises of the foreign post (paying particular attention to the contents of vehicles and persons' luggage);

[a] Annex of the Ordinance of the Prime Minister of 25 July 2016.

[b] Annex 1 of the Ordinance of the Minister of Foreign Affairs of 7 June 2022.

[27] Journal of Laws of 2022, item 1251.

	4) informing subordinate staff of the need to be more vigilant with regard to persons behaving in a suspicious manner; 5) ensuring the availability, on an alert basis, of the staff members necessary to reinforce the security of the premises; 6) carrying out checks on vehicles entering and on persons entering the premises; 7) checking, externally and internally, buildings in constant use for suspicious behaviour of persons and for suspicious objects; 8) checking the operation of communications equipment used for security purposes; 9) carrying out, as part of the tasks of facility administrators, checks on the operation of alarm systems, the capacity of evacuation routes and the functioning of video recording systems; 10) reviewing all procedures, orders and tasks related to the introduction of higher alert levels; 11) conducting information and instruction campaigns for the public on the potential threat, its consequences and course of action	5) informing members of staff at the foreign post of the need to carry out checks on vehicles before entering and starting them; 6) limiting business travel; 7) limiting the movement of vehicles and persons within the foreign post to the necessary minimum; 8) reducing to a minimum the number of pedestrian and vehicle entrances used within the foreign post; 9) strengthening control of postal, courier and other deliveries arriving at the foreign post; 10) strengthening control over activities related to services provided to the foreign post by external entities; 11) checking the security of the foreign post outside and inside the buildings; 12) closing the entrances and securing the buildings and premises of the foreign post that are not regularly used; 13) checking the operation of the communication systems in place for the foreign post; 14) reviewing all procedures, detailed personnel and logistical requirements and tasks related to the implementation of higher alert levels; 15) checking the operation of alarm systems, video recording systems and the capacity of evacuation routes; 16) reviewing alternate energy sources (generators), water tanks, shelters and other places of protection for members of staff of the foreign post; 17) inspecting the grounds and building of the foreign post and making necessary repairs and renovations;

		18) informing the relevant services in the event of noticing: unknown vehicles parked or moving in a suspicious manner (e.g. repeatedly touring the facilities of the foreign post) or abandoned packages and luggage, or other unusual behaviour; 19) taking preparatory measures for securing items and materials of particular value; 20) undertaking other organisational and executive actions to enhance the security of the foreign post; 21) establishing direct contact with local authorities responsible for crisis management and security; 22) conducting monitoring of unusual events taking place in the immediate vicinity of the foreign post; 23) resigning meetings and special events of an open nature on the premises of the foreign post; 24) preparing and transmitting periodic information on the situation in the country of the post to the Ministry of Foreign Affairs, at fixed times; 25) preparing and transmitting supplementary and ad hoc information on the situation in the country of post to the Ministry of Foreign Affairs; 26) reviewing classified material with a view to selecting material subject to possible evacuation (especially classified documents made in single copy, classified documents necessary for the functioning of a foreign post, log books, protocols for destruction of classified documents) and classified material scheduled for destruction in the event of the introduction of one of the higher alert levels. Assembling classified material in the classified documents handling point of the foreign post; 27) reviewing and updating notices and information addressed to Polish nationals travelling to the host country and published on the websites of the Ministry of Foreign Affairs and the foreign post;

		28) checking the validity of the evacuation plan, and in particular the list of documents and items deemed important due to the interest of the Republic of Poland
BRAVO	1) introducing, by the Commander-in-Chief of the Police, the Commander-in-Chief of the Border Guard or the Commander-in-Chief of the Military Police, the obligation to wear long-arms and bullet-proof waistcoats by uniformed officers or soldiers directly performing the tasks connected with securing places and objects which may potentially become a target of a terrorist event; 2) introducing additional controls of vehicles, persons and public buildings in the threatened areas; 3) strengthening the protection of means of public transport; 4) checking the functioning of the emergency power supply; 5) alerting staff to possible forms of terrorist incident; 6) ensuring the availability, on an alert basis, of personnel designated to implement procedures for dealing with terrorist incidents; and 7) checking and strengthening the protection of important public facilities; 8) prohibiting access to kindergartens, schools and universities by members of the public; 9) verifying the system of protection of facilities protected by specialised armed security formations; 10) 1introducing controls on all mail addressed to the office or institution; 11) locking and securing buildings and premises not regularly used; 12) reviewing the stock of materials and equipment, including the availability of medical supplies and materials, taking into account the possibility of use in the event of a terrorist incident	1) informing members of staff at the foreign post of possible forms of attack; 2) ensuring that members of the personnel of the foreign post necessary for the implementation of activities to strengthen the protection of the foreign post are available on an alert basis; 3) strengthening the security of the foreign post; 4) checking the foreign post; 5) reviewing the security system of the stock of materials and equipment held; 6) carrying out, directly at the entrance to the foreign post, checks on persons entering the premises and their luggage; 7) introducing irregular patrols to inspect vehicles and buildings used for the foreign post, as well as persons on the premises of the post; 8) requesting the local authorities to increase the security of the foreign post and its personnel; 9) issuing recommendations to members of the personnel of the foreign post and their family members on limiting or refraining from contact with the local population, as well as leaving the place of residence without good reason; 10) agreeing with the Crisis Management Team at the Ministry of Foreign Affairs the possibility of repatriation of those members of the personnel of the foreign post and their families whose further stay at the post is not necessary; 11) updating the list of Polish nationals residing in the host country and countries within the territorial jurisdiction of the foreign post;

		12) notifying Polish nationals residing in the host country (irrespective of the purpose of their stay) of a threatening danger and recommending them to return to their country; 13) creating conditions for providing assistance to Polish citizens residing in the host country and facilitating their return to the country; 14) adapting (if necessary and with the use of available means) basements and other rooms of reinforced construction to be used as shelters or other hiding places of a similar nature; 15) replenishing material supplies, including medicines and dressing materials, water, fuel, spare parts for generators and cars, and instructing family members of personnel of the overseas post to gather adequate supplies of their own, especially food, water, medicines and dressing materials; 16) stopping all construction, assembly or renovation work of any kind in the facilities of the foreign post, with the exception of work in progress, carried out by national staff delegated by the Ministry of Foreign Affairs or by local staff, if the performance of this work has a significant impact on the security situation of the foreign post; 17) recalling members of the staff of the foreign post from leave, with the exception of those residing outside the host country; 18) establishing and maintaining constant communication with the Ministry of Foreign Affairs, other Polish institutions and posts abroad and with diplomatic missions of other EU countries, as well as with representatives of the Polish community and Polish citizens residing in the host country; 19) preparing the foreign post for the temporary accommodation on its territory of all staff members and their families (excluding local staff) or staff members and their families (excluding local staff) residing in particularly endangered places;

		20) destroying selected classified material not qualified for evacuation in accordance with the evacuation plan approved by the head of the foreign post and the destruction protocol
CHARLIE	1) introducing, by the order of the minister in charge of internal affairs, 24-hour on-call duties in indicated offices or organisational units of public administration bodies; 2) introducing on-call duties for functional persons responsible for the implementation of procedures for action in the event of events of a terrorist nature; 3) checking the availability of facilities designated as substitute places of temporary residence in the event of evacuation of the population; 4) limiting to a minimum the number of public places in the facility and the area of the facility; 5) introducing, where warranted, strict controls on persons and vehicles at the entrance and entrance to the premises; 6) restricting the parking of vehicles at protected facilities; 7) issuing weapons and ammunition and personal protective equipment to authorised persons designated to perform protective tasks; 8) introducing additional round-the-clock surveillance of places that require it, hitherto not covered by surveillance; 9) ensuring the protection of means of official transport outside the premises, introducing vehicle checks before entering and starting the vehicle	1) introducing standby duty for those responsible for implementing procedures to deal with acts of terrorism or sabotage; 2) limiting to a minimum the number of public areas in the foreign post; 3) introducing strict control of persons and vehicles at the entrance and entry to the premises of the foreign post; 4) strengthening the security service of the foreign post and increasing the frequency of patrolling the facilities included in the security plans; 5) introducing 24-hour manned surveillance of places subject to security; 6) reviewing the available medical facilities and resources with a view to their use in the event of a terrorist attack or sabotage; 7) preparing, in line with the list referred to in ALFA alert level - point 28, for destruction of documents and items deemed important due to the interest of the Republic of Poland which have not been destroyed after the introduction of BRAVO alert level and have not been earmarked for evacuation; 8) carrying out the withdrawal of part or all of the cash at the disposal of a foreign post from banks, after agreement with the Ministry of Foreign Affairs; 9) preparing the foreign post for total evacuation; 10) carrying out a partial evacuation of members of the personnel of the foreign post whose departure will not disrupt the operation of the foreign post and their families;

		11) checking the possibility of hiding members of the personnel of the foreign post outside the building of the post and obtaining confirmation in this regard from the local authorities; 12) terminating the employment contracts of local staff or removing them completely from the substantive tasks of the foreign post; 13) securing documents, objects and cultural property in accordance with a predetermined list; 14) accommodating in the facilities of the foreign post the members of staff (excluding local staff) residing in particularly endangered places; 15) determining the main preparatory undertakings related to the suspension of the activities of the foreign post or its liquidation; 16) preparation for evacuation of selected classified material, log books and destruction protocols referred to at ALFA alert level in point 26
DELTA	1) implementing, where justified, traffic restrictions in at-risk areas; 2) carrying out identification of all vehicles already in the area of the facility and, where justified, relocating them out of the area of the facility; 3) controlling all vehicles entering the facility area and their load; 4) inspecting all items brought into the premises, including suitcases, bags, parcels; 5) carrying out frequent checks outside the building and in car parks; 6) limiting the number of business trips by persons employed at the facility and visits by persons not employed at the institution; 7) preparing to ensure the continuity of the authority's operations in the event that it is not possible to carry out its tasks at its current place of work	1) providing logistical and medical-sanitary facilities, appropriate to the scale of the possible threat; 2) evacuating the foreign post and, if that is not possible, destroying classified material, logbooks and destruction reports in line with the list referred to at alert level ALFA - point 28; 3) notifying the competent authorities of the host country of the temporary suspension of activities of the foreign post or the intention to temporarily suspend activities and evacuate the personnel of the post or part of them, as well as requesting protection along the evacuation route and facilitation of border crossings;

		4) agreeing with the Ministry of Foreign Affairs on the scope of the evacuation, the place, date and manner of the evacuation, the manner of dealing with the property left behind, the political tasks, and the organisation of communications until the evacuation is completed; 5) carrying out a complete evacuation of a foreign post on the order of the Chairman of the Crisis Management Team at the Ministry of Foreign Affairs or his deputy; 6) in the event of a lack of communication with the Ministry of Foreign Affairs, taking the evacuation decision independently

Source: Own elaboration based on the Ordinance of the Prime Minister of 25 July 2016 on the scope of undertakings carried out in particular alert levels and CRP alert levels and the Ordinance of the Minister of Foreign Affairs of 7 June 2022 on the detailed scope of undertakings carried out by managers of foreign posts of the Republic of Poland in particular alert levels or CRP alert levels.

Table 2. Scope of undertakings provided for in the regulations for CRP alert levels.

CRP alert level	Tasks of public administration bodies and heads of services and institutions responsible for security and crisis management[a]	Tasks of heads of foreign posts[b]
ALFA-CRP	1) introducing increased monitoring of the state of security of information and communication systems of public administration bodies or information and communication systems forming part of the critical infrastructure, hereinafter referred to as „systems", in particular using the recommendations	1) informing members of the personnel of the foreign post and their family members of the introduction of an appropriate CRP alert level; 2) introducing on-call duties for members of the personnel of the foreign post responsible for the security of information and communication systems or for the performance of tasks related

[a] Annex of the Ordinance of the Prime Minister of 25 June 2016.

[b] Annex 2 of the Ordinance of the Minister of Foreign Affairs of 7 June 2022.

	of the Head of the Internal Security Agency or units responsible for the response system in accordance with the jurisdiction, and monitoring and verifying that the security of electronic communication has not been breached, checking the availability of electronic services, making changes to the access to the systems, if necessary; 2) informing the institution's staff of the need to be more vigilant to abnormal states, especially the staff in charge of systems security; 3) checking the channels of communication with other emergency responders appropriate to the type of CRP alert level, verifying the established points of contact with the ICT security incident response teams appropriate to the type of operation of the organisation and the minister responsible for information technology; 4) reviewing the relevant procedures and tasks related to the implementation of CRP alert levels, in particular verifying the systems backup in relation to information and communication systems included in the critical infrastructure and systems crucial for the functioning of the organisation, and verifying the time required for the system to be restored to proper functioning; 5) verifying the current state of security of the systems and assessing the impact of threats to information and communication security on the basis of current information and event forecasts; 6) informing, on an ongoing basis, the ICT security incident response teams competent for the type of operation of the organisation and the cooperating crisis management centres, as well as the minister in charge of IT	to the security of the post in order to analyse and assess states deviating from the accepted standards; 3) 3checking channels of communication with other crisis response entities appropriate to the type of CRP alert level, with employees of the department responsible for responding to information and communication security incidents in the cell responsible for information and communication security at the Ministry of Foreign Affairs, and with other entities providing support in the subject area; 4) keeping the director of the organisational unit in charge of information and communication security at the Ministry of Foreign Affairs and employees of this unit responsible for matters of responding to information and communication security incidents informed on an ongoing basis about the effects of the actions conducted
BRAVO-CRP	1) ensuring that personnel responsible for the security of systems are available on an emergency basis;	1) ensuring readiness for immediate action by members of the personnel of the foreign post who are responsible for the security

	2) introducing a 24-hour on-call service for administrators of systems critical to the functioning of the organisation and personnel authorised to make decisions on matters of security of information and communication systems	of information and communication systems or for carrying out tasks related to the security of the post; 2) if necessary, making changes to access to ICT infrastructure in agreement with the director of the organisational unit in charge of ICT security at the Ministry of Foreign Affairs and employees of this unit responsible for matters of responding to ICT security incidents
CHARLIE--CRP	1) introducing a 24-hour on-call service for administrators of systems critical to the functioning of the organisation and personnel authorised to make decisions on system security matters; 2) reviewing available back-up resources with regard to the possibility of their use in the event of an attack; 3) preparing to put in place plans to enable business continuity after a potential attack has occurred, including: reviewing and possibly auditing contingency plans and systems, preparing to limit operations on servers so that they can be shut down quickly and without failure	preparing to limit operations on servers in order to shut them down quickly and without fail, with the prior approval of the director of the organisational unit in charge of ICT security at the Ministry of Foreign Affairs or employees of this unit responsible for matters of responding to ICT security incidents
DELTA-CRP	1) activating the organisation's contingency or business continuity plans in situations of failure or loss of business continuity; 2) initiating business continuity recovery procedures as appropriate	no additional tasks have been defined for the DELTA-CRP level only

Source: Own elaboration based on the Regulation of the Prime Minister of 25 July 2016 on the scope of undertakings carried out in particular alert levels and CRP alert levels and the Regulation of the Minister of Foreign Affairs of 7 June 2022 on the detailed scope of undertakings carried out by managers of foreign posts of the Republic of Poland in particular alert levels or CRP alert levels.

In the context of linking legislation to the alert level system, it is also worth noting the solutions adopted in the Act of 5 July 2018 on the national cyber security system[28]. Pursuant to Article 36(7)(5) of that Act, the Critical

[28] Consolidated text: Journal of Laws of 2020, item 1369, as amended.

Incidents Team, which is an auxiliary body for handling critical incidents[29] notified to CSIRT MON, CSIRT NASK or CSIRT GOV[30] and coordinating actions taken by them and the Government Centre for Security, (...) *in the case of a critical incident that may result in a threat of a terrorist event concerning ICT systems of public administration bodies or ICT systems that are part of critical infrastructure, referred to in Art. 15(2) of the Act of 10 June 2016 on anti-terrorist activities* (CRP alert levels), *prepares, with regard to such an incident, information and conclusions for the minister in charge of internal affairs and the Head of the Internal Security Agency.*

Introduction of alert levels – analysis of cases

The speed of the legislative process related to the preparation of the Act on anti-terrorist activities, as well as the date with which the Act entered into force - pursuant to Article 65 of the Act, with the exception of one article, it entered into force with a vacatio legis shortened in relation to the standard one, and resulting from the Act of 20 July 2000 on promulgation of normative acts and certain other legal acts[31], *vacatio legis*, i.e. after the lapse of seven days from the date of promulgation - were related to the desire of the proponent, in this case the Council of Ministers[32], to introduce new solutions before specific events held in Poland in 2016: The NATO Summit in Warsaw and the 31st World Youth Day in Kraków.

[29] Critical incident - an incident resulting in significant damage to security or public order, international interests, economic interests, operation of public institutions, civil liberties and rights or human life and health, classified by the relevant CSIRT MON, CSIRT NASK or CSIRT GOV. CSIRT - Computer Security Incident Response Team, explanation of names in the next footnote (editor's note).

[30] CSIRT MON - Computer Security Incident Response Team operating at the national level, led by the Minister of National Defence; CSIRT NASK - Computer Security Incident Response Team operating at the national level, led by the Scientific and Academic Computer Network - National Research Institute; CSIRT GOV - Computer Security Incident Response Team operating at the national level, led by the Head of the Internal Security Agency.

[31] Consolidated text: Journal of Laws of 2019, item 1461. Standard *vacatio legis* - 14 days after the date of announcement - Article 4(1) of the Act on announcement of normative acts and certain other legal acts.

[32] Government project, which was prepared under the responsibility of the Chancellery of the Prime Minister, in cooperation with the Ministry of Interior and Administration - Regulatory Impact Assessment for the draft Act on anti-terrorist activities.

These events, which were particularly difficult in terms of guaranteeing the necessary security measures, were not only organised on the basis of specific and episodic legislation[33], but also required specific solutions of a systemic nature. The aforementioned events thus became a catalyst for the implementation of a comprehensive reorganisation of legal solutions with regard to the Polish anti-terrorist system. It is worth noting that the original government draft in the version addressed to the Sejm contained an even shorter deadline for the Act to enter into force - the day following the day of announcement, but due to constitutional standards it was prolonged.

Although the justification for the Act on anti-terrorist activities does not directly indicate that the date of entry into force of the Act is closely linked to the aforementioned events, this is obvious both in the context of the course of the parliamentary debate and the normative side itself. Indeed, the Act on anti-terrorist activities amended the Act on special solutions concerning the organisation of the visit of His Holiness Pope Francis to the Republic of Poland and the World Youth Day - Kraków 2016.

In this context, it can be concluded that the legal institution of alert levels was used for the first time on the basis of the provisions of the Act on anti-terrorist activities as part of the safeguards for the aforementioned events.

In the period when alert levels were standardised in orders issued on the basis of the Crisis Management Act, i.e. prior to the entry into force of the Act on anti-terrorist activities, alert levels were introduced only once - in relation to the organisation in Poland of the UEFA EURO 2012 Final Tournament. The introduction of the alert level at that time was connected with the discovery by the Border Guard of a package containing explosives and a telephone with a photograph of the National Stadium, which were placed on a raft floating on the Bug River[34]. As a spokesman for

[33] Act of 18 March 2016 on special solutions related to the organisation of the visit of His Holiness Pope Francis to the Republic of Poland and World Youth Day - Kraków 2016 (i.e. Journal of Laws of 2017, item 685) and Act of 16 March 2016 on special arrangements related to the organisation of the 2016 North Atlantic Treaty Organisation Summit in the Republic of Poland in Warsaw (i.e. Journal of Laws of 2016, No item. 379, as amended).

[34] Cf.: *Tusk: Stopień alarmowy nie zmienia poziomu bezpieczeństwa na Euro 2012* (Eng. Tusk: The alert level does not change the level of security at Euro 2012), Dziennik Gazeta Prawna, 28 VI 2012, https://www.gazetaprawna.pl/wiadomosci/artykuly/628995,tusk-stopien-alarmowy-nie-zmienia-poziomu-bezpieczenstwa-na-euro-2012.html [accessed: 2 VII 2022]; *Pierwszy stopień alarmowy w Polsce. Grozi nam zamach?* (Eng. First alert level

the Ministry of the Interior at the time pointed out: *After analysing the case, it was concluded that there is no threat to the safety of persons or places in Poland. However, taking into account the fact that this is the first such significant signal during Euro 2012 concerning the possibility of a terrorist event, it was decided to introduce the first alert level on a four-stage scale*[35].

On the basis of the Act on anti-terrorist activities, alert levels, in addition to the levels referred to in Article 16(2) of that Act, i.e. with regard to foreign posts of the Republic of Poland and the ICT systems of the minister responsible for foreign affairs, were introduced in the following cases[36]:

- **NATO Summit in Warsaw, 2016** - the first alert level (ALFA) was introduced in the area of the capital city of Warsaw, which was in force from 7 to 10 July 2016;
- **31st World Youth Day in Kraków, 2016** - the first alert level (ALFA) and the second CRP alert level (BRAVO-CRP) were introduced on the entire territory of the Republic of Poland, which were in force from 20 July to 1 August 2016;
- **24th session of the Conference of the Parties to the UN Framework Convention on Climate Change (COP24) in Katowice, 2018** - the first alert level (ALFA) was introduced in the area of the Silesian Voivodeship and the city of Kraków, which was in force from 26 November to 15 December 2018;
- **Ministerial meeting on security in the Middle East in Warsaw, 2019** - the first alert level (ALFA) and the second CRP alert level (BRAVO-CRP) were introduced in the area of the capital city of Warsaw, effective from 11 to 15 February 2019;
- **European Parliament elections, 2019** - the second CRP alert level (BRAVO-CRP), which was in force from 23 to 27 May 2019, was introduced throughout the territory of the Republic of Poland;

in Poland. Are we in danger of an attack?), Wprost, 28 VI 2012, https://sport.wprost.pl/euro-2012/330817/pierwszy-stopien-alarmowy-w-polsce-grozi-nam-zamach.html [accessed: 2 VII 2022].

[35] *Pierwszy stopień alarmowy. Znaleźli ładunki wybuchowe* (Eng. First alert level. They found explosives), TVN24, 27 VI 2012, https://tvn24.pl/polska/pierwszy-stopien-alarmowy-znalezli-ladunki-wybuchowe-ra261245-3500262 [accessed: 2 VII 2022].

[36] *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: 2 VII 2022].

- **commemoration of the 80th anniversary of the outbreak of World War II, 2019** - the first alert level (ALFA) and the first CRP alert level (ALFA-CRP), which were in force from 28 August to 3 September 2019, were introduced throughout the Polish territory;
- **Sejm and Senate elections, 2019** - a second CRP alert level (BRAVO-CRP) was introduced on the territory of the Republic, which was in force from 10 to 14 October 2019;
- **ceremonies commemorating the 75th anniversary of the liberation of the Auschwitz-Birkenau German Nazi concentration and extermination camp, 2020** - the second alert level (BRAVO) was introduced in the Małopolskie Voivodeship, the first alert level (ALFA) was introduced in the remaining territory of the Republic of Poland; additionally, the first CRP alert level (ALFA-CRP) was introduced in the entire territory of the Republic of Poland. The alert levels were in force from 23 to 29 January 2020;
- **election of the President of the Republic of Poland, 2020** - a second CRP alert level (BRAVO-CRP) was introduced throughout the Republic of Poland, effective from 26 to 29 June 2020 and from 10 to 13 July 2020;
- **UN Digital Summit - IGF 2021 (the UN Internet Governance Forum) in Katowice, 2021** - the first CRP alert level (ALFA-CRP) was introduced across the entire territory of the Republic of Poland, which was in force from 5 to 10 December 2021;
- **the occurrence of a potential risk to the security of ICT systems due to identified threats resulting from the tense situation in the region:**
  - the first CRP alert level (ALFA-CRP) was introduced across the entire territory of Poland, which was in force from 18 to 23 January 2022 and from 15 to 21 February 2022;
  - a third CRP alert level (CHARLIE-CRP) was introduced across the entire territory of the Republic of Poland, which is in force from 21 February 2022 to 30 November 2022;
- **the occurrence of an increased and foreseeable threat of a terrorist event resulting from a mass influx of refugees from Ukraine to the territory of the Republic of Poland:**
  - on the territory of the Lubelskie and Podkarpackie Voivodeships, the second alert level (BRAVO) was introduced, which was in force from 28 February to 15 April 2022;

- on the entire territory of the Republic of Poland, the second alert level (BRAVO) was introduced, which is in force from 16 April 2022 until 30 November 2022.

Having analysed this overview, it can be concluded that in the vast majority of cases the introduction of the alert level was associated with the organisation in Poland of important events of international dimension or with the participation of representatives of other countries (a total of seven such cases). The nature of these events varied, as did the role of Poland and the state authorities in them - from the organiser (e.g. the celebrations of the 80th anniversary of the outbreak of World War II), co-organiser (e.g. the ministerial meeting on security in the Middle East co-organised with the United States of America, which took place in Warsaw) to the host state or even providing access to its territory, while the event itself was of a quasi-extraterritorial nature (COP24 or IGF 2022, whose organisers were various United Nations agencies).

Alert levels were also introduced on three occasions in connection with elections, while in 2022 they were introduced and then extended (on the basis of separately issued orders of the Prime Minister) due to the situation beyond Poland's eastern border.

The last of these cases is distinct from the previous ones. The first difference is that the alert levels were not introduced as a result of the planned organisation of a particular type of event, such as celebrations, international meetings or elections, but in the context of events beyond the control of the Polish authorities. These events include a deliberate attack by Belarus against Poland and the European Union in general, in the form of a deliberately caused and top-down driven migration crisis on the Polish-Belarusian border, which is at the same time the external border of the EU, to be seen as a hybrid attack. The second event resulting in the introduction of alert levels is the armed attack by the Russian Federation on Ukraine and the resulting consequences - on the one hand, the unprecedented influx of refugees to Poland from the conflict area (Ukraine), and on the other hand, the threat of various types of hybrid actions from Russia, also in cyber space.

The second key difference from the previous circumstances surrounding the introduction of alert levels is the period for which they were adopted. Here, for the first time, they are in force not for a few days or a dozen days, but for several months. As rightly pointed out by the authors

of the commentary to the Act on anti-terrorist activities Paweł Łabuz, Tomasz Safjański and Waldemar Zubrzycki:

> Alert levels and CRP alert levels are introduced in justified cases, however, they entail numerous impediments to the functioning of various institutions as well as citizens. Undoubtedly, their implementation also has a huge impact on the functioning of services and formations responsible for ensuring the security of citizens and facilities of the Republic of Poland, also operating in an alert mode, i.e. unusual and unnatural, with regard to abnormal and unconventional situations. Maintaining such a state in the long term will cause significant disruptions to their functioning and may also prove impossible. Therefore, alert levels shall be revoked as soon as the threat or impact of the event that prompted the alert level has been minimised. This may mean either lifting it completely or lowering the alert level on a multi-level scale[37].

In the case in question, the rationale for the alert level existed for an extended period of time, justifying the maintenance of this level with all its functional challenges for public administration bodies and heads of services and institutions competent in security and crisis management matters, but also, to a certain extent, for the owners, sole holders and dependent holders of critical infrastructure facilities. At the same time, the proclamation of an alert level for a prolonged period of time is subject to the potential risk of routine and thus a decrease in concentration in the implementation of legal undertakings at the individual level, whereas alert levels are precisely intended to provide a heightened degree of preparedness.

From a subject perspective, it can be pointed out that levels have been introduced in various configurations, i.e. both alert levels sensu stricto (e.g. NATO Summit 2016 or COP24) and CRP alert levels (e.g. the aforementioned elections) on their own, as well as both types of alert levels at the same time (e.g. World Youth Day) depending on the nature of the threat. When combining alert levels sensu stricto and CRP alert levels, usually the CRP alert level was higher on the four-level scale. It is also worth noting that in the case of alert levels sensu stricto, the highest one introduced so far is the second alert level BRAVO, while in the case of CRP alert levels, the third alert level CHARLIE-CRP was used.

---

[37] P. Łabuz, T. Safjański, W. Zubrzycki, *Ustawa o działaniach antyterrorystycznych. Komentarz*...

Alert levels are therefore a repeatedly used instrument in the preventive dimension - they have so far been used as a tool to raise the level of preparedness in the event of a terrorist event and not as a consequence of a terrorist event. In turn, authorised authorities declare alert levels in a flexible manner, including with regard to:

- the type of circumstances giving rise to their introduction - from safeguarding planned undertakings to responding to external threats;
- territorial scope - applied on the territory of the entire country or specific areas thereof, such as cities or voivodeships, as well as in some Polish outposts abroad;
- determination of the level within a four-grade scale - from the first alert level ALFA to the second alert level BRAVO, and from the first alert level ALFA-CRP to the third alert level CHARLIE-CRP;
- the type of levels applied - alert levels stricto sensu and CRP alert levels separately and in combination;
- temporality - the duration adapted to the event to which they are linked or the duration of the threat concerned;
- appropriateness - there have been instances of increasing the level or changing its territorial scope.

Relevance of solutions – summary

The effectiveness of the mechanisms for the introduction of the alert levels and the relevance of the undertakings carried out after the introduction of the levels was assessed several times within the Interministerial Team for Terrorist Threats[38]. However, the members of the Team did not make any proposals for changes in this respect, which may prove the correct construction of the institution of alarm levels.

The system of alert levels established on the basis of the provisions of the Act on anti-terrorist activities was positively evaluated during the visit of the Executive Directorate of the United Nations Counter-Terrorism Organisation (UN CTED) in December 2019. Its purpose was to evaluate

[38] Established by Order No. 162 of the Prime Minister of 25 October 2006 on the establishment of the Interministerial Team for Terrorist Threats [legal basis for the establishment of the Team: Article 12(1)(3) and (2) of the Act of 8 August 1996 on the Council of Ministers (i.e. Journal of Laws of 2022, item 1188) - editor's note].

the UN Security Council counter-terrorism resolutions implemented into the Polish legal system[39].

The authors also agree with the position expressed by Piotr Chorbot that the benefit of the introduction of provisions on alert levels and the creation of appropriate behavioural algorithms based on them is the opportunity to practice the coordination of actions of relevant services and other entities, and (...) *any provisions established to create the right attitudes and consisting in the practice of responses to a threat allow better preparation of services to act, and thus - to increase the standard of security of the Republic of Poland*[40].

Having analysed the speed of activation of the procedure on the introduction of alert levels, it remains worth considering the implementation of a provision unambiguously indicating that the motions and opinions referred to in Article 16 item 1 and 2 of the Act on anti-terrorist activities (motions and opinions of the minister in charge of internal affairs and the Head of the Internal Security Agency constituting the basis for issuing an order for the introduction of the alert level), delivered also orally, by telephone, by means of electronic communication within the meaning of Article 2 item 5 of the Act of 18 July 2002 on provision of services by electronic means[41] or by other means of communication - are deemed to be delivered in an effective manner. Their content and the relevant motives for such settlement shall be recorded in writing. This solution, which is already familiar to national legislation[42], would make it possible to guarantee speed and efficiency without waiting for the circulation of documents. Although the Act on anti-terrorist activities does not directly indicate the obligation of a written form of presenting the required motions and opinions, taking into account the consequences of the introduction of the level and possible limitations of citizens' freedoms and rights (e.g. prohibition of organising assemblies and mass events - Article 21 of the Act), it seems

[39] Cf.: M. Cichomski, I. Idzikowska-Ślęzak, *Strategic level of the Polish anti-terrorist system - 15 years of the Interministerial Team for Terrorist Threats,* "Terroryzm – studia, analizy, prewencja" 2022, no. 1, p. 306.

[40] P. Chorbot, *Ustawa o działaniach antyterrorystycznych. Komentarz...*, p. 73.

[41] Consolidated text: Journal of Laws of 2020, item 344.

[42] For example, art. 11h(11) of the Act of 2 March 2020 on specific solutions related to the prevention, prevention and control of COVID-19, other infectious diseases and emergencies caused by them (i.e. Journal of Laws of 2021, item 2095, as amended).

that the proposed solution would be significant and would guarantee the effectiveness of the activities carried out.

The provisions of the Act should also unambiguously indicate which body is competent to fulfil the information obligations (listed in Article 16(3) of the Act on anti-terrorist activities) towards the President of the Republic of Poland, the Marshal of the Sejm and the Marshal of the Senate - in the case of the introduction of the alert level in a special mode, i.e. in a case of urgency.

Another topic is the possible, mentioned in the earlier part of the study, clarification of Article 16(4) of the Act, according to which the introduction of the alert level or CRP alert level is the basis for the implementation by public administration bodies and heads of services and institutions competent in matters of security and crisis management of a certain type of undertakings (among others, explicitly indicating among the addressees of this standard the owners, sole owners and dependent owners of critical infrastructure facilities). The current wording of this provision does not correlate with the wording of the implementing regulations issued on the basis of paragraph 5 of this Article. The Prime Minister's Regulation of 25 July 2016 takes into account the role of owners, sole holders and dependent holders of critical infrastructure facilities. This solution reflects the *ratio legis* of the legislator.

With regard to this regulation, in addition to the legal-legislative doubts described in the earlier section, it is also worth pointing out that at least two of the projects contained therein:

- the introduction of a ban on outsiders entering kindergartens, schools and public universities - in the event of the introduction of a second or higher alert level,
- introduction, on the recommendation of the minister in charge of internal affairs, of 24-hour standby services in indicated offices or organisational units of public administration bodies - envisaged for the third alert level

should ultimately become statutory norms.

The first of the undertakings - as encroaching into the sphere of civil liberties and rights - may be implemented in order to fulfil the obligation resulting from Article 31(3) of the Constitution of the Republic of Poland, according to which limitations on the use of constitutional freedoms and rights may be established only by statutory law and only when they are necessary in a democratic state for its security or public order,

for the protection of the environment, health and public morals or the freedoms and rights of other persons. The second one - when there is a need to extend the competences of the minister in charge of internal affairs to entities that are not subordinate to him and are not supervised by him. Moreover, the issues related to the circulation of information on alert levels, included in the regulation referred to above, should find their precise basis in the statutory authorisation.

The directions of possible changes indicated above, however, are only of a supplementary or strictly legal nature and do not affect the overall assessment of the alert levels, which have become one of the most essential elements of the Act on anti-terrorist activities, and the multiple use of this legal institution in various circumstances and variants testifies to the effectiveness and adequacy of the adopted solutions.

Bibliography

Chorbot P., *Ustawa o działaniach antyterrorystycznych. Komentarz do niektórych regulacji* (Eng. Act on anti-terrorist activities. Commentary on some regulations), in: *Uprawnienia służb specjalnych z perspektywy współczesnych zagrożeń bezpieczeństwa narodowego. Wybrane zagadnienia* (Eng. The powers of the special services from the perspective of contemporary threats to national security. Selected issues), P. Burczaniuk (ed.), Warszawa 2017.

Cichomski M., Horoszko M., Idzikowska I., *Przygotowanie do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym oraz reagowanie w przypadku wystąpienia takich zdarzeń w świetle rozwiązań ustawy o działaniach antyterrorystycznych – w kontekście zadań resortu spraw wewnętrznych*, (Eng. Preparing to take control over terrorist events and reacting in case of such events in the light of solutions of the act on anti-terrorist actions - in the context of the tasks of the ministry of internal affairs), in: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (ed.), Szczytno 2016.

Cichomski M., Idzikowska-Ślęzak I., *Strategic level of the Polish anti-terrorist system - 15 years of the Interministerial Team for Terrorist Threats*, "Terroryzm – studia, analizy, prewencja" 2022, no. 1, pp. 297–319.

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: 2 VII 2022].

Kolory, stopnie i terminologia NATO. Jak odczytać alerty terrorystyczne (Eng. NATO colours, levels and terminology. How to interpret terrorist alerts), TVP Info, 23 III 2016, https://www.tvp.info/24554977/kolory-stopnie-i-terminologia-nato-jak-odczytac-alerty-terrorystyczne [accessed: 7 XII 2018].

Łabuz P., Safjański T., Zubrzycki W., *Ustawa o działaniach antyterrorystycznych. Komentarz* (Eng. The Act on anti-terrorist activities. Commentary), Warszawa 2019, access through the Legal Information System Legalis, sip.legalis.pl [accessed: 20 VII 2022].

Pierwszy stopień alarmowy w Polsce. Grozi nam zamach? (Eng. First alert level in Poland. Are we in danger of an attack?), Wprost, 28 VI 2012, https://sport.wprost.pl/euro-2012/330817/pierwszy-stopien-alarmowy-w-polsce-grozi-nam-zamach.html [accessed: 2 VII 2022].

Pierwszy stopień alarmowy. Znaleźli ładunki wybuchowe (Eng. First alert level. They found explosives), TVN24, 27 VI 2012, https://tvn24.pl/polska/pierwszy-stopien-alarmowy-znalezli-ladunki-wybuchowe-ra261245-3500262 [accessed: 2 VII 2022].

Tusk: Stopień alarmowy nie zmienia poziomu bezpieczeństwa na Euro 2012 (Eng. Tusk: The alert level does not change the level of security at Euro 2012), Dziennik Gazeta Prawna, 28 VI 2012, https://www.gazetaprawna.pl/wiadomosci/artykuly/628995,-tusk-stopien-alarmowy-nie-zmienia-poziomu-bezpieczenstwa-na-euro-2012.html [accessed: 2 VII 2022].

Uzasadnienie do projektu ustawy o działaniach antyterrorystycznych (Eng. Explanatory memorandum to the draft Act on anti-terrorist activities), https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=516 [accessed: 2 VII 2022].

Legal acts

Constitution of the Republic of Poland of 2 April 1997 (i.e. Journal of Laws of 1997, No. 78, item 483, as amended).

Act of 11 March 2022 on defence of the homeland (Journal of Laws of 2022, item 655, as amended).

Act of 21 January 2021 on the foreign service (i.e. Journal of Laws of 2022, item 1076, as amended).

Act of 2 March 2020 on special solutions related to the prevention, prevention and combating of COVID-19, other infectious diseases and crisis situations caused by them (i.e. Journal of Laws of 2021, item 2095, as amended).

Act of 5 July 2018 on the national cyber security system (i.e. Journal of Laws of 2020, item 1369, as amended).

Act of 10 June 2016 on anti-terrorist activities (i.e. Journal of Laws of 2021, item 2234, as amended).

Act of 18 March 2016 on special solutions related to the organisation of the visit of His Holiness Pope Francis to the Republic of Poland and World Youth Day - Kraków 2016 (i.e. Journal of Laws of 2017, item 685).

Act of 16 March 2016 on special solutions related to the organisation of the 2016 North Atlantic Treaty Organisation Summit in the Republic of Poland in Warsaw (i.e. Journal of Laws of 2016, item 379, as amended).

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

Act of 20 March 2009 on safety of mass events (i.e. Journal of Laws of 2022, item 1466, as amended).

Act of 26 April 2007 on crisis management (i.e. Journal of Laws of 2022, item 261, as amended).

Act of 29 August 2002 on martial law and on the competences of the Commander-in-Chief of the Armed Forces and the principles of his subordination to the constitutional bodies of the Republic of Poland (i.e. Journal of Laws of 2017, item 1932, as amended).

Act of 18 July 2002 on provision of services by electronic means (i.e. Journal of Laws of 2020, item 344).

Act of 21 June 2002 on the state of emergency (i.e. Journal of Laws of 2017, item 1928).

Act of 18 April 2002 on the state of natural disaster (i.e. Journal of Laws of 2017, item 1897).

Act of 20 July 2000 on promulgation of normative acts and certain other legal acts (i.e. Journal of Laws of 2019, item 1461).

Act od 6 June 1997 - Criminal Code (i.e. Journal od Laws of 2022, item 1138).

Act of 6 April 1990 on the Police (i.e. Journal of Laws of 2021, item 1882, as amended).

Ordinance of the Minister of Foreign Affairs of 7 June 2022 on the detailed scope of undertakings carried out by managers of foreign posts of the Republic of Poland in particular alert levels or CRP alert levels (Journal of Laws of 2022, item 1251).

Ordinance of the Prime Minister of 4 March 2022 amending the Ordinance on the scope of undertakings performed in particular alert levels and CRP alert levels (Journal of Laws of 2022, item 538).

Ordinance of the Prime Minister of 25 July 2016 on the scope of undertakings carried out in particular alert levels and CRP alert levels (Journal of Laws of 2016, item 1101).

Order No. 16 of the Minister of Internal Affairs and Administration of 2 July 2019 on the implementation of tasks related to the opinion, introduction, change or cancellation of CRP alert levels or alert levels (unpublished).

Order No. 18 of the Prime Minister of 2 March 2016 on the list of undertakings and procedures of the crisis management system, https://www.stawiguda.pl/userfiles/OC/Komunikaty_zew/Zarz%C4%85dzenie%20nr%2018%20Prezesa%20Rady%20Ministr%C3%B3w%20z%20dnia%202%20marca%202016%20r.pdf.

Order No. 74 of the Prime Minister of 12 October 2011 on the list of undertakings and procedures of the crisis management system (unpublished).

Order No. 162 of the Prime Minister of 25 October 2006 on the establishment of the Interministerial Team for Terrorist Threats, amended by Order No. 95 of the Prime Minister of 4 September 2008, Order No. 74 of the Prime Minister of 21 September 2009, Order No. 18 of the Prime Minister of 3 April 2014, Order No. 84 of the Prime Minister of 18 September 2015, Order No. 86 of the Prime Minister of 5 July 2016, Order No. 32 of the Prime Minister of 27 April 2017, Order No. 160

of the Prime Minister of 9 November 2017, Order No. 92 of the Prime Minister of 7 June 2018 and Order No. 37 of the Prime Minister of 8 April 2021.

Notice of the Prime Minister of 27 July 2016 on the correction of errors (Journal of Laws of 2016, item 1116).

DOI: 10.4467/27204383TER.22.026.16346

ORCID: 0000-0003-1514-7657

MICHAŁ PIEKARSKI

Possible scenarios of terrorist attacks in Republic of Poland in the context of hybrid threats

Abstract

The article analyzes the problem of employment of terrorist attacks as tools of hybrid warfare. Using scenario-based forecasting, possible scenarios of terrorist attacks as part of hybrid warfare on the territory of the Republic of Poland were generated and analyzed.

Keywords:

terrorism, terrorist attack, hybrid warfare

In connection with the situation in Ukraine, on 28 February 2022, the Bravo alert level was introduced in Poland, for the first time since the entry into force of the Act of 10 June 2016 on anti-terrorist activities[1], on the territory of two provinces - Podkarpackie and Lubelskie. On 15 April 2022, its duration was extended and its territorial coverage was extended to the whole country. At the time of writing this article, the duration was extended until the end of June. The introduction of the Bravo alert level is interesting in terms of research on potential terrorist threats on the territory of the Republic of Poland. Taking such decisions means that, pursuant to the act, there was (...) *an increased and foreseeable threat of a terrorist event*[2]. In this situation the question arises as to what is the possible nature of such a threat in the light of the current international situation, primarily the aggressive policy of the Russian Federation.

---

1 Consolidated text: Journal of Laws of 2021, item 2234, as amended.

2 Act on anti-terrorist activities, Article 15(4).

The aim of this article is to indicate and discuss the scenarios of terrorist threats on the territory of Poland in the context of hybrid threats. Searching for an answer to the research question posed is in itself a methodological challenge, since no terrorist events have occurred, but only we are dealing with an increased risk of their occurrence. This means that the answer will be predictive in nature. Therefore, the methodological basis for the research is the scenario-based forecasting method, which consists in ing, by means of scenarios, the possible course of future trends and assessing their impact on the currently diagnosed problem. Scenarios are structured descriptions of trends and their impact on the studied area, and the result of their application is a description of a possible final state or - more often - several possible final states. This method is used, among others, in security or economic es[3]. The literature gives several different, although in some respects similar, stages in the process of scenario development and es. Jay Ogilvy, for example, distinguishes eight of them, starting with the initial activities and ending with the implementation of conclusions. These are:

1. Identification of the Focal Issue.
2. Identification of key factors.
3. Description of external factors.
4. Identification of critical uncertainties.
5. Description of the internal logic of the scenario.
6. Development of the scenarios themselves.
7. es of implications and available choices.
8. es of early indicators that distinguish the scenarios.

In comparison, Hannah Kosow and Robert Gaßner give five stages. These include:

1. Identification of the scenario field.
2. Identification of the most important factor.
3. rs of the most important factor.
4. Generation of scenarios.
5. Scenario transfer (application)[4].

---

[3] More widely in: J. Ogilvy, *Scenario Planning and Strategic Forecasting*, Forbes, 8 I 2015, https://www.forbes.com/sites/stratfor/2015/01/08/scenario-planning-and-strategic-forecasting/?sh=2de3fee5411a [accessed: 18 V 2022].

[4] H. Kosow, R. Gaßner, *Methods of Future and Scenario es. Overview, Assessment, and Selection Criteria*, https://www.die-gdi.de/uploads/media/Studies_39.2008.pdf [accessed: 22 VI 2022].

The main topic of the scenario therefore needs to be identified first. In the case of the research described in this article, this was an easy task as it was formulated in the research question. It also reveals the most important factor affecting the ed scenarios, i.e. the possible use of terrorist attacks in hybrid actions conducted by Russia on the territory of Poland. It is therefore necessary to e the issue of hybrid actions and the use of terrorist tools in them. This will enable the construction of scenarios and subjecting them to es, and will allow to assess the possible use of the resources of the state security system, and above all its integral part - the anti-terrorist system.

The description of the most important factors and the construction of scenarios was made on the basis of two sets of information. The first is available, reliable information on Russia's policy to date and its use of force in international relations. The second is information on possible ways of carrying out terrorist attacks, both on a broader, strategic scale, and on the tactical and technical level.

The scenario method has already been used in the es of the Polish anti-terrorist system[5]. Using it, challenges related to the contemporary nature of this type of threats were clearly presented. An additional value is the ease of adaptation of this type of es to training and didactic needs[6].

Hybrid threat es in the context of terrorist threats - general remarks

There is no single, precise, generally accepted definition of hybrid threats in the literature. The way they are perceived has undoubtedly been influenced by two armed conflicts. The first was Israel's war with Hezbollah, which some ts have called hybrid[7]. The second, resulting in a more frequent and wider use of the term, is the events in Ukraine beginning in 2014. This is because the annexation of Crimea was carried out with military units using limited force, initially appearing without nationality markings. After this

[5] M. Piekarski, K. Wojtasik, *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku* (Eng. The Polish anti-terrorist system and the reality of attacks in the second decade of the 21st century), Toruń 2020, pp. 158–207.

[6] See J. Sovolainen i in., *Hybrid CoE Working Paper 5. Handbook On Maritime Hybrid Threats – 10 Scenarios and Legal Scans,* https://www.hybridcoe.fi/wp-content/uploads/2020/07/NEW_Handbook-on-maritime-threats_RGB.pdf [accessed: 29 IV 2022].

[7] F. Hoffman, *Conflict in the 21st Century: The Rise of the Hybrid Wars,* https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf [accessed: 29 IV 2022].

success, the Russians began operations in the Donbass, in which they used irregular armed formations, composed of both local pro-Russian volunteers or mercenaries, as well as special forces soldiers and regular forces sent from Russia, although officially it did not take an active part in this war[8]. This does not mean, however, that hybrid threats are discussed only in the context of these two conflicts. There are works devoted to broader es of the concept and contexts of its use. For example, Robert Seely in a 2017 article points out that the term 'hybrid' in relation to armed conflict is most often used in one of three contexts: 1) 'frozen', long-running conflicts resulting from Russia's policies in the post-Soviet area, 2) new-generation wars, often identified with theses attributed to the Russian military, particularly Sergei Gerasimov, and 3) kinetic and non-kinetic actions by intelligence services described as active measures[9]. It also characterises the tools used by Russia as belonging to one of six areas: 1) governance (including the spheres of culture, religion and law), 2) economy and energy, 3) politics and political violence, 4) military power, 5) diplomacy, and 6) information and disinformation activities. These broad categories include narrower forms of action - for example, the use of culture, including cultural organisations, for political purposes, the use of energy for energy blackmail, political assassinations, the creation of pro-Russian organisations, including armed ones. Measures falling into the above categories can be used simultaneously. Importantly, there is a blurring of the traditional distinctions between the use of military force and non-military means, and peace and war. This way of using these means by the state leads to the phenomenon of using as weapons (tools of policy) numerous tools and factors, referred to in English as weaponisation. As Mark Galeotti writes, this can manifest itself, among other things, in the use of humanitarian and medical aid, organised crime groups, international law, culture and information for political purposes[10]. The authors of the *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare* report[11] indicate that hybrid threats have the following characteristics:

---

[8] More widely in: L.M. Nadolski, *Kampania zimowa w 2015 roku na Ukrainie* (Eng. Ukraine's 2015 winter campaign), Bydgoszcz 2017, pp. 43–44.

[9] R. Seely, *Defining Contemporary Russian Warfare*, "The RUSI Journal" 2017, vol. 162, no. 1, pp. 50–59.

[10] M. Galeotti, *The Weaponisation of Everything: A Field Guide to The New Way of War*, New York–London 2022.

[11] P.J. Cullen, E. Reichborn-Kjennerud, *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*, The Multinational Capability Development Campaign, 2017, https://

- use a broad spectrum of military, political, economic, civilian and information tools,
- they attack, in a non-traditional manner, areas of society that are vulnerable to attack,
- they synchronise the means used in a novel way,
- intentionally exploit the uncertainty, ambiguity and perceptions of the environment of the state under attack in order to reduce the risk of detection,
- can be spotted and identified at a late stage of implementation.

All these factors do not unequivocally place terrorist threats within hybrid action. However, the possibility of terrorist actions as an element of hybrid actions is pointed out by various researchers of the problem. Przemysław Gasztold and Aleksandra Gasztold indicate that the already mentioned war between Israel and Hezbollah was a conflict between a state and an organization using terrorist methods, which could be used by another state (Iran) to carry out terrorist actions against other states[12]. These authors further note that techniques typical of terrorism are used during the armed conflict in Ukraine.

Interesting observations on hybrid threats can also be found in literature from earlier years. In the article published in 1998 Andrzej Makowski and Krzysztof Kubiak e the possibility of using the military factor in a covert and indirect way in actions conducted in such a way as to make it difficult or impossible to identify their actual organiser. These were actions aimed at important military and economic objects, persons holding key positions in the state in order to create a sense of threat among the inhabitants of the attacked country, undermine their trust in the authorities and state institutions, complicate the international situation and cause social unrest[13]. The authors of this article indicate that such actions may involve residents of the territory of a given state, whom the attacking party will recruit to cooperate, members of foreign terrorist or criminal organisations (de facto mercenaries), as well as soldiers, especially special forces, of the attacking

assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf, p. 10 [accessed: 20 V 2022].

[12] A. Gasztold, P. Gasztold, *The Polish Counterterrorism System and Hybrid Warfare Threats*, "Terrorism and Political Violence" 2020, https://www.tandfonline.com/doi/abs/10.1080/09546553.2020.1777110?journalCode=ftpv20 [accessed: 28 V 2022].

[13] A. Makowski, K. Kubiak, *Terroryzm jako sposób prowadzenia wojny?* (Eng. Terrorism as a way of waging war?), "Raport – wojsko – technika – obronność" 1998, no. 4, pp. 41–43.

state, taking part in actions simulated as actions of local extremist groups. These comments correspond with the content of a 2015 article by Łukasz Skoneczny[14]. He noted that hybrid actions may be used precisely to prevent the use of force from crossing the threshold, as this would be unambiguously interpreted as open aggression and would therefore force the allies of the attacked state to respond, for example. The use of terrorist methods, which this author also includes in the group of measures that can be used in hybrid actions, makes it possible to create an unclear and uncertain situation in terms of response.

However, these general es do not lead to detailed conclusions about possible crisis scenarios. This is because terrorism is a diverse and heterogeneous phenomenon in terms of its strategies and tactics. These result primarily from the ideology of the organisations using terrorist methods, the environment in which they operate, the reaction of the states under attack and other variables. The choice of tactics, in turn, is influenced by current conditions, the broader strategy adopted, the operational situation, training and weaponry, among other factors[15]. An important variable is the conduct of terrorist activities directly or indirectly by the state. Bartosz Bolechów writes about several degrees of state support for terrorist activities, i.e.: full control (state terrorism), recruitment and training of persons for terrorist activities by state bodies, a significant degree of control over a terrorist organisation, providing support to a highly autonomous group, assistance to a de facto independent group, passive support[16]. In the case of hybrid activities, the first four degrees are the most likely to influence the choice of objectives and methods. State support means the provision of training, funding, equipment, reconnaissance information, safe haven and other forms of assistance (e.g. ideological or diplomatic support)[17]. This leads to the important conclusion that such activities supported or carried out by a state actor will be able to be carried out with greater resources than those available to terrorist organisations without such protection. It must therefore be assumed that

[14] Ł. Skoneczny, *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia* (Eng. Hybrid warfare - a challenge of the future? Selected issues), "Przegląd Bezpieczeństwa Wewnętrznego", Special issue: *Wojna hybrydowa*, pp. 39–50.

[15] More widely in: B. Bolechów, *Polityka antyterrorystyczna w świetle badań nad terroryzmem* (Eng. Anti-terrorist policy in the light of terrorism research), Wrocław 2012, pp. 134–174.

[16] Ibid., p. 173.

[17] Ibid., p. 174.

in an es devoted to the conduct of terrorist activities as part of a broader perception of hybrid activities, one of the essential factors that must be taken into account is the involvement of the actors who may support or carry out their hybrid activities or political objectives.

Hybrid operations in Poland's security environment

The es of Poland's security environment shows that currently one of the main factors shaping it is the aggressive actions of the Russian Federation. The current *National Security Strategy of the Republic of Poland* indicates that (...) *the Russian Federation also conducts activities below the threshold of war (of a hybrid nature), carrying the risk of a conflict outbreak (including unintentional, resulting from a rapid escalation as a result of an incident, especially military), and also undertakes comprehensive and complex activities through non-military means (including: cyber attacks, disinformation) to destabilise the structures of Western states and societies and cause divisions among allied states*[18]. Actions below the threshold of war, including those of a hybrid nature, remain, as already mentioned, an important means of conducting policy, serving state and non-state actors to achieve their goals. In Russia's activity, also during the war with Ukraine, there is a visible strategy of restoring and maintaining its former power, as well as perceiving the West as a threat. In order to neutralise this threat, Russia seeks to displace or reduce the American presence in Europe and to minimise European influence and control over the continent. Marek Menkiszak writes that the Russian Federation has set itself four main strategic goals. These are:

1. *Strategic control over the post-Soviet area (with the temporary exclusion of the Baltic states)*.
2. *Creation of a security buffer zone in Central Europe*.
3. *Minimization of US influence and presence in Europe*.
4. *Maximisation of Russia's influence in Europe*[19].

[18] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* (Eng. National Security Strategy of the Republic of Poland), Warszawa 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf, p. 6 [accessed: 22 VI 2022].

[19] M. Menkiszak, *Strategiczna kontynuacja, taktyczna zmiana. Polityka bezpieczeństwa europejskiego Rosji* (Eng. Strategic continuity, tactical change. Russia's European security policy), Warszawa 2019, p. 12.

Their achievement would enable the creation of a new European security architecture in which Russia would play an important economic and political role. Hybrid actions are one of the tools for exerting pressure on the states of the region. Their aim may be to force certain behaviour on states neighbouring Russia and to discourage allied states from providing assistance to those attacked. This may translate into more specific operational objectives concerning individual states. For example, the author of this study in 2019 identified the following objectives for hybrid operations targeting Poland:

1. Preventing the use of Polish and allied armed forces and infrastructure (roads, railways, ports, airports, staging areas) in support operations for Lithuania, Latvia and Estonia.
2. Forcing Poland to withdraw from any actions contrary to Russia's interests.
3. Potentially - compelling Poland to enable the establishment of a land connection between Russia and the Kaliningrad region or at least to disrupt the Polish land connection with Lithuania.
4. Potentially - forcing Poland to remove US and other NATO forces from its territory[20].

It is worth noting that the migration crisis in 2021 was an element of hybrid actions and was clearly part of the second point mentioned above, as the migration of people to Poland (and other EU states) inspired by the Belarusian-Russian authorities - with the evident knowledge and consent of the Russian authorities - was in retaliation for the support of pro-democratic protests in Belarus. During this crisis, not only was direct pressure exerted on states and societies, including border protection services, but there was also an effort to create a narrative portraying Poland, Lithuania and Latvia as states reluctant to accept refugees and violating human rights. There was also an attempt to polarise public opinion against the background of the crisis and to provoke further internal divisions.

This means that terrorist actions as part of hybrid actions can be carried out with the intention of achieving similar goals and parallels can be drawn between them and the migrant crisis. Four elements are apparent that characterise terrorist actions as part of hybrid actions and make them similar to other tools used, such as migratory pressure.

---

[20] M. Piekarski, *Polish Armed Forces and hybrid war: current and required capabilities*, "The Copernicus Journal of Political Studies" 2019, no. 1, pp. 43–64.

Firstly, a state that becomes a target of terrorist action is forced to deal primarily with an ongoing internal security threat. This may mean that the resources of the State's security system are diverted to counter-terrorism and counter-counter-terrorism activities, especially if the forces and resources allocated to these tasks prove or may prove to be insufficient. It may also be that the costs of the attacks themselves and of maintaining the resources needed to stop them exceed the benefits of the policy pursued by the state under attack, leading to a rapid change of policy.

Secondly, terrorist attacks can create new social divisions and deepen existing ones, especially if carried out by a state that poses as a de facto or deliberately created entity (false flag attacks).

Thirdly, the way in which the state reacts, which may lead to restrictions on civil rights, freedoms and liberties, for example by introducing heightened security measures, may result in further social divisions[21].

Fourthly, it should be borne in mind that actions carried out directly by a state actor or with his support will be characterised by a potentially wider range of combat means, tactics and techniques of action, going beyond the modus operandi observed in recent years of perpetrators of terrorist attacks who did not have such support.

These four elements allow us to specify scenarios for possible crisis situations. It is not legitimate to e every possible case of a terrorist attack, but only those that fall within the outlined boundary conditions.

Possible attack scenarios

This main part of the article presents an es of the scenarios (with their possible variants) concerning the use of terrorism as a tool of hybrid warfare. The scenarios are divided according to the criterion of the potential target of attack. This target, or more precisely its type, is the factor ordering the internal logic of the scenario, i.e. possible benefits and limitations from the perpetrators' point of view. A second factor important to the internal logic of the scenario is the coexistence of other forms of pressure. In constructing the scenarios, the legal

[21] More widely in: A.M. Dyner, *Kryzys graniczny jako przykład działań hybrydowych* (Eng. Border crisis as an example of hybrid action), Polski Instytut Spraw Międzynarodowych, 2 II 2022, https://www.pism.pl/publikacje/kryzys-graniczny-jako-przyklad-dzialan-hybrydowych [accessed: 22 VI 2022].

and organisational status in May 2022 was taken into account. An open question that could not be answered at the time of writing is the impact of the conflict in Ukraine on Russia's military and non-military activity.

Scenario 1. Terrorist attack against military infrastructure and equipment

The word 'war', which is one of the components of the concept of hybrid warfare, evokes associations with armed forces. An attack on military installations may therefore appear to be a likely scenario. Military installations are by definition important for the defence of the state. Their damage or destruction means a reduction in the defence potential of the state, and therefore increases vulnerability to military pressure, in this case from Russia. The same mechanisms may arise in a situation of an attack on troops and subdivisions of the armed forces of allied states which are present in Poland. It should be noted, however, that weakening the military potential in this way is a difficult task. For example, according to available data, in 2021 the Armed Forces of the Republic of Poland had 797 tanks, 1611 infantry fighting vehicles, 751 guns and mortars[22]. It is difficult to expect that any terrorist actions will manage to noticeably weaken their potential. Some infrastructure can be replaced relatively easily. For example, destroyed or damaged fixed radiolocation stations of the Backbone system can be replaced with mobile devices. At the same time, some facilities would not be easy to attack with methods typical of terrorist organisations.

The situation changes when possible targets are narrowed down only to objects that are difficult to replace easily and whose damage will have a clear impact on the capabilities of the Polish Armed Forces. For example, a smaller resource in terms of numbers are combat aircraft. The Air Force is currently equipped with 48 F-16C/D Block 52+ aircraft, 29 MiG-29 aircraft and 18 Su-22M4/UM3K aircraft[23], with the latter two types soon to be withdrawn in favour of 32 F-35A aircraft. Carrying out an attack resulting in the destruction or damage of even just a few combat aircraft will cause damage to military property, which should be estimated at tens of millions of dollars. In addition, it would mean permanently or temporarily taking aircraft out of service that could not be used for training and other activities, such as reconnaissance or protection of our own and allied airspace.

[22] *The Military Balance 2021*, The International Institute for Strategic Studies.

[23] Ibid.

The scenario described had its counterpart in reality. In 1981, the Muñiz air base on the island of Puerto Rico became the target of a terrorist attack. The perpetrators managed to plant explosive charges under 11 A-7D and F-104 aircraft[24]. If a similar attack were to occur in Poland, the destruction or damage to eight F-16 aircraft would result in the elimination of one-sixth of the aircraft of this type. The attack could be carried out by infiltrating an airbase or using unmanned aerial vehicles, especially if the perpetrators were able to identify a convenient opportunity for such action.

Other equipment and systems that exist in small numbers and are difficult to replicate quickly could also be potential targets for attacks in the Polish Armed Forces. The obvious limitation in this case is the necessity for perpetrators to identify adequate targets of attack (devices, military equipment) and to gain access to the attacked object, in order to obtain information, among other things, on its operations and applied security measures.

One should bear in mind not only the strictly material and military consequences of such a scenario. A successful attack will be very easy to use in propaganda and disinformation activities, exposing the fact that a military facility has been attacked and military equipment destroyed. This may lower the level of public confidence in the armed forces and the defence policy of the state.

Scenario 1a. Terrorist attack against military personnel

The scenario involves an attack targeting not military equipment but soldiers. The attack may be carried out on military premises (as in the 2008 Fort Hood attack) or outside military premises and facilities (as in the 2013 attacks in France)[25] and then used for propaganda. From the perpetrators' point of view, an important variant of this scenario is the possibility to launch an attack on people outside military facilities - in residential areas, public places (means of transport, commercial establishments) and other easily accessible places, as this makes it easier to plan and execute. It may also be easier to obtain information on the target (a specific person or persons). In particular, the target may be personnel who require long-term training and are difficult to replace. These include individuals such as:

[24] https://www.globalsecurity.org/wmd/ops/secmuniz.pdf [accessed: 28 V 2022].

[25] More widely in: M. Piekarski, K. Wojtasik, *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku* (Eng. The Polish anti-terrorist system and the reality of attacks in the second decade of the 21st century), Toruń 2020.

- command staff, especially those in the ranks of generals,
- flying personnel and special forces soldiers, naval crew members,
- persons in specialised positions, particularly those involved in operating vital weapon systems and support and security functions and with access to sensitive information,
- persons likely to occupy important positions in the future (persons attending courses, training, military academies).

An attack on such individuals means that, as in the previous scenario, it is possible to inflict serious damage on the armed forces. Depriving the military of a person with specialist knowledge and qualifications can have major psychological effects, as in the previous scenario. It is important to note that the soft consequences (psychological and social) will be more serious than the hard ones. For example, a successful assassination attempt on a squad or tactical compound commander will result in his place being quickly taken by a deputy commander. In the case of other personnel, too, it is unlikely that one person will be the only one with unique competencies and will therefore be replaceable. However, the psychological effects can be far-reaching for both the armed forces and the public, as an attack on a soldier, especially one in a command position, can undermine public confidence in the armed forces and also have a negative impact on soldier morale.

In this scenario, the attack may take the form of assassination or abduction of a person (similar to the abduction of General James Dozier in 1981 in Italy[26]). The latter option should be assessed as more complicated and involving greater risk for the perpetrators. It is possible to disseminate the abducted person's image, force them to make a statement with the content dictated by the perpetrators or even execute them and make their recording public. Importantly, the abducted person may be induced or forced to disclose classified information. In this scenario, the families of those who may be targeted are also at risk. Moreover, the possibility of an attack aimed at soldiers of allied armed forces residing in Poland should be taken into account. Then, the target group of the message generated by such an attack would also be the public opinion of the allied states.

[26] T. Philips, *The Dozier Kidnapping: Confronting the Red Brigades,* https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/phillips.pdf [accessed: 28 V 2022].

Scenario 1b. Terrorist attack against infrastructure and equipment of police, intelligence or counter-intelligence services

This scenario is equivalent to scenario 1, with the difference that the targets of an attack are facilities and equipment used by police services (the Police, Border Guard) or special services. Also in this case, the likely targets are important equipment which is difficult to restore or replace quickly, as well as causing disruptions in its operation, which will impede the day-to-day functioning of those services. It should be pointed out that, in contrast to the majority of military installations, facilities of police services, such as Border Guard posts or police headquarters, are places where activities are performed with the participation of civilians. An attack on the headquarters of a police headquarters may therefore significantly reduce the level of confidence in this service.

Scenario 1c. Terrorist attack against police, intelligence or counter-intelligence personnel

The scenario is equivalent to scenario 1a. The only difference is the identity of the person or persons who are the target of the attack. These may primarily be people holding important positions in the investigative or counter-terrorist service of the Police, police chiefs and people in key positions in the intelligence and counter-intelligence services. Here, too, the psychological and media impact of such an attack may be important, as in scenario 1a.

Scenario 2. Attack on a critical infrastructure facility

The scenario assumes an attack aimed at systems and their facilities, equipment, installations and services which are regarded as critical infrastructure in accordance with the provisions of the *A*ct of 26 April 2007 on crisis management,[27] including energy, raw materials and fuels supply, communications, transport, food and water supply, ensuring the continuity of public administration.

The aim of an attack on such facilities may be both to disrupt or prevent their functioning and to cause fear in society and undermine the confidence of citizens in the authorities. For this reason, the most likely targets of an attack will be those facilities and systems whose disruption will be felt most quickly and can be used for propaganda.

[27] Consolidated text: Journal of Laws of 2022, item 261, as amended.

Several possible variants of this scenario can be identified, which differ in the specific target of an attack.

Scenario 2a. Attack on electricity infrastructure

The scenario assumes an attack targeting the electricity system, i.e. the system responsible for the generation and distribution of electricity. For such an attack to be effective, the perpetrators must disrupt or interrupt one of these processes. In Poland, electricity is generated in various types of power plants - thermal, hydroelectric, wind - and can also be imported from neighbouring countries. Due to the specific nature of energy facilities and their diversity, disrupting or interrupting their operation may be difficult. Potentially, an attack on the transmission network would be easier. It is located over a large area and consists of overhead lines and node points (substations). An attack on such installations, by means of gunfire, mechanical overthrowing of poles or planting explosive devices, could lead to the interruption of power supply to consumers, as well as interrupting lines leading from power stations[28]. In the context of hybrid warfare, it is likely that an attack could be carried out in a coordinated manner and lead to the disruption of the power supply to one or even several large urban areas. Constructing explosive devices to disrupt lines due to blowing up poles should be relatively easy if the support of the intelligence services and special forces of the state (in this case Russia) is used or the activities carried out directly by these services and forces. Attacks on the electricity system may continue even after supply has been restored.

The consequences of such attacks can be catastrophic. Interruption of energy supply to a large urban area will mean disruption of industrial production, service sector activities, hospitals and communication and telecommunication systems. Emergency local power supplies (e.g. generators) can only provide power to some customers and only for a limited period of time. A cascade effect is likely, as further emergencies will occur. For example, a power cut may force the evacuation of hospital patients, and as hospitals will not be able to admit new patients, they too will have to be transported to other cities. It can also be expected that communications and other systems will be paralysed.

[28] More widely in: *IP Note: Most Significant Activity Surrounding Tactics, Techniques, and Procedures Against the Electricity Subsector*, https://info.publicintelligence.net/DHS-ElectricGridAttacks.pdf [accessed: 22 VI 2022].

An attack of this kind, even one that results in only a partial loss of power, will certainly be used in psychological activities aimed at undermining confidence in the state authorities and institutions responsible for national security, and may have far-reaching social and political effects.

Scenario 2b. Attack on fuel infrastructure

The scenario assumes an attack against installations and systems used for production, transport and distribution of liquid fuels. Similarly as in the case of energy infrastructure, these systems consist of fuel production or import sites (refineries, mines, extraction platforms, transshipment terminals) and transport infrastructure. The main difference in this case is the possibility to store fuels (crude oil, petrol, natural gas) and various methods of their transport (pipelines, rail transport, road transport).

Attacks on transhipment infrastructure, fuel storage facilities and transports may be particularly attractive from the perpetrators' point of view. Supply disruptions may not only lead to local fuel shortages, but also have wider consequences. For example, an attack on maritime gas transhipment installations (the Świnoujście terminal or the planned floating installation in the Gulf of Gdańsk) may be an element of activities linked to economic and political pressure, e.g. the creation of a crisis by a foreign state offering to resume supplies by land or other benefits[29].

An attack of this kind can only be a prelude to a disinformation campaign in which false information will be presented, suggesting much greater losses and disruptions to fuel supplies. This in turn is expected to trigger reckless actions by individuals (e.g. buying up fuel at retail), as was seen after the cyber attack on the Colonial Pipeline in the US.

Scenario 2c. Attack on transport infrastructure

In this scenario, the attack targets facilities and systems related to road, rail, sea and air transport. Attacks on these may be an attractive option for a hybrid state due to their importance to the state's defence system and the functioning of the economy. For example, if it were possible to block traffic in a sea port such as Gdańsk, it would cause serious economic consequences related to delays in the transport of goods, which would have to wait for the port to be unblocked or be reloaded elsewhere, which is

[29] More widely in: M. Piekarski, *Bezpieczeństwo dostaw surowców energetycznych do Polski drogą morską*, "Wschodnioznawstwo" 2020, vol. 14, pp. 177–195.

time-consuming. An attempt to blockade transport routes could occur at a time of crisis and an attack would then have wider consequences.

This is evident in the context of the war in Ukraine. In this case, Poland is a transit country through which aid to the attacked country, including military equipment, is moved. At the same time, in the early stages of the conflict, large groups of refugees were transported through Poland, as well as grain, which Ukraine was unable to export via its blocked Black Sea ports. Terrorist actions aimed at paralysing even one major railway junction, such as those in Kraków or Wrocław, could, in such a situation, greatly complicate these ways of assisting Ukraine.

Scenario 3. Attack on a symbolic target

The scenario assumes that an attack will be carried out on a target which is not of economic or military importance, but primarily of symbolic significance. These may be persons, places or objects such as places of worship, monuments, memorials, and events such as demonstrations or mass events.

This type of attack aims to provoke polarisation in society. It is particularly attractive for perpetrators to carry out an attack under a false flag, i.e. in a manner simulating the actions of another actor (an extremist organisation or movement). After an attack, it is possible to carry out another one, also aimed at suggesting the actions of people of a different (opposing) ideological orientation. The aim is to suggest the existence of a deeper conflict than actually exists, to provoke actual tensions and to unleash a spiral of violence. Particularly intensified disinformation activities should be expected in this scenario. It is possible that the technical means used will be limited, due to the need to maintain the appearance of action by individuals or groups not linked to or supported by the state actor. Three variants of this scenario can be identified.

Scenario 3a. Assassination of a well-known person

The scenario assumes that a provocation is carried out using the murder, infliction of bodily harm or abduction of a person widely known for their political, social or media activity. In this case, the recognisability of such a person (including that brought about by controversial statements) is more important than the position they currently hold. This could be someone who has never held state office or sat in parliament. An attack on such a person would be posed as someone from the opposite end of the ideological

spectrum, with the aim of provoking those who identify with the values and views presented by the victim to overreact emotionally, fuelled by disinformation activities. They may suggest a lack of or erroneous actions by state bodies carrying out investigative and operational-reconnaissance activities, or even indicate the involvement in the attack of persons linked to state services.

Scenario 3b. Assassination during a celebration, manifestation or other public event

The scenario assumes that the target of the attack is a celebration, demonstration or other event organised by the state, local government, or a non-governmental or religious organisation. The aim of the attack would primarily be to cause fear, but it is also possible to cause loss of life. In this scenario, too, the perpetrators will aim to make the attack look like an act carried out by an extremist organisation (movement) other than a Russian-backed one which is in opposition to the organiser of the event in question.

Given the likelihood of a large number of dead and injured, such an attack could lead to strong polarisation and extreme reactions, and could be used in the final phase of hybrid action. It is also possible for an attack to be carried out in a way that would undermine the credibility of state bodies. It is therefore to be expected that an attack during a Catholic celebration would be posed as an attack by left-wing extremists, while an attack during a left-wing demonstration would be posed as an attack by a far-right organisation.

Scenario 3c. Assault on a symbolic site

The scenario assumes an attack aimed not at persons, but at property in the form of buildings, such as monuments, museums, temples and other sites of symbolic importance for society or parts of it. In this case, the attack would only aim to generate publicity and interest in the media and public opinion, stimulated by disinformation activities. These factors make it likely to be an attack that would be a prelude to further action.

Scenario 4. An attack demonstrating ineffective performance of services

The last of the ed scenarios is a special case of an attack. Its objective would not be to inflict losses but, first and foremost, to demonstrate the ineffectiveness of the Polish police services and armed forces. The attack would be planned taking into account the identified deficits

in the state security system. Two variants are possible. The event would be so serious that a response to it would be impossible or would be hasty and makeshift. Such a case could be a highly complex hostage situation, for example on board a vessel (e.g. a passenger ferry) or a large public building. The perpetrators may declare a desire to get to Russia or Belarus with the hostages, or they may bring about - which is less likely - a situation in which an attempt to resolve it by force would end in a large number of deaths. In any case, it would not be a matter of achieving a tactical objective, but of demonstrating the inefficiency of the Polish authorities and services, which failed to resolve the situation in a way beneficial to Poland. This would provide a basis for disinformation and political, and possibly military, action. Such a risk exists especially in maritime areas, where it is even possible to bring about a staged operation to "recapture" a supposedly abducted vessel by Russian forces. A successful operation, ending with the capture or killing of the direct perpetrators of the incident by Russian special forces or FSB counterterrorist units, would then be used for propaganda and politically as "proof" of Poland's inability to ensure security in maritime areas and confirmation of the effectiveness of Russia's security apparatus.

Conclusion

The most important conclusion from the scenarios presented is that terrorist threats must be constantly taken into account in efforts to build resilience to hybrid threats. Another is that terrorist threats as an element of hybrid warfare will be derived from the actions of a foreign state, meaning that preferences in the choice of targets and methods of carrying out attacks would be different than in other known strands of terrorism. While in the case of attacks by perpetrators belonging to or supporting Islamic fundamentalist organisations, soft targets (nightclubs, workplaces, means of passenger transport) were the typical choice, in the case of hybrid threats, attacks on critical infrastructure or military facilities are more likely, and only one set of scenarios includes attacks on soft targets and only one of this set - attacks likely to result in a large number of civilian casualties.

Therefore, it is reasonable to take into account the scenarios discussed in the text both in planning anti-terrorist actions, organizing counter-

terrorist actions, and more broadly - in preparing to counteract hybrid threats. It should be remembered that the discussed scenarios indicate the necessity of a hybrid response to such threats. Apart from anti-terrorist and counter-terrorist actions themselves, it will be necessary to carry out other actions, including in the field of counteracting disinformation and information fight.

Bibliography

Bolechów B., *Polityka antyterrorystyczna w* świetle *badań nad terroryzmem* (Eng. Anti-terrorist policy in the light of terrorism research), Wrocław 2012.

Galeotti M., *The Weaponisation of Everything: A Field Guide to The New Way of War*, New York–London 2022.

Makowski A., Kubiak K., *Terroryzm jako sposób prowadzenia wojny?* (Eng. Terrorism as a means of waging war?), "Raport – wojsko – technika – obronność" 1998, no. 4, pp. 41–43.

Menkiszak M., *Strategiczna kontynuacja, taktyczna zmiana. Polityka bezpieczeństwa europejskiego Rosji* (Eng. Strategic continuity, tactical change. Russia's European security Policy), Warszawa 2019.

Nadolski L.M., *Kampania zimowa w 2015 roku na Ukrainie* (Eng. Ukraine's 2015 winter campaign), Bydgoszcz 2017.

Piekarski M., *Bezpieczeństwo dostaw surowców energetycznych do Polski drogą morską* (Eng. Security of energy resources supplies to Poland by sea), "Wschodnioznawstwo" 2020, vol. 14, pp. 177–195.

Piekarski M., *Polish Armed Forces and hybrid war: current and required capabilities*, "The Copernicus Journal of Political Studies" 2019, no. 1, pp. 43–64.

Piekarski M., Wojtasik K., *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku* (Eng. The Polish anti-terrorist system and the reality of attacks in the second decade of the 21st century), Toruń 2020.

Seely R., *Defining Contemporary Russian Warfare*, "The RUSI Journal" 2017, vol. 162, no. 1, pp. 50–59.

Skoneczny Ł., *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia* (Eng. Hybrid warfare - a challenge of the future? Selected issues), "Przegląd Bezpieczeństwa Wewnętrznego", Special issue: *Wojna hybrydowa*, pp. 39–50.

The Military Balance 2021, The International Institute for Strategic Studies.

Internet sources

Cullen P.J., Reichborn-Kjennerud E., *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*, The Multinational Capability Development Campaign, 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf [accessed: 20 V 2022].

Dyner A.M., *Kryzys graniczny jako przykład działań hybrydowych* (Eng. Border crisis as an example of hybrid action), Polski Instytut Spraw Międzynarodowych, 2 II 2022, https://www.pism.pl/publikacje/kryzys-graniczny-jako-przyklad-dzialan-hybrydowych [accessed: 22 VI 2022].

Gasztold A., Gasztold P., *The Polish Counterterrorism System and Hybrid Warfare Threats*, "Terrorism and Political Violence" 2020, https://www.tandfonline.com/doi/abs/10.1080/09546553.2020.1777110?journalCode=ftpv20 [accessed: 28 V 2022].

Hoffman F., Rise of the hybrid wars https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf [accessed: 29 IV 2022].

https://www.globalsecurity.org/wmd/ops/secmuniz.pdf [accessed: 28 V 2022].

IP Note: Most Significant Activity Surrounding Tactics, Techniques, and Procedures Against the Electricity Subsector, https://info.publicintelligence.net/DHS-ElectricGridAttacks.pdf [accessed: 22 VI 2022].

Kosow H., Gaßner R., *Methods of Future and Scenario is: Overview, Assessment, and Selection Criteria*, https://www.die-gdi.de/uploads/media/Studies_39.2008.pdf [accessed: 22 VI 2022].

Ogilvy J., *Scenario Planning and Strategic Forecasting*, Forbes, 8 I 2015, https://www.forbes.com/sites/stratfor/2015/01/08/scenario-planning-and-strategic-forecasting/?sh=2de3fee5411a [accessed: 18 V 2022].

Philips T., *The Dozier Kidnapping: Confronting the Red Brigades*, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/phillips.pdf [accessed: 28 V 2022].

Sovolainen J. i in., *Hybrid CoE Working Paper 5 Handbook On Maritime Hybrid Threats — 10 Scenarios and Legal Scans*, https://www.hybridcoe.fi/wp-content/uploads/2020/07/NEW_Handbook-on-maritime-threats_RGB.pdf [accessed: 29 IV 2022].

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (Eng. National Security Strategy of the Republic of Poland), Warszawa 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf, p. 6 [accessed: 22 VI 2022].

Legal acts

Act of 10 June 2016 on anti-terrorist activities (i.e. Journal of Laws of 2021, item 2234, as amended).

Act of 26 April 2007 on crisis management (i.e. Journal of Laws of 2022, item 261, as amended).

DOI: 10.4467/27204383TER.22.027.16347

ORCID: 0000-0001-9815-6035

KRZYSZTOF IZAK

Anders Behring Breivik. A case study of a far-right terrorist - a lone wolf (Part I)

Abstract

The aim of this article is to present the characteristics of Anders Behring Breivik, including the influence of his childhood and early youth on the development of his personality, and to describe his activities and preparations for the attacks carried out on 22 July 2011 in Oslo and on the island of Utøya, as well as their course. The author has sought to answer the questions of whether it was possible to prevent the attacks and what impact they had on social mood, the nature of changes in the shaping of internal security policy in Norway and the improvement in the efficiency of security services in this country. He also attempted to e what level of threat of a similar attack exists in Poland at present. Conclusions from this es have been enriched by reflections on the consequences of Russia's aggression against Ukraine.

Keywords:

Anders Breivik, active shooter, manifesto, lone wolf, terrorist

In January 2022, reports circulated around the world that Anders Behring Breivik had applied for conditional release from prison after serving 10 years of the 21-year sentence he was sentenced to in 2012 for the murder of 77 people. Breivik greeted those gathered in the courtroom with a Nazi gesture and expressed extreme views during his speech. However, he assured that he had changed and would no longer use violence when he was free. He claimed that it was possible to be a Nazi without being a fighter,

and he dissociated himself from violence, terrorism and the goals described in his manifesto entitled *2083 - A European Declaration of Independence*[1]. He expressed the opinion that he could not be held responsible for his actions because, through no fault of his own, he had been indoctrinated on the Internet. He announced that for the next 50 years he would fight in the Nordic resistance movement or found a non-militant nationalist movement in Europe. He stated that he was working for the Nordic state and was a candidate for parliament for the Nazi party. In the courtroom, he presented a text entitled *Stop the Genocide of Our White Nations*, a view familiar in right-wing extremist circles about the West being dominated by ethnically and culturally alien immigrants. Breivik placed one of the leaflets in the pocket of his suit so that it would be more visible, while the other he stuck to a briefcase which he showed during the court session. He also argued that he could give up his political activity if such a condition was set by the court. Then, he would be ready to move to Svalbard (a Norwegian archipelago in the Arctic Ocean) and take up business or leave the West altogether. The court rejected his request for parole. Prosecutor Hulda Karlsdottir called Breivik's submission of such a request a public relations exercise aimed at improving the conditions of his detention and a reminder of himself. The opinions of the psychiatrist and the prison authorities were also unfavourable to the inmate. Theoretically, he can reapply for parole in a year and repeat this request every 12 months. It is more likely, however, that he will be kept behind bars until his death on the basis of being sentenced to consecutive years of imprisonment, as allowed by Norwegian criminal law[2].

Terrorist attacks in the first decade of the 21st century confirmed international public opinion that radical Islam is the main threat to security and world order. This message was reinforced by the war on terror declared by President George W. Bush after the terrorist attacks in the USA on

[1] See A. Berwick, *2083. A European Declaration of Independence. De laude novae militiae. Peuperes commilitiones Christi Templique Solomonici*, London 2011, https://info.publicintelligence.net/AndersBehringBreivikManifesto.pdf, p. 1437 [accessed: 1 II 2022].

[2] J. Potocka, *Hitlerowskie pozdrowienie i nowe hasła. Breivik chce wyjść na wolność* (Eng. Hitler salute and new slogans. Breivik wants to go free), RMF24, 18 I 2022, https://www.rmf24.pl/raporty/raport-zamachy-w-norwegii/fakty/news-hitlerowskie-pozdrowienie-i-nowe-hasla-breivik-chce-wyjsc-na,nId,5777148#crp_state=1 [accessed: 18 I 2022]; A. Grochot, *Anders Breivik zostanie w więzieniu. Sąd odrzucił jego wniosek* (Eng. Anders Breivik will stay in prison. The court rejected his request), RMF24, 1 II 2022 r., https://www.rmf24.pl/fakty/swiat/news-anders-breivik-zostanie-w-wiezieniu-sad-odrzucil-jego-wniose,nId,5806130#crp_state=1 [accessed: 1 II 2022].

11 September 2001. The bloody attacks carried out by Islamic extremists in Europe, from Russia to Spain, meant that almost every subsequent incident was immediately attributed to al-Qaeda or to organisations and individuals inspired by the ideology and activities of Osama bin Laden's group[3]. It was no different immediately after the reports of the terrorist attack in Oslo and the massacre on the island of Utøya on 22 July 2011. Before the perpetrators were apprehended, one of Poland's terrorism experts said on television that Islamic radicals were behind it. Similar claims were made in Norway and other countries until it emerged that the perpetrator of the attack was Anders Breivik, a then unknown Norwegian extreme nationalist.

The aim of this article is to present the characteristics of Breivik and his activities, and to describe the preparations for the attack and its course. The author has sought to answer the questions whether it was possible to prevent the attack and what impact it had on social moods, the nature of changes in the shaping of internal security policy in Norway and the improvement in the efficiency of the security services in that country. He has also attempted to e whether there is currently a threat of a similar attack in Poland. The occurrence of such an event seems real not only due to the appearance of Breivik's followers, who have made their presence felt in various countries, but also due to radicalisation of social attitudes and sentiments, as well as sharp political discourse in Poland, which has recently been somewhat mitigated by the situation in Ukraine. The conclusions of this es are enriched by reflections on the consequences of Russia's aggression against Ukraine. If the hostilities do not escalate, it can be assumed that they will result in terrorist attacks across our eastern border. Attacks may also take place on Polish territory. Diversionary actions are also to be expected. The war in Ukraine, like any other war, will facilitate access to weapons, ammunition and explosives. Their possession by extremists may have tragic consequences. If hostilities are extended to other states, some of the conclusions formulated at the end of the article will be outdated due to new threats and challenges, the scale of which is currently difficult to predict. The state of war will change the optics of terrorist threat perception.

In this article, the author has used the following research methods: historical - allowing to trace Breivik's biography, behavioural - when ing

[3] The exception was the attack on the Madrid suburban railway trains on 11 March 2004. Immediately after informing the head of government about these events, Prime Minister José Luis Rodríguez Zapatero announced on television that ETA terrorists were behind the attack.

his behaviour, comparative, by means of which he has confronted Breivik's activity with other terrorists motivated by anti-immigrant, racist ideology.

Biography of the assassin

In her book on the Breivik case, Elżbieta Czykwin wrote:

> The key to understanding Anders Breivik's life trajectory seems to be an is of his family ties. They were severely violated from birth. His mother, who was undoubtedly the most important person in his life, brought with her a psychological baggage that put a fundamental strain on their relationship. Wenche was unable to cope with herself, a symptom of which was both the unwanted and rather accidental first child and the unwanted second child. The divorce clearly revealed the instability of her psyche, her bipolar disorder and her difficulties in arranging her relationship with her husband. The pathological baggage of childhood was shared not only by her but also by Anders[4].

As an adult, Breivik displayed traits of emotional deprivation, narcissism and misogyny. This, combined with feelings of alienation, hatred, extreme right-wing ideology and the influence of computer games, led him to commit murder on an unprecedented scale. Unni Turrettini pointed out the similarities between Breivik's traumatic childhood, Timothy McVeigh's[5] and Theodore Kaczynski's[6], which influenced their adult lives filled with hatred and aggression[7].

---

[4] E. Czykwin, *Anders Breivik. Między dumą a wstydem* (Eng. Anders Breivik. Between pride and shame), Warszawa 2019, p. 87. In this section of the article, most of the information on Breivik is taken from this book.

[5] On 19 April 1995, Timothy McVeigh detonated a car filled with 2.5 tonnes of explosives at the Federal Building in Oklahoma City. The explosion caused a partial collapse of the building and the death of 169 people (over 500 were injured). The investigation revealed that the perpetrator was affiliated with the radical-right Michigan State Militia movement, of which there are many in the US to date. McVeigh was sentenced to death.

[6] Theodore D. Kaczynski, known as the "Unabomber", sent explosive devices through the mail between 1978 and 1995. As a result of their explosions, 3 people died and 29 in it and handed him over to the authorities. The court sentenced him to life imprisonment without the possibility of parole. He is serving his sentence in a Colorado prison.

[7] U. Turrettini, *The Mystery of the Lone Wolf Killer: Anders Behring Breivik and the Threat of Terror in Plain Sight*, New York 2015, pp. 16–31.

Anders Behring Breivik was born on 13 February 1979 in Oslo. His mother, Wenche Behring (died 2013), came from a poor family. Even as a few years old, she took care of her mother, paralysed by childbirth, who blamed her for her disability and hated her. Wenche's father died early and the family was excluded from the local community. Breivik's sister in a way replicated her mother's fate and took over the family's caretaking functions when she was a few years old. Wenche completed a nursing course and worked in a hospital as an orderly. The turning point in her life came when she met Jens Breivik, a diplomat, 12 years older than her, a divorcee and father of three. Six months after Anders was born, the family moved to London, where Jens was seconded to work at the Norwegian embassy. After another six months Wenche demanded a divorce and returned with Anders and his half-sister Elisabeth to Oslo, where she occupied her ex-husband's flat. The mother could not cope with the children, especially Anders, which was brought to the attention of Bernevernet, a Norwegian state institution that works to ensure proper social and educational conditions for children and young people from difficult backgrounds. Bernevernet did not, however, place Anders in a foster family. His mother was an uneducated orderly, his father a member of the elite. Breivik aspired to his father's status, but felt that in Norwegian society he had a lowly position inherited from his mother. In doing so, he had the opportunity to see his father's world. He attended school in Oslo's most elegant district, and had previously gone to kindergarten with the grandson of the Norwegian king. He had a sense of belonging to the elite, but on the other hand he was aware of the material gap between him and his classmates. He was also an average student. He was not liked by his neighbours for his arrogance, rudeness, lack of education and bullying of those weaker than himself. He took great pleasure in watching the suffering of other children and animals, to whom he himself was cruel. During this period, his relationship with his father was good. Jens remarried and settled in France. Anders used to visit him and even took a liking to his father's new wife. At the age of 13, he entered secondary school. He began to build his identity by participating in a subculture of graffiti artists. He adopted the nickname "Morg" and tried to dominate a group of similar young people. He felt particularly comfortable in the company of graffiti artists coming from a background of Arab immigrants. At that time, graffiti was not socially perceived as an innocent, artistic expression of youthful creativity, but as an illegal, hooligan activity, a kind of vandalism prosecuted by the police. Breivik was also arrested by

them. Jens' reaction to his son's involvement in the graffiti community was to cut off contact with him, in accordance with the agreement they had made between themselves. Over time, however, "Morg" was excluded from the community for trying to impose his dominance on it. He lost his position and was humiliated. The sentence handed down by the graffiti community sealed the marginalisation of Anders by his colleagues at school.

At the age of 16, Breivik entered the prestigious Oslo Commerce School. He stopped using street language and presented himself as an open and friendly boy. He began to consider himself metrosexual[8]. He spent a lot of time in front of the mirror and wore make-up. He even underwent plastic surgery on his nose. However, in a personality sense he was not metrosexual, in his case it was more of a pose. Since his adolescence, Breivik devoted a lot of time to weight training and also started taking anabolic steroids. This made him look big and strong. While attending the Commerce School, he worked as a telemarketer and was a good salesman. He started to play the stock market and on just one transaction he earned 200 thousand crowns (approx. 90 thousand zlotys). As a result, in 1998 he dropped out of school and made a plan to become a millionaire. He also saw himself as a member of a Masonic lodge. He saw this as an opportunity to make a name for himself and become part of the elite. However, he did not know anyone who could introduce him to Freemasonry. He wanted to be someone with an appointment, with a title, and not someone whose work and devotion to others earned him respect and social approval. He did not have a high school diploma, but he boasted that he had read enough to be titled "bachelor of small business and management", as well as that he had familiarised himself with all the readings required for economic studies. Until 2001 he worked for the telemarketing company Direkte Respons Senteret, where he was promoted to head of customer service. While still at trade school, he began to see his place in the right-wing Progress Party (Frem-skrittspartiet, Norway). He met Lene Langemyr, a youth activist in the party. Lene was adopted by a Norwegian family as a one-and-a-half-month-old Hindu infant, abandoned in India. However, she believed that Norway should

[8] The term 'metrosexual' was first used in 1994 by Mark Simpson, a columnist for The Independent. This neologism, derived from the words "metropolis" and "heterosexuality", refers to the stereotype of a man in love with himself, an inhabitant of a big city, focused on his own appearance, associated rather with feminine care for beauty and manifesting stereotypically feminine personality traits, such as: emotionality, sensitivity, tenderness, warmth, empathy.

tighten its immigration policy and strengthen the army. Anti-immigrant slogans were already a source of growing popularity for the Progress Party, which was in opposition to the Labour Party (Arbeiderpartiet[9]) in the 1980s. Lene and Anders began to think about a political career. Not only did they share political ambitions for the Progressive Party, anti-immigrant rhetoric and the stigma of childhood rejection, but also a love of guns. Anders was an expert in this field. This was astonishing, especially as he had been overlooked for conscription due to his criminal record (graffiti painting). He himself claimed that he had obtained an exemption from military service due to caring for his sick mother. Breivik's political goal was to be on the election list for Oslo councillors. However, he was not a good speaker. His advantage was his constant presence in cyberspace, but this made it difficult for him to participate personally in party life. This resulted in him not being on the party list, not even being called for a conclusive interview. He felt humiliated, especially since it included Lena and his party supervisor, who were both elected as city councillors.

In 2001 Breivik founded an E-Commerce Group, a company operating on the edge of the law, which sold diplomas-gadgets (in Poland similar products offered on the Internet, including replicas of ID cards or driving licenses, are called collector's documents), e.g. of graduation from any university, at an affordable price of about 100 dollars. His company stipulated on its website that the diplomas were offered as props and ornaments. The signatures on them were fictitious, electronically generated, so no one could sue for infringement of personal rights. On the other hand, these documents could be used by immigrants to legalise their stay and, if sent outside Europe, provide the basis for obtaining a visa from the country in which the university issuing the original diplomas was located. In his company, Anders employed his mother (for cleaning and laundry) and a graphic designer from Indonesia to create the document templates. At first he had doubts about the legality of such activities, but for 30,000 kroner a month he took the job and proved to be a very skilful designer. Breivik offered him a higher salary in exchange for working on the black market, but the graphic designer did not accept the offer. However, this company did not last long either, nor did others, including one that rented advertising space on billboards. In February 2004. Anders went with his mother to Malta as part of a ten-day trip. Perhaps it was then

[9] Until 2011, it operated as the Norwegian Labour Party (Det norske Arbeiderparti).

that his fascination with the Crusaders awoke. At that time, he also started looking for a girl on the Internet sites of Eastern European countries. He believed that such a woman would be submissive and compliant to him, unlike the liberated Norwegians. He ordered the contact details of two women on a Belarusian dating site for 100 euros and selected two of them, after which his mother decided on the final choice. He chose Natasha from Minsk, who lived in a block of flats in a working-class neighbourhood and spoke little English. In 2005 Anders visited her in Minsk in 2005 and she, on his invitation and with the ticket he bought, came to Oslo later. However, they parted without much emotion. He considered her a dowry hunter, she considered him a male chauvinist. According to some, Breivik had homosexual tendencies and that is why he did not get on well with women, but the reason could also be his inability to relate and bond with people. On one occasion, Wenche and his son were invited to visit his mother's cousin, who turned out to be a member of a Masonic lodge. Breivik, who, as already mentioned, dreamed of joining this community, asked his uncle about the possibility. The latter stressed the importance of the brotherhood of Freemasons, Christian values, nobility, humility and tolerance. Anders, however, did not want a sense of community. He wanted to stand above others. Thanks to the patronage of his uncle, Breivik was to be - despite the difficulties - admitted to the lodge. This did not happen, because a new fascination meant that he had no time for anything, not even to attend the solemn ceremony of admission to Freemasonry. This fascination was computer games. This did not prevent him from later taking photos of himself in an elegant outfit decorated with the symbols of Freemasonry. This was not the only outfit that was supposed to make him look more valuable and reveal his vanity. He also photographed himself in a military gala uniform of an officer, with badges and insignia pinned to it, a special forces diver's suit of the navy or an anti-chemical suit[10].

When Anders turned 27, he moved back in with his mother. As "Andersnor-dic" he played a computer game 17 hours a day for two years, which allowed him to become the leader of the guild "Virtue". He also received the title "Justicar". Leading the guild put him in charge of keeping up the motivation of the participants, who often, like Breivik, fell into addiction. He became addicted under the influence of "World

[10] *Profile: Anders Behring Breivik*, BBC, 12 IV 2012, https://www.bbc.com/news/world-europe-14259989 [accessed: 14 V 2012].

of Warcraft". For success-seeking individuals of Breivik's ilk, the game can be very appealing, as it offers a clear structure for promotion and the path to achieve it. While holed up in his family home, he became more and more immersed in the world of mages and sword fighting. His need for elitism, success and connection was satisfied in the virtual world. The few years he spent playing games also allowed him to get to know another virtual world, including that of Muslim extremists. He delved into online knowledge of Islam, the Quran and the Crusades. He also became interested in anti-Muslim and anti-immigration websites, particularly Stormfront, whose slogan "White Pride, World Wide" appealed to him. He wanted to fight for the purity of white man's Europe, or, as he claimed, to defend Europe from Eurabia (Arab influence on the continent). He thought more and more about the Islamisation of Europe. He tormented his few surroundings with his beliefs about the dangers of Arab immigrants. His mother hoped that this was a temporary phase which would pass when her son finally found a job and a wife. Friends shunned his lectures and invited him less and less to social gatherings. Over time, Breivik began to create an alternative reality. He dreamt of creating a pan-European resistance movement against Islam, which he himself would lead. He decided to write a book in order to convey what he thought were innovative and revolutionary ideas to the world. He had neither writing talent nor leadership charisma, so in his "work" he used mainly biased fragments of the Quran and other texts, often simply copied. One can find there, among others, references to the manifesto of the aforementioned Theodore Kaczynski. He selected facts to fit his thesis. He saw conspiracy theories everywhere. He compared the problem with Islam to a broken tap. When water floods the bathroom, the first thing to be dealt with is fixing the fault, not wiping it out. The water for him was the Muslims, the faulty tap the Norwegian government and left-wing parties. This may explain why Breivik attacked not immigrants, but a government district of Oslo and a Labour Party youth rally[11].

The desire for authority and connection was too strong in Breivik to remain unexpressed. So Anders found someone with whom he shared his views and identified completely. This was the blogger Peder Are

[11] A. Sobańda, *Skąd wziął się Breivik i czy można go było powstrzymać? Przejmująca opowieść o Norwegii* (Eng. Where did Breivik come from and could he have been stopped? A moving story about Norway), Dziennik, 21 VIII 2015, https://kultura.dziennik.pl/ksiazki/artykuly/498350,jeden-z-nas-przejmujaca-opowiesc-o-norwegii-autorstwa-asne-seierstad.html [accessed: 24 VIII 2015].

Nøstvold Jensen, known online as 'Fjordman'. He preached hate towards immigrants, which he combined with apocalyptic prophecies. Such a narrative brought in an element of transcendence and was somewhat reminiscent of the virtual game world that Anders had mentally been in over the past few years. He addressed 'Fjordman' with the words: *Keep up the good work mate. You are a true hero of Europe*. In an e-mail to him, in which Anders wanted to recommend his book, he wrote: *Much of the knowledge I possess remains inaccessible to most people, even to you*[12]. In another letter he assessed: *Defeating Eurabia is brilliant*[13]. Fjordman ignored him, however, and so this time too Breivik remained alone. So he concentrated on writing the manifesto, which caused him to move further and further away from the "World of Warcraft" gaming community. As with the games, however, he mentally followed the direction of increasing authoritarianism and cruelty. He advocated the deportation of all Muslims from Europe. In order to reach as many people as possible with his ideas, he wanted to found a conservative newspaper. He also proposed and developed unrealistic projects and boasted of his influence in the Progressive Party and the Masonic lodge. When in 2009. Progress Party again lost the election to the Storting (the Norwegian parliament), Breivik turned to it for help in establishing a new newspaper. The refusal made him feel humiliated and alienated again.

Preparations for the attack

In his manifesto, Breivik stated that he began a nine-year plan to prepare for terrorist attacks in 2002, when he was 23 years old. In order to finance them, he set up his own software company. He was to earn his first million kroner when he was 24. He lost two million on stock market speculation, but still had two million kroner to finance the attack[14]. The information in which Anders presents himself as a financially successful man

[12] Å. Seierstad, *Jeden z nas. Opowieść o Norwegii* (Eng. One of us. A story about Norway), Warszawa 2013, p. 71. The book Breivik referred to in his letter to "Fjordman" is his famous manifesto, which he worked on.

[13] Ibid.

[14] *Norway gunman claims he had nine-year plan to finance attacks*, The Guardian, 25 VII 2011, https://www.theguardian.com/world/2011/jul/25/norway-gunman-attack-funding-claim [accessed: 27 I 2022].

contradicts his biography. During the period he writes about, he owned the aforementioned E-Commerce Group company. Despite the demand for the documents it produced, it is difficult to see how Breivik could have made millions by trading in them. In the following years he could not deal with the planning of the attack either, as he was completely absorbed by computer games. The disregard from "Fjordman" may have triggered a desire in Anders to show him and others that he could do much more than just write a book. The thought of shedding blood in the name of the only right idea may have already been in Breivik's mind while he was writing it. The subsequent parts of the manifesto show the intensification of radicalisation. At first it is quite moderate, containing content and ideas circulating on the Internet at the time. Then, the opinions expressed become more and more radical, and by the end Breivik's words are an overt call to fight and shed blood. The cultural revolution, restoring the purity of race in Norway, was to be led by the organisation Knights Templar, which Breivik established in the pages of his "work", and made himself the highest-ranking Commander of the anti-communist Resistance Movement against the Islamisation of Europe and Norway. Breivik despised left-wing views, was against feminists, gender equality and tolerance for sexual minorities. However, he saw the main threat in immigrants, who, in his opinion, were destroying the culture and society of Europe. An expression of Breivik's progressive radicalisation was the preparations for the attack. These began in 2009. On 18 May, Anders registered a one-man company, Geofarm, allegedly to carry out agricultural activities, including growing vegetables. The following year, he began stockpiling chemicals in the basement of the house where his mother lived[15].

Part of his plan was based on the use of firearms. In early 2009. Breivik was stopped during a routine check near the town of Wetzlar, near Frankfurt am Main. The Norwegian was carrying ammunition and gun parts. The ammunition was seized, but he was allowed to keep the parts because it was not considered possible to build a functioning weapon from them. The incident was not reported to the Norwegian police[16]. At the end

[15] A. Sobańda, *Skąd wziął się Breivik…*

[16] *Anders Breivik był zatrzymany przez niemiecką policję dwa lata przed zamachem na wyspie Utöya. Miał przy sobie amunicję i części uzbrojenia. Został wypuszczony na wolność* (Eng. Anders Breivik was detained by German police two years before the Utöya island attack. He had ammunition and weapon parts on him. He was released), Wirtualna Polska, 14 I 2016, https://wiadomosci.wp.pl/anders-breivik-byl-zatrzymany-przez-niemiecka-

of August 2010 Breivik travelled to Prague, where he spent six days. While surfing the Internet, he realised that it was fairly easy to obtain weapons illegally in the Czech Republic. He intended to buy an AK-47 carbine, a Glock pistol, hand grenades and an RPG-7, the latter two of which he hoped to receive as a bonus. He provided himself with an alibi in the form of a prospectus on the mining and sale of minerals in the Czech Republic, so that if necessary he could explain the purpose of his stay. To his surprise, he did not buy any firearms in Prague. He decided to forego obtaining them abroad and try to acquire them legally in Norway. Obtaining a firearms licence, even though he had bought two pistols seven years earlier, proved more difficult than he had anticipated. For it was necessary to prove regular attendance at one of the shooting clubs. Breivik therefore enrolled in a shooting club in Oslo, where he received 15 hours of training in rifle shooting. He also practised his marksmanship skills in the computer game "Call of Duty: Modern Warfare", set in the reality of modern conflicts. As he wrote in his manifesto, this game helped him to improve his concentration and reaction speed. At the shooting club, he was given permission to buy short and long guns. He bought a Glock 17 pistol, a Sturm Ruger Mini-14 calibre 5.56mm semi-automatic carbine, 300 rounds of rifle cartridges and 150 rounds of pistol ammunition, a laser sight, an extra trigger to facilitate rapid shooting and a rifle bayonet. He named the pistol Mjølnir after the hammer of the Norse god Thor, and the rifle Gugnir after Odin's spear that always hit the target. He engraved the corresponding runes on the weapons. He also gave names to other objects, which he altered as he saw fit, and treated them as amulets[17].

Acquiring chemicals was a sensitive phase of Breivik's activities. This was the sphere where it was easiest to arouse suspicion and to be deconstructed. He bought chemicals to produce explosives via the Internet or in person. In December 2010, he bought 0.3 kg of sodium nitrite (a chemical used in Norway for preserving meat) from Keten, an internet sales company in Wrocław. He paid 10 euro by card. In the same month, he ordered 150 kg of aluminium powder from the same Polish shop, for which he paid 2 000 euro by bank transfer. Powdered aluminium increases

policje-dwa-lata-przed-zamachem-na-wyspie-utoya-mial-przy-sobie-amunicje-i-czesci-uzbrojenia-zostal-wypuszczony-na-wolnosc-6027685648360577a [accessed: 15 I 2016].

[17] E. Czykwin, *Anders Breivik*…, p. 98; M. Piekarski, K. Wojtasik, *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku* (Eng. The Polish anti-terrorist system and the reality of attacks in the second decade of the 21st century), Toruń 2020, p.18.

the explosive power of the charge. Breivik wrote in his manifesto that up to 100 kg of this substance can be purchased in Poland without raising suspicion. Buying chemicals in our country was not a problem at the time[18]. He stated in his order that he needed the powder as an ingredient in paint to protect his boat. In fact, the two substances bought in Poland were necessary for him to construct the detonator. After making these purchases, Breivik was blacklisted by the British special services[19]. At the time, his personal contacts with Łukasz Mikuś, the owner of Keten, who had been in Sweden several times, were not ruled out[20]. Breivik had contacts with yet another online shop, located in Pobiedziska near Poznań, where he bought the fuse. The shop was popular and recommended on forums, also among Norwegians, because its owner, Tomasz P., did not ask customers uncomfortable questions. Under the pseudonym "Czort" he also published instructional videos and advertising materials about his shop's offer on Internet forums. All of them concerned the construction of explosive devices. A few months before the attack in Oslo, Tomasz P.'s transactions

[18] After the attacks in Norway, the situation in Poland changed dramatically. Internet shops offering dual-use chemicals were obliged to register their customers' personal data, the type and quantity of substances ordered, and to inform the Internal Security Agency or the police when an order was placed.

[19] Keten was a legally operating company selling chemicals. At the time, the Polish Explosives Act and the Ordinance of the Minister for the Economy did not require a licence for the purchase and storage of most pyrotechnic articles. A licence was required for the sale of finished explosives. The company in Wrocław where Breivik bought the components for the bomb also did not need a licence.

[20] Łukasz Mikuś was passionate about chemistry. After graduating from university, he opened an online shop with chemicals. In 2001, he was legally convicted of offences involving explosives. In one case it was about the purchase and possession of two kilograms of TNT and ammunition for small arms. In the second case, he constructed and sent an explosive device to Ryszard H. The package exploded during sorting at the Main Post Office in Wrocław. The police then ordered the evacuation and search of the building, Mikuś's flat, the recipient of the package and a dozen or so other people who were in contact with Mikuś. Ryszard H. was a member of the Silesian "Danon" gang at the time. The group was broken up in 2002. According to the Central Investigation Bureau of the Police, the bandits planted an explosive charge near an escort agency in Rydułtowy. In the explosion 5 people were injured, 3 of them seriously. The owner of the premises lost his arm, one of the municipal guards called to the scene of the attack was also seriously injured. Ryszard H. was sentenced for participation in a criminal group to 5 years in prison. See M. Rybak *Wrocławianin, który sprzedał chemikalia Breivikowi, miał kiedyś problemy z prawem* (Eng. Wrocław man who sold chemicals to Breivik once had legal problems), "Gazeta Wrocławska", 22 XI 2011; B. Kittel, J. Jabrzyk, *Czy Polak pomógł Breivikowi* (Eng. Did a Pole help Breivik), TVN24, 22 XI 2011, https://tvn24.pl/polska/czy-polak-pomogl-breivikowi-ra191578-3531692 [accessed: 23 XI 2011].

aroused suspicion in the "Global Shield" programme, which brings together customs offices from NATO countries which supervise the trade in goods useful in the manufacture of explosive devices. The Norwegian customs office sent a list of 41 suspected transactions to the Norwegian counterintelligence service. Breivik's name was on it, but his person did not arouse the suspicions of the special services. According to "Global Shield", Breivik bought a fuse that was not on the restricted goods list. The purchase was small and Breivik was not a prime suspect on the list[21].

In his manifesto, the future bomber mentioned that while shopping, not only in Poland, he pretended to be the owner of a company conducting research related to agriculture or suggested that he was a pyrotechnician and wanted to put on a low-budget fireworks display at his sister's wedding. Poland is mentioned dozens of times. Breivik pointed out that in this country you can buy an AK-47 and legally try out the carbine at a shooting range. His idol is King Jan III Sobieski, who stopped the Turks at Vienna. The Norwegian also mentioned Polish nationalist groups. He included Self-Defence of Poland, League of Polish Families, National Rebirth of Poland, League for the Defence of Sovereignty and Law and Justice. In his manifesto, he quoted Czesław Miłosz's *The Captive Mind*[22]. He placed online orders for most of the chemicals in December 2010, when postal workers were too busy to notice anything suspicious about them. He collected them in the basement of the house where his mother lived. Thanks to a company he set up in 2009 called Geofarm, he was able to buy fertiliser, which was used as the main ingredient in the explosive, without raising suspicion. In the spring of 2011, he rented an abandoned farmhouse, Vålstua, in Åmot municipality, Hedmark County. He drew up a list of the most important equipment, tools and chemical components, together with the approximate cost of purchasing them. This was necessary due to the limited preparation time and capital available. He drew inspiration from an assassination attempt by the aforementioned Timothy McVeigh in the USA. He bought ammonium nitrate fertiliser for the purpose of allegedly growing vegetables. As it later turned out, there was enough of it left on the farm to make one more explosive. Perhaps Breivik overestimated his strength, ran

[21] M. Kącki, *Breivik kupił lont w Polsce* (Eng. Breivik bought the fuse in Poland), "Gazeta Wyborcza", 23 VIII 2011.

[22] J. Haszczyński et al., *Robił zakupy we Wrocławiu, podziwiał Jana III Sobieskiego* (Eng. He shopped in Wrocław, admired Jan III Sobieski), "Rzeczpospolita", 26 VII 2011.

out of time, money or everything at once[23]. He ordered powdered sulphur on eBay as a material for plastic artists, and bought Chilean saltpeter from a pharmacy in a nearby town. He had a detailed story prepared for each purchase. He said, for example, that he needed an aquarium cleaner or meat preservative. The fuse was allegedly to be used during the New Year's Eve party. He precisely calculated and experimentally investigated how long it would take for it to burn in time to escape. To obtain acetylsalicylic acid he needed several kilograms of aspirin. In order not to arouse suspicion, he only bought two packs each from different pharmacies in Oslo. He travelled to the capital several times at two-week intervals. He appeared at the pharmacies dressed smartly. To disguise himself, he initially chose the more expensive equivalent of aspirin, and only later the cheaper ones. Buying sulphuric acid (30 l) also required cleverness. He bought it in small quantities from various sellers connected mainly with the automotive industry. Instead of three tonnes of ammonium nitrate, he took six - he ordered the unnecessary half to disguise himself. From China he imported 60 watertight bags used for transporting and storing chemicals and liquid nicotine. He bought three steel containers from Ikea, which he planned to convert into detonators. He also brought chemicals to the farm that he had previously collected in Oslo[24].

He was systematically manufacturing an explosive in a farm building. It was not an ordinary ANFO charge made from the aforementioned ammonium nitrate. ANFO is made by soaking ammonium nitrate in one of the liquid fuels, but the explosive prepared in this way is difficult to detonate. Typically, detonators are used to create the explosion, and aluminium dust is added to increase its force. Breivik began to construct a high-powered explosive himself, based on information gleaned from the internet. First of all, he proceeded to laboriously centrifuge fertilizer granules in a blender to obtain pure ammonium nitrate free of the antihygroscopic lagging, which he then poured over diesel fuel. He worked systematically, soaking it evenly into each 50kg quantity of pellet-free fertiliser. He then packed the substance into double-layered bags imported from China. He sealed each bag and set it aside. The work progressed slowly and he was under time pressure. When he realised that he would not be able to fully implement the plan, he centrifuged only part

[23] E. Czykwin, *Anders Breivik…*, pp. 90–91.

[24] Ibid., pp. 93–94.

of the fertiliser from the pellets and packed the remaining fertiliser into bags as well. This had the effect of reducing the explosive force. The work was dangerous. After a long period of purifying ammonium nitrate, which involved a lot of chemical dust floating in the air, he wrote: *I will surely die of cancer within twelve months. So much of this shit must have got into my lungs, although I used a mask*[25]. The barn where he worked was filled with harmful volatile substances, corrosive liquids and aluminium dust. In addition, he boiled 30 litres of sulphuric acid on a primitive cooker to increase its concentration by evaporating water. The wafting stench made him decide to heat the acid at night. He used almost no special protective equipment. He worked in a mask with an acid filter, a thick protective apron and rubber gloves. The risk of explosion was very high. Breivik was aware of this because he read the warnings on the packaging. He feared that a possible explosion would not kill him immediately, but that he would be badly burned or lose his hands. In that case he planned to commit suicide by shooting himself in the head with a rifle using his feet. Another stage of the work involved preparing a suitable detonator. He was to use diazodinitrophenol, also known as dinitrobenzenediazoxide, as the initiating explosive. Anders had all the chemicals needed to make it, except for picric acid, which he had to produce himself[26]. The first sample he produced failed to ignite. This failure was compounded by a computer malfunction, and Anders needed it on an ongoing basis during the subsequent phases of explosive production. Obtaining acetylsalicylic acid from crushed aspirin tablets also proved too laborious. At first, he tried crushing them with a pestle, but this method was inefficient. So he covered the tablets with foil and smashed them with a heavy dumbbell. Eventually, he managed to obtain the desired chemical compound. He also came up with the idea of using a small concrete mixer to mix Chilean saltpeter with aluminium dust, despite fears that a spark would cause a detonation. However, this proved to be safe and greatly reduced production time. One of the final stages of work on the bomb was to test the fuse. The experiment was a success[27]. Anders modified some of the ammunition he bought - he filled the cartridges with poison in the form of liquid nicotine imported

[25] Å. Seierstad, *Jeden z nas...*, p. 247.

[26] See *Diazodinitrofenol*, Vortal Młodego Chemika, 4 XII 2011, https://www.vmc.org.pl/pirotechnika/materiay-wybuchowe/inicjujce/item/297-diazodinitrofenol [accessed: 31 I 2022].

[27] E. Czykwin, *Anders Breivik...*, pp. 98–101.

earlier from China. In the next batch of cartridges, he cut off the tips and replaced them with lead ones. This was to increase the fatality rate from gunshots. He bought a tight-fitting sweatshirt from a sports shop, which he used to imitate a police uniform. A month before the planned attack, he began to experience financial shortages. He had already taken out loans amounting to 28 750 euros with nine credit cards, which had to be repaid[28]. Failure to do so meant he risked being put on the debtors' list, which in turn made it impossible to rent a car. Thanks to some financial acrobatics, he managed to postpone the critical moment until mid-July. As in the past, he acted on the edge of the law or broke it. The fact that he only ran out of money at the end of the preparatory work meant that he had considerable sums at his disposal even though he was not working.

During the preparations for the assassination, Breivik kept fit by weight training and taking anabolic steroids. He gained courage through online games, especially the "Cataclysm" add-on for the game "World of Warcraft". Morale and motivation were kept up by contemplation, which he used three times a week during walks. When times were tough, he would reach for food as a reward. He also used a protein supplement to increase his muscle mass and a thistle preparation to protect his liver from the effects of steroids. In addition, he stockpiled various tablets to get a boost of energy just before the actual action. When in danger, he would also reach for Red Bull and other drugs[29]. Breivik could have been uncovered several times. One such incident was the arrival of the farm owner's daughter at the end of June 2011. She showed up in the evening and stayed overnight. Anders was determined to kill her if she found anything suspicious. However, this did not happen, so he let her go. Other uninvited guests also disturbed him in his preparations. One of them offered to remove the stones and to fertilise the field. Breivik firmly refused. He suspected that his neighbour had figured out what he was using the fertiliser for and reported him to the police. When a strange car appeared in his yard, he was almost sure he had been exposed. In the meantime they were random visitors, four Poles[30]. Local farmers noticed Breivik's unusual behaviour (for example, he hung a padlock on the door, which was not a local custom), but they were too busy with their summer jobs to pay attention to their isolated neighbour.

---

[28] A. Berwick, *2083. A European Declaration of Independence...*, p. 1437.

[29] E. Czykwin, *Anders Breivik...*, pp. 94–95.

[30] Ibid., pp. 103–104.

Breivik began the final phase of preparations for the assassination on 2 May and it lasted 81 days. He described each day's work in detail in a diary that forms part of his manifesto[31]. He concluded the diary with the conclusion that the knowledge he had gained while working on preparing all the components of the bomb would allow another person acting on his instructions to reduce this time from 81 to 29 days. He also gave an estimate of the reduction in time if more people had been involved in such work. With two people it would be 20 days, with three people 16 days, with four people 13 days and with five people 12 days. He also indicated the scale of the risk of deconspiration depending on the number of people involved in the preparation of the explosive - from 30 per cent for one person to 90-95 per cent if five people were involved[32]. Potential imitators received detailed information about the various phases of the bomb's construction[33]. The bomber set 22 July 2011 as his personal D-Day. The date was important for several reasons: it was a Friday in July after working hours, a time when many officers were on leave or starting a weekend break. Gro Harlem Brundtland of the Labour Party, three times prime minister of Norway, was then scheduled to address participants in the party's youth group, during its camp on the island of Utøya near Oslo. Breivik also wanted to kill Norway's Prime Minister Jens Stoltenberg, who was in office and present at work that day[34]. On 19-20 July Anders loaded an explosive weighing 950 kg (sources also claim that it was 1050 kg) into a Volkswagen Crafter van rented a few days earlier, which had been converted into a VBIED (Vehicle-Borne Improvised Explosive Device) bomb. The front of the vehicle bore the words "Sewer Cleaning". He also had at his disposal a Fiat Doblo, also on hire[35]. On 21 July he drove both vehicles to Oslo and refuelled them. He then parked the Volkswagen at a garden centre. He changed to the Fiat, which contained weapons and ammunition. He parked the car at Hammersborg Square, opposite the government district. He quickly walked around it to see if there were any new blockades. He had already monitored this area several times during his stay in Oslo. He took a taxi to his mother's house. The next

[31] A. Berwick, *2083. A European Declaration of Independence...*, pp. 1454–1470.

[32] Ibid., pp. 1470–1471.

[33] Ibid., pp. 1438–1453.

[34] E. Czykwin, *Anders Breivik...*, p. 92.

[35] S. Death, *Anders Breivik massacre: Norway's worst nightmare*, The Guardian, 25 III 2015, https://www.theguardian.com/world/2015/feb/22/anders-breivik-massacre-one-of-us-anne-seierstad [accessed: 28 IV 2015].

day, before leaving home, he switched on his computer to send a file to 1000 e-mail addresses containing the aforementioned manifesto entitled 2083: A European Declaration of Independence, with a Templar cross and the Latin subtitle De laude novae militiae Peuperes commilitiones Christi Templique Solomonici (Praises of the new warrior. Poor Knights of Christ and the Temple of Solomon), signed with his pseudonym, with the place and date of publication: (see the figure). At the end Breivik has included seven photographs of himself[36]. The study runs to 1515 pages and is the second largest ideological text, after Mustafa Setmarian Nasar alias Abu Musab al-Suri's work entitled Dawa al-mukawama al-islamiyya al-alamiyya (Call for Islamic World Resistance) published in cyberspace in 2004 and running to 1604 pages. A short but interesting is of Breivik's manifesto was conducted by Ryszard M. Machnikowski[37].

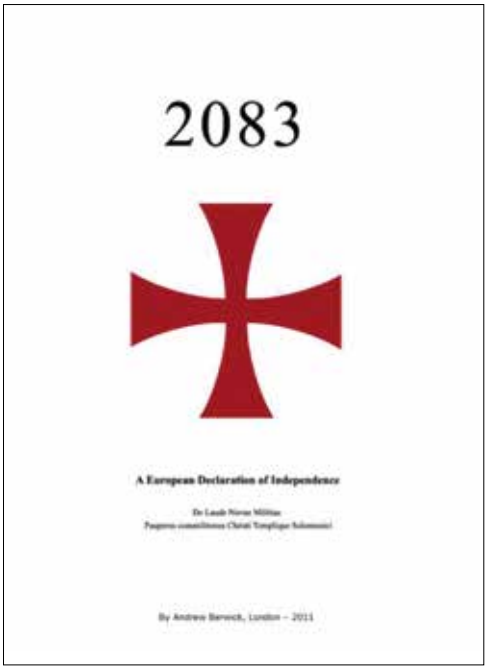

Figure. Title page of Anders Breivik's manifesto.

Source: https://info.publicintelligence.net/AndersBehringBreivikManifesto.pdf [accessed: 1 II 2022].

[36] A. Berwick, *2083. A European Declaration of Independence...*, p. 1.

[37] R.M. Machnikowski, *Zabójcze idee. Co próbują nam przekazać terroryści?* (Eng. Lethal ideas. What are the terrorists trying to tell us?), Łódź 2020, pp. 157–170.

The course of the attack

On 22 July 2011, after 12:00, Breivik returned to the vicinity of the garden centre where he had parked the van the previous day. He got into it through the back door. He changed into an imitation police uniform. He put a bulletproof vest over his sweatshirt. He got out of the luggage compartment, where the bomb had been placed, and sat behind the wheel. He drove up near the seventeen-storey building housing the Ministry of Justice and the Prime Minister's Office. There was a no-entry sign on a chain between two pillars, but he easily avoided it. When he turned towards the entrance of the building, he saw that the best place to park was taken by two cars. Because of this, he had to place the volkswagen differently than he had planned, because the force of the explosion would have focused not on the building, but in the opposite direction. And he planned to destroy the entire office building, just like the aforementioned Timothy McVeigh. Nervously, he lit a fuse sticking out of a hole in the wall separating the cabin from the luggage area. He feared he might be killed by a pre-explosion due to the fumes coming from the bags, but this did not happen. He took the keys but forgot his mobile phone, which he had left on the dashboard, and got out. He locked the car and looked around. In the planning phase of the attack, he had taken into account the possibility of security agents or policemen whom he would have to eliminate, but there was no one. Nevertheless, he took out his pistol and with the gun in his hand started to move away from the car. The two guards monitoring the building on screens did not notice the van. They were informed about the improperly parked car by one of the receptionists in the office building. By this time, Breivik was already out of camera range. He passed a man with a bouquet of roses, who was surprised to see a police officer with a gun in his hand getting into a Fiat Doblo. He noted the make and registration number of the vehicle: VH 24605. At 15:25 there was an explosion. Prime Minister Jens Stoltenberg, who was due to make a speech at Utøya the next day, was on the phone when he heard the bang. His press spokesman, who was injured by the glass, called from his direct phone and made sure that the prime minister was not hurt. Breivik found out about the explosion from the car radio when the broadcast was interrupted to report a strong explosion in the government district[38].

[38] Å. Seierstad, *Jeden z nas...*, pp. 287–292.

The first police car arrived at the scene three minutes after the explosion. At the same time, ten ambulances were sent to the area. The injured were given first aid by passers-by. A state of emergency was declared at Oslo University Hospital. Nine minutes after the explosion, a man identifying himself as Andreas Olsen called the police emergency phone. He reported that a few minutes earlier he had passed a strangely behaving man in police uniform, with a gun in his hand, walking from the government district. He gave details of the car in which the alleged policeman had driven away. It was Olsen who walked with a bouquet of roses and turned his attention to Breivik. The phone call was answered by the policewoman on duty, who carried the piece of paper with the make and registration number of the car noted down into the room and placed it on the chief's desk. The officer on duty was on the phone at that moment. At that time, Breivik was standing in a traffic jam near the capital's opera house. Oslo District Police Headquarters had no notification procedures, so the duty officer at the operations headquarters, instead of coordinating with the commanding officer on the scene, decided that it would be more important to call the officers on duty by phone. During the critical phase, there was no contact between the duty officer at headquarters and the commander in the field, who was in charge of the security and rescue work in the government district. Meanwhile, Breivik was still standing in a traffic jam. He feared that because of the terrorist attack the entire city had been shut down and the streets leaving the capital blocked. But this was not done, not even considered as a possibility. All available patrols were directed to the government district to join the ongoing rescue operations there. Beredskapstroppen - Delta, a special unit of the Norwegian police, whose members are trained to carry out dangerous operations, was also sent in[39]. The explosion killed seven people, an eighth died in hospital and 209 people were injured. The destruction was visible even within a kilometre radius of the epicentre of the explosion. There was little indication in the way the Oslo police operated that a terrorist attack had taken place in Norway and there was a high risk of another. When other police districts offered support, the capital generally rejected it, even though many of Oslo's most strategic facilities were still not secured. The police have closed all roads, but only those leading to and from the centre of the capital, the main railway station, large shopping centres

[39] Ibid., pp. 293–295.

(City and Byporten), the headquarters of the Norwegian news agency NTB, the dailies: "Verdens Gang" and "Aftenposten" and TV2[40]. The attack in the government district was initially attributed to Islamic terrorists and al-Qaeda. This was the opinion of experts on television.

Meanwhile, employees of the parliament administration asked for extra security because there were no armed guards in front of the building. The police informed them that they had to manage on their own. The head of parliamentary security was instructed to lock the buildings. The administration of the Labour Party headquarters asked for police protection and the People's House also requested it[41]. All were refused and advised to evacuate the people. In 2011, the Norwegian police had only one helicopter, and in July its crew was on leave. As a consequence of subsequent budget cuts, there was no system in place in the police force for calling the crew back from leave. One of the pilots himself reported for duty just after 16:00, after hearing about the explosion on the news. He was told he was not needed. At the same time, Delta asked for a helicopter twice over the next hour. The reply was that it was not available, although it was standing on the ground fully prepared for flight. Nor did the police take any steps to mobilise military helicopter crews or use civilian machines. After the explosion in Oslo, a national alert was not immediately issued. Such an alarm triggered special procedures for sending important reports to all police headquarters in the country. In the event of a national alarm, the district commands had specific rules of operation. At Asker and Baerum district headquarters this involved setting up a police blockade on the E16 road near Sollihøgda, where Breivik was travelling. Furthermore, communication between the different police authorities and units was unclear and imprecise. There was a lack of concrete information and decisions[42].

At 15:55, i.e. half an hour after the explosion, someone at the police headquarters happened to notice a piece of paper with the car details given by Andreas Olsen. He was contacted by phone and asked to repeat the report.

[40] E. Czykwin, *Anders Breivik...*, p. 16.

[41] The tradition of People's Houses has been known throughout Scandinavia since the 19th century. They were established with the development of the labour movement as places for meetings and gatherings. In Norway, the first Folk House (Folkets Hus) was built in the 1890s. Today they are used for conferences, celebrations, entertainment and recreational activities.

[42] Å. Seierstad, *Jeden z nas...*, pp. 298–300.

The information was then passed on to the patrols in the capital. However, the media was not asked to provide information on the vehicle being sought and the armed man wearing a police uniform. Nor was the Oslo Traffic Headquarters, which had an extensive camera system, notified. There was a plan in place to deal with a terrorist threat, but it was not implemented. Nor were existing capabilities and resources used. Breivik, meanwhile, had left Oslo. At 16:03 he drove past the police station in Sandvika, and at 16:16 he passed the aforementioned Sollihøgda, heading towards Utøi. At 16:43, the Criminal Police Headquarters (Kripos) broadcast an announcement: *National alert - explosion. Possible bomb(s) in the centre of Oslo. We urge people to be on the lookout for a small grey van, possible registration number 24605. The connection between the explosion and the vehicle is currently unclear. If the vehicle is found, notify the duty officer at Kripos or K.O.P. Oslo for further instructions. Be cautious of the driver and the vehicle. Yours sincerely, Officer on Duty at Kripos*[43]. No word was passed on the fact that the driver of this car, whose letters in the registration number Kripos did not include in the message, was wearing a police officer's uniform. Besides, not many police stations received the message. Either the receiving equipment was not switched on in time, or the alarm frequencies were incorrectly set. This was also the case at the police station for Nordre Buskerud, where Breivik was already in the area. It was located a few kilometres from the ferry landing on Lake Tyrifjorden. Breivik parked his car at some distance from this marina and waited for the ferry that would take him to the island. He told the young people concerned, who were also waiting for the vessel, that because of the attack in Oslo he needed to get to the island to ensure the safety of the young people staying at the camp there. When the ferry MS "Thorbjørn" arrived at the harbour from Utøya, the passengers boarded and the boat headed back towards the island. Breivik's luggage consisted of a box on wheels and a rifle wrapped in plastic. Among the passengers was Monika Bøsei, the head of the centre on Utøya. At 17:10 the ferry reached the shore. Its captain helped Breivik carry the crate ashore, believing it to contain explosive detection equipment. The fake policeman was approached by Trond Bernsten, one of two (unarmed) guards guarding order on the island. Breivik introduced himself as Martin Nilsen (the identity of his former colleague)[44].

[43] Ibid., p. 304.

[44] Ibid., p. 308.

At the time, about 600 young people belonging to the Labour Party youth group were on Utøya, an island measuring about 500 by 300 metres. At 17:22 Breivik fired the first gun shots. The victim was Bernsten. After him, Monika Bøsei was shot. To those lying down Breivik fired two more shots each in the head. The ferry captain, who saw the whole incident, started running towards the island, shouting to the people he met to run away. The other guard, Rune Havdal, was shot in the back as he ran towards the grove. The killer approached the man lying down and fired another shot to the head. He was his third victim. Breivik was in no hurry. He walked calmly behind the largest group of fleeing youths. He planned to shoot as many people as possible and scare others into throwing themselves into the lake and drowning. Within five minutes he had shot 9 people. He then entered the building of the centre where he committed mass murder of the boys and girls there[45]. At about 17:29, the daughter of an officer of the Police Headquarters, who was on the island, called her on-duty father and informed him about the uniformed man who was killing the campers. Residents of the area around the lake, alerted by the sound of gunshots and the sight of smoke rising from the island, called the emergency services. The first units - a fire engine and a police patrol - arrived near the ferry landing at 17:38, followed by ambulances. Local residents rushed to the rescue in their boats and fished out the teenagers who had swum away from the island. On the advice of the village chief, a logistics centre was set up in the nearest village at a hotel 3 km away with a golf course to serve as a landing pad. The decision was also dictated by the fact that the bomber's car was parked at the marina and it was suspected that it might contain explosives. A Criminal Police operations officer arrived at the jetty from a neighbouring district and took charge. At the same time, a medical helicopter arrived with an anaesthetist on board, who was also a paramedic instructor and therefore familiar with most of the emergency services personnel in the area. He took charge of the medical services. The operation was extremely difficult due to the lack of adequate communication systems. Mobile phones were mainly used, which increased the time taken to transmit information, as one call blocked the connection with another caller waiting - a police officer, doctor or ambulance worker. In addition, part of the area was out of mobile phone coverage. The walkie-talkies they had were also failing. The weather made

[45] Ibid., pp. 311–320.

the rescue operation even more difficult. Short briefings were held every 15-20 minutes in the established command centre. Fifty units of various services took part in the action. During the course of the murder, Breivik called the police emergency number twice and introduced himself by name as a member of the anti-communist resistance. He also stated where he was and declared his willingness to hand himself over to the officers. He then interrupted the conversation and continued killing. In Oslo, the decision was made to use Delta. The lack of a helicopter meant that its officers had to use a car. They set off around 17:30 and had to make their way through the congested city. When they reached the shore of Lake Tyrifjorden, a speedboat was waiting for them. Unfortunately, at 18:11 it got stuck in the middle of the lake due to overloading. Support was provided by local residents with their boats. At 18:27 the Delta team reached the shore of the island[46]. It advanced towards the roar of gunfire in a covering formation. In the last seven minutes Breivik shot five more people: four girls and one boy. At 18:34, the bomber, offering no resistance, surrendered to Delta officers, who were surprised to see a white man. He waited for their arrival but did not stop the killing. In 72 minutes he shot 67 people. He shot in the torso and the head. In total, he fired 186 shots, an average of more than two shots per minute. He therefore still had a large supply of ammunition left. He also caused the deaths of two more people, one of whom fell off a high cliff and the other drowned as he tried to swim away from the island. In addition, 32 people were seriously injured but survived. Over the course of an hour and 12 minutes, Breivik shot a total of 99 people, so it took him on average less than a minute to kill or injure each person. In addition, more than 70 people were injured as a result of their attempts to flee the island and the accompanying stress. Most of Breivik's victims killed on Utøya were between 14 and 18 years old. The bomber hoped to find former Prime Minister Gro Harlem Bruntland on the island, but she had returned to Oslo a few hours earlier. He intended to decapitate her with a knife and filmed the incident and posted it on the Internet[47]. Among the injured was Adrian Pracoń, a Norwegian citizen of Polish origin, who recounted his experiences in a book[48].

---

[46] M. Piekarski, K. Wojtasik, *Polski system*..., pp. 20–21.

[47] R.M. Machnikowski, *Zabójcze idee*..., p. 158.

[48] A. Pracoń, *Masakra na wyspie Utøya* (Eng. Massacre on the island of Utøya), Bielsko Biała 2013. In court, Breivik said that he spared Pracoń because he had a right-wing appearance. Even if the terrorist had indeed judged Pracoń in this way, this was to be his last victim.

Conclusions

After ing Breivik's biography, it can be concluded that the Norwegian state, which for years has had a protective policy towards its citizens, in this particular case completely failed. Anders' mother and himself needed psychological care. The environment in which Breivik grew up contributed greatly to his problems. After the attack in Oslo, the state services also failed all the way. After detonating a bomb in the capital, the terrorist easily made his way to the island. The Prime Minister's house was not secured after the incident. Despite the fact that the so-called man with roses informed the police about Breivik's suspicious behaviour, gave his description and car registration numbers, the note got stuck on someone's desk. No roads were closed, no helicopter was dispatched. The pilot, who heard about the events on television, reported himself for duty but was sent home. A helicopter appeared over Utøya during the massacre, but it did not belong to the police, but to one of the TV stations. The cameraman filmed Breivik shooting at the terrified people. It took a long time for the Delta officers to reach the island on the shore of the lake, and only with the help of local residents. When they arrived on the scene, Breivik had surrendered and all that remained was to arrest him. He even had a photograph prepared for the occasion. Had it not been for the mistakes and negligence committed, it would have been possible, if not to prevent this tragic event by surrounding the future assassin with proper care during his adolescence, to significantly reduce the number of victims and even prevent Breivik from reaching Utøya. Now one can only hope that he spends the rest of his life in prison, simply because he has never shown any compassion either for the victims or for their families. Moreover, according to the opinion of Elżbieta Czykwin, there is no chance of rehabilitation in his case. The limit he crossed when he killed so many people caused such big changes in his brain and personality that a return to normality is no longer possible[49].

Breivik was already very tired at this point. Pracoń is a declared homosexual and his appearance may have mattered to Anders, but in a different sense than he described in court. For one of his friends testified that Breivik is a closeted homosexual. So far it is not known if this is true, or what really stopped him from shooting Pracoń. See I. Grelowska, *Anders Breivik. Nakręcony do zbrodni* (Eng. Anders Breivik. Driven to crime), Interia, 20 IX 2019, https://styl.interia.pl/magazyn/news-anders-breivik-nakrecony-do-zbrodni,nId,3213764 [accessed: 21 IX 2019].

[49] I. Grelowska, *Anders Breivik*...

Breivik's followers had similar views, similar problems and personality traits, which consequently led them to extreme violence. Their motivation was also racist ideology and hatred of immigrants or people with dark skin colour. In addition to the imitators already mentioned, similar cases, albeit not as dramatic, but also with fatalities, or attempts to carry out terrorist attacks have been reported in Germany, France, the United Kingdom, Sweden, Estonia, Russia, the Czech Republic and Slovakia, among others. Some of these perpetrators were inspired by Anders Breivik, while others were called "Breiviks" by the media. The Norwegian example has shown that not only Islamic terrorism, which until recently remained the greatest threat, but also extreme right-wing ideologies increasingly find their followers, ready to murder others in their name. Until the attacks in Norway on 22 July 2011, almost all the effort had been focused on combating the threat from Islamic extremists, whose actions are focused on murdering Americans and their allies and, more broadly, all non-believers and Muslims who do not share the only correct views propagated by radical preachers and their followers. Meanwhile, opposition to a multicultural society in Europe and the growing number of Muslim minorities is growing in strength. Political correctness and the self-censorship of pro-government media in Western Europe, which are silent on the negative effects of the presence of immigrants from high-risk countries, including the increase in terrorist threats and common crime, have made cyberspace the main platform for exchanging opinions on this issue. These are often accompanied by racist content and calls for violence, and far-right organisations are growing in strength and using anti-immigrant slogans to gain public support and parliamentary seats. In their shadow, further radicalised individuals are following in the footsteps of Anders Breivik. Meanwhile, the fact that the attack on 22 July 2011 was a protest against multicultural society is ignored, despite the fact that Scandinavian countries, especially Norway, are extremely tolerant and open to foreign cultures, and the Norwegian standard of living has for years been among the highest in the world.

The far right is growing in strength throughout Europe, but within the EU countries, Germany is the worst in this respect. For many years, the German services did not see this threat or underestimated it, because they also focused on Islamic terrorists. There has been an increase in the number of attacks perpetrated by people with a far-right ideology who are loosely connected to some organisational structure or who have no such connection. These are individuals acting alone who, thanks to the Internet and social

media, have gained access to ideological manifestos, instructions on how to carry out terrorist attacks or how to obtain weapons. This is exacerbating the terrorist threat. The popularity of far-right ideology is growing, especially in the context of an anti-immigrant and anti-Muslim narrative. It enjoyed particularly strong support after 2015, which saw the largest influx of irregular migrants into Europe after World War II. It was then that Breivik's followers became even more active. Norway has become a model for a new type of terrorism, because the proponents of the theory of white supremacy and the alleged threat of the native population being replaced by immigrants from Muslim countries are not united by formal organisational structures. Lone wolves seek inspiration online and - following Breivik's example - leave their message before embarking on a terrorist operation. In its 2019 report, the Australian Institute for Economics and Peace pointed out, for example, that the rise in Germany of terrorism motivated by far-right ideology is only part of a much broader phenomenon spanning the entire West. In five years, the number of attacks carried out by people associated with this group has increased by 320 percent[50]. In 2021, more politically motivated crimes were recorded in Germany than in previous years. More than 19 000 of these were committed by suspects from the right-wing political spectrum, more than 17 000 crimes were not classified ideologically by the police (they were linked to public opposition to the authorities' decisions on combating the pandemic), and around 9 000 were attributed to perpetrators motivated by extreme left-wing political views[51].

Breivik and his followers prove that similar terrorist attacks can be carried out anywhere in the world. Classic right-wing thought patterns are also present in Poland. Racism, hatred of Israel, contempt for Islam, anger directed at supporters of migration and volunteers helping migrants are motivating factors. These, combined with the paranoia typical of some right-wing extremists, can give impetus to actions that will have tragic consequences. After the attack in Norway, the Polish police and special

[50] J. Bielecki, *Naśladowcy Breivika rosną w Europie w siłę* (Eng. Breivik's followers are growing in strength in Europe), rp.pl, 23 II 2020, https://www.rp. pl/swiat/art. 871721-nasladowcy-breivika-rosna-w-europie-w-sile [accessed: 24 II 2020].

[51] PAP, *Fala przestępstw politycznych w Niemczech. „Więcej niż kiedykolwiek w ciągu ostatnich 20 lat"* (Eng. Political crime wave in Germany. "More than at any time in the last 20 years"), InfoSecurity 24, 19 I 2022, https://infosecurity24.pl/za-granica/fala-przestepstw-politycznych-w-niemczech-wiecej-niz-kiedykolwiek-w-ciagu-ostatnich-20-lat [accessed: 20 I 2022].

services faced new challenges in preventing acts of terrorism. Cooperation between individual services and units of state and local administration has been institutionalised and tightened, and specialist units have been created within the ABW and Police to monitor cyberspace for racist content[52]. The adopted recommendations made it possible to prevent a terrorist attack prepared by Brunon Kwiecień. This does not mean, however, that the situation in Poland is completely under control, because year by year the confidence of society in the state is decreasing. The results of the 2020 survey of Poles' moods turned out to be so bad that they surprised even the authors themselves. The various shields introduced by the government at the time, which were supposed to protect companies during a coronavirus pandemic, did not reassure citizens fearing a lack of work and money. There was no faith in the effectiveness of the proposed solutions, and confidence in the state proved extremely low. Since then, the country's economic situation has deteriorated. Disputes within the government and social divisions meant that, after the improvement recorded in autumn 2021, public sentiment further deteriorated[53]. This difficult situation was partly masked by the conflict in Ukraine. Poles became aware that refugees from across the eastern border had lost everything but saved their lives. The involvement of a large part of the population in helping the Ukrainians and the images of war damage and victims shown by the media distracted Polish citizens for a while from worrying information about the economic situation, inflation, high prices and the coronavirus pandemic. The war has also caused the further perspective on life to cease to have much meaning for people. They are worried about the immediate future. They fear that military action will move into our country and that a nuclear conflict, however unlikely at present, is not impossible. Vladimir Putin has nothing left to lose. Forecasting the scale of the terrorist threat, not to mention

---

[52] This issue is presented in detail in: *Zamach w Norwegii. Nowy wymiar zagrożenia terroryzmem w Europie* (Eng. Assassination in Norway. A new dimension of the terrorist threat in Europe), K. Liedel, P. Piasecka, T.R. Aleksandrowicz (sci. eds.), Warszawa 2011.

[53] *Tsunami uderzy w gospodarkę i finanse Polaków. Wyniki badań zszokowały nawet ich autorów* (Eng. Tsunami will hit the economy and finances of Poles. Research results shocked even their authors), Forbes, 12 V 2020, https://www.forbes.pl/gospodarka/nastroje-spoleczne-w-polsce-w-kwietniu-2020-badanie-irg-sgh-i-zpf-dr-slawomir-dudek/4mdqnw7 [accessed: 14 III 2022]; PAP, *Jakie są nastroje społeczne w Polsce? Zaskakujące wyniki najnowszego sondażu* (Eng. What is the public mood in Poland? Surprising results of the latest poll), DEON, 21 X 2021, https://deon.pl/swiat/jakie-sa-nastroje-spoleczne-w-polsce-zaskakujace-wyniki-najnowszego-sondazu, 1654190 [accessed: 14 III 2022].

including lone wolves in these predictions, is very difficult because it is impossible to predict the development of the situation in Ukraine, and it has a huge impact on security in our country. We can only say with certainty that the threat is currently high and will continue to grow.

The Russian invasion of Ukraine has also increased the level of terrorist threat online. Russian attacks on Polish cyberspace have been ongoing for a long time. The fears and anxieties present in society, fuelled by the activity of trolls and the dissemination of fake news, are exacerbating social tensions. Agents of influence play a significant role in this. A few days before the Russian aggression, the number of anti-Ukrainian and pro-Russian comments suddenly increased in Polish cyberspace. Many of them were fake news, but a large part of them were opinions of authors from extreme right-wing circles, who had previously spoken about the threat from Ukrainian nationalists, motivated to a large extent by the heritage and ideology of Stepan Bandera and the Organisation of Ukrainian Nationalists. The posts reproduced, among other things, themes from Putin's speech, in which he argued for Russia's recognition of the independence of two separatist republics in eastern Ukraine. This anti-Ukrainian narrative was reproduced in far-right forums[54]. The historically justified anti-Ukrainian character of nationalist organisations in Poland (far-right Ukrainian organisations have similar resentments towards Poland) is nothing special, especially since, during the protracted war, the hostile rhetoric became almost silent on internet portals, where neutral journalism, not referring to either side of the conflict in Ukraine, began to dominate. However, hateful comments still appear on social media. The situation may become more acute in the event of a prolonged conflict in Ukraine and an increasing number of war refugees from the country. Admiration for the determination of the defenders, patriotically motivated and united, public recognition of the heroism of the Ukrainians, enthusiasm and help for the refugees will gradually wane and may turn into indifference and then into dissatisfaction with the presence of hundreds of thousands of newcomers from across the eastern border. It can be assumed that refugees and the EU will be blamed for the deterioration of the economic

[54] See *„Mądry Putin" i „sztuczne państwo Ukraina" – antyukraińskie narracje w polskiej sieci* (Eng. "Wise Putin" and "artificial state of Ukraine" - anti-Ukrainian narratives in Polish internet), Konkret 24, 23 II 2022, https://konkret24.tvn24.pl/polska,108/madry-putin-i-sztuczne-panstwo-ukraina-antyukrainskie-narracje-w-polskiej-sieci,1097200.html [accessed: 23 II 2022].

situation in Poland and the high prices of goods. It can also be assumed that the Ukrainians staying in Poland will be too insistent in expressing their patriotism and spreading nationalist ideas, for example by placing Ukrainian symbols and slogans on the facades of buildings. This may displease Polish society and inflame the activity of domestic nationalist groups, becoming a source of hatred, aggression, violence and mutual recrimination. In the initial period of the migration wave from Ukraine such activists were 'patrolling' areas near border crossings in Podkarpacie and behaving aggressively towards Asians and Africans crossing the border with Ukrainians. It follows that the war across the eastern border has not significantly affected racist behaviour, it may have reduced its scale, but it has not eliminated it from the public space.

Depending on how the war in Ukraine ends, it will have far-reaching implications for security in Europe and the terrorist threat. On 27 February 2022, three Russian saboteurs were arrested in Ukraine. On one of them a notebook was found with the address of a hotel in Zgorzelec (its owner turned out to be a person with a criminal past), the names of two nearby towns: Liberec in the Czech Republic and Markersdorf in Germany, as well as the phone numbers and names of two people: Igor and Artem. The second one was marked "coordinator"[55]. The danger is therefore great. This has also been pointed out by the German services, which estimate that there may be between 200 and 2 000 Russian agents operating in their country. Their aim is not only to gather information on politicians and companies that criticise Russia, but they may also be preparing attacks on NATO bases in Germany as well as acts of sabotage and diversion. They recruit young men, especially in East Germany, where in recent years there have already been several mysterious explosions at armament plants and arms depots[56]. Russia will also carry out destabilising and

[55] M. Rybak, *Rosyjscy dywersanci, złapani na Ukrainie mieli w notesie adres hotelu w Zgorzelcu* (Eng. Russian saboteurs caught in Ukraine had address of hotel in Zgorzelec in notebook), Wyborcza, 28 II 2022, https://wroclaw.wyborcza.pl/wroclaw/7,35771,28164136,dywersanci-zlapani-przez-ukrainskie-sluzby-mieli-kartke-z.html [accessed: 3 III 2022]; the same, *"Wyborcza" ustaliła hotel w Zgorzelcu z notesu dywersantów złapanych na Ukrainie. Ma gangsterską przeszłość* (Eng. "Wyborcza" established a hotel in Zgorzelec from the notebook of divers caught in Ukraine. It has a gangster past), Wyborcza, 1 III 2022, https://wroclaw.wyborcza.pl/wroclaw/7,35771,28167910,wyborcza-ustalila-hotel-w-zgorzelcu-z-notesu-dywersantow.html [accessed: 3 III 2022].

[56] V. Baran, *Niemcy. Służby: grożą nam akty dywersji* (Eng. Germany. Services: we are threatened by acts of diversion), Wirtualna Polska, 7 III 2022, https://wiadomosci.wp.pl/niemcy-sluzby-groza-nam-akty-dywersji-6744701005154912a [accessed: 7 III 2022]; T. Waleński,

subversive activities in Poland. This creates room for terrorists with different ideologies and sympathies. They may be anti-Polish, anti-Russian, anti-Ukrainian, anti-NATO or anti-EU. In any case, the new group of terrorists may have an easier task when it comes to choosing their targets and motivation. They may not necessarily be driven by a racist, anti-immigrant ideology like Anders Breivik, but his successors may also want to exist.

Bibliography

Czykwin E., *Anders Breivik. Między dumą a wstydem* (Eng. Anders Breivik. Between pride and shame), Warszawa 2019.

Haszczyński J. et al., *Robił zakupy we Wrocławiu, podziwiał Jana III Sobieskiego* (Eng. He shopped in Wrocław, admired Jan III Sobieski), "Rzeczpospolita", 26 VII 2011.

Kącki M., *Breivik kupił lont w Polsce* (Eng. Breivik bought the fuse in Poland), "Gazeta Wyborcza", 23 VIII 2011.

Zamach w Norwegii. Nowy wymiar zagrożenia terroryzmem w Europie (Eng. Attack in Norway. A new dimension of the terrorist threat in Europe), K. Liedel, P. Piasecka, T.R. Aleksandrowicz (sci. eds.), Warszawa 2011.

Machnikowski R.M., *Zabójcze idee. Co próbują nam przekazać terroryści?* (Eng. Lethal ideas. What are the terrorists trying to tell us?), Łódź 2020.

Piekarski M., Wojtasik K., *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku* (Eng. The Polish anti-terrorist system and the reality of attacks in the second decade of the 21st century), Toruń 2020.

Pracoń A., *Masakra na wyspie Utøya* (Eng. Massacre on the island of Utøya), Bielsko Biała 2013.

Rybak M., *Wrocławianin, który sprzedał chemikalia Breivikowi, miał kiedyś problemy z prawem* (Eng. Wrocław man who sold chemicals to Breivik once had legal problems), "Gazeta Wrocławska", 22 XI 2011.

Stingery i Javeliny sieją strach u Rosjan. Ale broni dla Ukrainy może zabraknąć (Eng. Stingers and Javelins sow fear in the Russians. But there may not be enough weapons for Ukraine), Wirtualna Polska, 11 III 2022 r., https://wiadomosci.wp.pl/moga-sie-pojawic-problemy-z-dostawami-sprzetu-wojskowego-do-ukrainy-6746062264457824a [accessed: 11 III 2022].

Seierstad Å., *Jeden z nas. Opowieść o Norwegii* (Eng. One of us. A story about Norway), Warszawa 2013.

Turrettini U., *The Mystery of the Lone Wolf Killer: Anders Behring Breivik and the Threat of Terror in Plain Sight,* New York 2015.

Internet sources

Anders Breivik był zatrzymany przez niemiecką policję dwa lata przed zamachem na wyspie Utöya. Miał przy sobie amunicję i części uzbrojenia. Został wypuszczony na wolność (Eng. Anders Breivik was detained by German police two years before the Utöya island attack. He had ammunition and weapon parts on him. He was released), Wirtualna Polska, 14 I 2016, https://wiadomosci.wp.pl/anders-breivik-byl-zatrzymany-przez-niemiecka-policje-dwa-lata-przed-zamachem-na-wyspie-utoya-mial-przy-sobie-amunicje-i-czesci-uzbrojenia-zostal-wypuszczony-na-wolnosc-6027685648360577a [accessed: 15 I 2016].

Baran V., *Niemcy. Służby: grożą nam akty dywersji* (Eng. Germany. Services: we are threatened by acts of diversion), Wirtualna Polska, 7 III 2022, https://wiadomosci.wp.pl/niemcy-sluzby-groza-nam-akty-dywersji-6744701005154912a [accessed: 7 III 2022].

Berwick A., *2083. A European Declaration of Independence. De laude novae militiae. Peuperes commilitiones Christi Templique Solomonici,* London 2011, https://info.publicintelligence.net/AndersBehringBreivikManifesto.pdf [accessed: 1 II 2022].

Bielecki J., *Naśladowcy Breivika rosną w Europie w siłę* (Eng. Breivik's followers are growing in strength in Europe), rp.pl, 23 II 2020, https://www.rp.pl/swiat/art.871721-nasladowcy-breivika-rosna-w-europie-w-sile [accessed: 24 II 2020].

Death S., *Anders Breivik massacre: Norway's worst nightmare,* The Guardian, 25 II 2015, https://www.theguardian.com/world/2015/feb/22/anders-breivik-massacre-one-of-us-anne-seierstad [accessed: 28 IV 2015].

Grelowska I., *Anders Breivik. Nakręcony do zbrodni* (Eng. Anders Breivik. Driven to crime), Interia, 20 IX 2019, https://styl.interia.pl/ magazyn/ news-anders-breivik-nakrecony-do-zbrodni,nId,3213764 [accessed: 21 IX 2019].

Grochot A., *Anders Breivik zostanie w więzieniu. Sąd odrzucił jego wniosek* (Eng. Anders Breivik will stay in prison. The court rejected his request), RMF24, 1 II 2022, https://www.rmf24.pl/fakty/swiat/news-anders-breivik-zostanie-w-wiezieniu-sad-odrzucil-jego-wniosek,nId,5806130#crp_state=1 [accessed: 1 II 2022].

https://www.vmc.org.pl/pirotechnika/materiay-wybuchowe/inicjujce/item/297-diazodinitrofenol [accessed: 31 I 2022].

Kittel B., Jabrzyk J., *Czy Polak pomógł Breivikowi* (Eng. Did a Pole help Breivik), TVN24, 22 XI 2011, https://tvn24.pl/polska/czy-polak-pomogl-breivikowi-ra191578-3531692 [accessed: 23 XI 2011].

„Mądry Putin" i „sztuczne państwo Ukraina" – antyukraińskie narracje w polskiej sieci (Eng. "Wise Putin" and "artificial state of Ukraine" - anti-Ukrainian narratives in Polish internet), Konkret 24, 23 II 2022, https://konkret24.tvn24.pl/polska,108/madry-putin-i-sztuczne-panstwo-ukraina-antyukrainskie-narracje-w-polskiej-sieci,1097200.html [accessed: 23 II 2022].

Norway gunman claims he had nine-year plan to finance attacks, The Guardian, 25 VII 2011, https://www.theguardian.com/world/2011/jul/25/norway-gunman-attack-funding-claim [accessed: 27 I 2022].

PAP, *Fala przestępstw politycznych w Niemczech. „Więcej niż kiedykolwiek w ciągu ostatnich 20 lat"* (Eng. Political crime wave in Germany. "More than at any time in the last 20 years"), InfoSecurity 24, 19 I 2022, https://infosecurity24.pl/za-granica/fala-przestepstw-politycznych-w-niemczech-wiecej-niz-kiedykolwiek-w-ciagu-ostatnich-20-lat [accessed: 20 I 2022].

PAP, *Jakie są nastroje społeczne w Polsce? Zaskakujące wyniki najnowszego sondażu* (Eng. What is the public mood in Poland? Surprising results of the latest poll), DEON.pl, 21 X 2021, https://deon.pl/swiat/jakie-sa-nastroje-spoleczne-w-polsce-zaskakujace-wyniki-najnowszego-sondazu, 1654190 [accessed: 14 III 2022].

Potocka J., *Hitlerowskie pozdrowienie i nowe hasła. Breivik chce wyjść na wolność* (Eng. Hitler salute and new slogans. Breivik wants to go free), RMF24, 18 I 2022, https://www.rmf24.pl/raporty/raport-zamachy-w-norwegii/fakty/news-hitlerowskie-pozdrowienie-i-nowe-hasla-breivik-chce-wyjsc-na,nId,5777148#crp_state=1 [accessed: 18 I 2022].

Profile: Anders Behring Breivik, BBC, 12 IV 2012, https://www.bbc.com/news/world-europe-14259989 [accessed: 14 V 2012].

Rybak M., *Rosyjscy dywersanci, złapani na Ukrainie mieli w notesie adres hotelu w Zgorzelcu* (Eng. Russian saboteurs caught in Ukraine had address of hotel in Zgorzelec in notebook), Wyborcza.pl, 28 II 2022, https://wroclaw.wyborcza.pl/wroclaw/7,35771,28164136,dywersanci-zlapani-przez-ukrainskie-sluzby-mieli-kartke-z.html [accessed: 3 III 2022].

Rybak M., *„Wyborcza" ustaliła hotel w Zgorzelcu z notesu dywersantów złapanych na Ukrainie. Ma gangsterską przeszłość* (Eng. "Wyborcza" established a hotel in Zgorzelec from the notebook of saboteurs caught in Ukraine. It has a gangster past), Wyborcza.pl, 1 III 2022, https://wroclaw.wyborcza.pl/wroclaw/7,35771,28167910,wyborcza-ustalila-hotel-w-zgorzelcu-z-notesu-dywersantow.html [accessed: 3 III 2022].

Sobańda A., *Skąd wziął się Breivik i czy można go było powstrzymać? Przejmująca opowieść o Norwegii* (Eng. Where did Breivik come from and could he have been stopped? A moving story about Norway), Dziennik.pl, 21 VIII 2015, https://kultura.dziennik.pl/ksiazki/artykuly/498350,jeden-z-nas-przejmujaca-opowiesc-o-norwegii-autorstwa-asne-seierstad.html [accessed: 24 VIII 2015].

Tsunami uderzy w gospodarkę i finanse Polaków. Wyniki badań zszokowały nawet ich autorów (Eng. Tsunami will hit the economy and finances of Poles. Research results shocked even their authors), Forbes.pl, 12 V 2020, https://www.forbes.pl/gospodarka/nastroje-spoleczne-w-polsce-w-kwietniu-2020-badanie-irg-sgh-i-zpf-dr-slawomir-dudek/4mdqnw7 [accessed: 14 III 2022].

Waleński T., *Stingery i Javeliny sieją strach u Rosjan. Ale broni dla Ukrainy może zabraknąć* (Eng. Stingers and Javelins sow fear in the Russians. But there may not be enough weapons for Ukraine), Wirtualna Polska, 11 III 2022, https://wiadomosci.wp.pl/moga-sie-pojawic-problemy-z-dostawami-sprzetu-wojskowego-do-ukrainy-6746062264457824a [accessed: 11 III 2022].

DOI: 10.4467/27204383TER.22.028.16348

ORCID: 0000-0003-4892-6112

KRZYSZTOF KAROLCZAK

Financing of terrorism - an overview

Abstract

The article discusses the basic sources of financing of 20th-century and 21st century terrorism: seizures for banks, abductions for ransom, smuggling and drug trafficking. As specific methods, those that used Islamic State were also listed, including Crude oil trading in occupied areas, trade in monuments and others. The issue of terrorism sponsored by the state was included separately.

Keywords:

financing terrorism, attacks on banks, abduction of ransom, drug smuggling and trade, Islamic State, terrorism sponsored by the state

(...) *one thing remains certain - terrorism is a business requiring low financial resources*[1].

This article discusses the ways in which terrorism is financed with a historical perspective. Learning about the mechanisms that accompany the phenomenon of terrorist financing can potentially help in countering

[1] The motto comes from the book: W. Dietl, K. Hirschmann, R. Tophoven, *Terrorism*, Warszawa 2009, p. 315.

and combating terrorism. Terrorism is a method of political activity that is subject to change over time, but at the same time repetitive, as a result of the socio-economic-political conditions in which people who use terrorism operate. It is therefore worth looking at how the financing of terrorism has evolved over the last 150 years. Technological advances allow terrorists use the latest technical inventions that can guarantee their success. In the nineteenth century, they used bladed weapons, firearms and homemade bombs, but it was not until the proliferation of means of transport (cars, trains, aeroplanes) in the twentieth century that it became easier for terrorists to move around, transport the means to carry out an attack and even be a tool for carrying it out. The technological revolution in information technology in the 21st century has made it possible for terrorists to communicate not only through classical methods (messengers, mail, landlines), but also through networks and computer systems (i.e. in cyberspace). On the internet, they can also find instructions on how to construct explosives, recruit members to their organisations and send money. The terrorists' use of cyberspace and their search for sources of funding for their activities is a challenge for special services, which should prevent attacks and not only react to their effects.

The article shows how specific attacks were financed and how terrorist organisations obtained funds for their activities. The author does not address the issue of countering the financing of terrorism - both domestically and internationally - and so-called money laundering, as these are issues that require a separate analysis.

The history of terrorism and the activities of groups deemed to be terrorist have been the subject of hundreds of studies. However, their authors have rarely dealt with financial issues, treating them marginally. Presumably, they assumed that terrorists have the financial means to carry out their activities, without going into where these funds come from. It was not until detailed multi-pronged research into the phenomenon of terrorism that the sources of funding for terrorist activities were identified. This kind of systematic research only started to be carried out from the 1990s onwards, not least because terrorism (especially after the attacks of 11 September 2001) was recognised as one of the greatest threats to the modern world.

Several proposals for a systemic view of terrorist financing have emerged in recent years. One of these is the 1987 classification of terrorist

groups by their main source of funding, developed by William A. Tupman of the University of Exeter[2].

Table. Classification of terrorist groups by source of funding[3].

Type of group or scenario (activity)	Source of funding
Domestic terrorism	
Anticolonial (nationalist).	State-sponsored, also donations.
Ethnic, religious and cultural minorities.	Donations, kidnappings; criminal activities.
Ideological minorities, left.	Bank robberies.
Ideological minorities, right.	Wealthy individuals.
Government sponsored groups.	Employers.
Urban guerrillas, i.e. groups large enough to have serious chance of overthrowing government.	Donations, revolutionary tax.
International terrorism	
Exiles.	Bank robberies and some donations.
Exiles auxilliaries.	Funded by "exiles".
Internationalists.	Attempting to make use of so-called *war chests* [in which, according to tradition, resources, funds gained in previous actions, are stored].
Playing the role of a screen for other [groups] (*catspaws*).	State sponsored.
Counterrevolutionaries	State sponsored and also wealthy individuals.
Islamic fundamentalist groups (now more frequently referred to as jihadist).	Charities [of the faithful], individuals.
Unorganised imitators	If funded at all, not really unorganized, but many trained in Afghanistan in credit card fraud and similar small scale white collar crime.

Source: *Funding of terrorist groups compared*, http://moneyjihad.wordpress.com/2013/01/21/funding-of-terrorist-groups-compared/ [accessed: 3 V 2022].

More than 30 years have passed since Tupman's publication and during this time many new sources of terrorist funding have emerged. While one may have reservations not so much about the classification

[2] See *Funding of terrorist groups compared*, Money Jihad, 21 I 2013, http://moneyjihad.wordpress.com/2013/01/21/funding-of-terrorist-groups-compared/ [accessed 3 V 2022].

[3] The table is an accurate translation of the original text. The translations of the table text and the other texts in the article are from the author (editor's note).

of the groupings themselves, but about the unambiguous identification of the sources of funds held by the groupings, it is nevertheless worth keeping in mind, as it can be seen as a prelude to further research into the phenomenon, which in turn will effectively halt the acquisition of these funds from the sources identified.

In 2014, the Australian government agency AUSTRAC[4] produced a report on the source of terrorist funding in Australia. The precise identification of these sources may be useful for research on other geographical areas as well. According to the authors of the report[5]: *Key channels used to raise funds for terrorist financing in or from Australia include:*

- charities and not-for-profit organisations,
- self-financing from legitimate sources,
- fraud, theft and drug trafficking,
- ransom payments.

What the report finds interesting from the perspective of examining terrorist financing is what it says about self-financing terrorist activities from legitimate sources:

> Smaller groups or individuals acting on their own may seek to fund their activities from legitimate sources, allowing them to raise small or moderate amounts relatively quietly. In such cases, it may be difficult for financial institutions to distinguish between transactions designed to fund terrorist activities and ordinary day-to-day transactions - in both cases, the funds come from legitimate sources that are unlikely to arouse suspicion. In the case of smaller extremist groups and lone wolves, self-financing may provide them with sufficient resources to launch an uncomplicated but potent attack. (...) Small, loosely organised Australian extremist groups have been observed to collect regular contributions from members. In at least one case of Australian terrorism (...) a cash box known as 'sandooq' was used to collect financial contributions[6].

---

[4] Australian Transaction Reports and Analysis Centre – Australian government agency responsible for detecting and containment criminal abuse of the financial system of the state.

[5] *Terrorism financing in Australia 2014*, AUSTRAC website, https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/terrorism-financing-australia-2014 [accessed: 3 V 2022].

[6] Ibid.

In this passage of the report, the concept of 'sandooq' (Urdu: صندوق.) - unheard of in other analyses - appears (some analyses often write about the hawala system, but it consists of something else). The word 'sandooq' can be translated as 'box', used to store the contributions of members of a group planning a terrorist attack. The report describes a case from Melbourne in 2005. One person was the treasurer and holder of the sandooq. Another approved members of the group who could use the funds held in the sandooq. All members contributed to the fund, some contributing 100 Australian dollars a month. At the time of the group's arrest, its budget was approximately 19,000 Australian dollars.

The methods of financing terrorist activities listed in the AUSTRAC report are obviously not the only ones used by terrorists, as evidenced by the fact that the report cites examples relating to Australia only (other methods of financing terrorism with examples are described later in the article).

The Forbes list of the 10 richest terrorist groups dates from the same year as the Australian report[7]. Its author, Itai Zehorai, a journalist from the Israeli edition of Forbes, characterises the successive organisations in terms of their region of operation, objectives, methods used and financial resources, and lists their main sources of funding.

1. ISIS:
   - annual turnover: USD 2 billion,
   - main sources of funding: oil trafficking, kidnapping and ransoms, collection of ransoms and taxes, bank robberies and looting.
2. Hamas:
   - annual turnover: USD 1 billion,
   - main sources of funding: taxes and fees, financial aid and donations (especially from Qatar).
3. FARC[8]:
   - annual turnover: USD 700 million,
   - main sources of funding: drug production and trafficking, kidnapping and ransom, mineral extraction (especially gold), fees and taxes.

[7] *The World's 10 Richest Terrorist Organizations*, Forbes, 12 XII 2014, http://www.forbes.com/sites/forbesinternational/2014/12/12/the-worlds-10-richest-terrorist-organizations/#336a6802ffae [accessed: 22 V 2022].

[8] Fuerzas Armadas Revolucionarias de Colombia – Colombian guerrilla group, now operating legally as the party Revolutionary Alternative People's Force.

4. Hezbollah:
   – annual turnover: USD 500 million,
   – main sources of funding: financial aid and donations (especially from Iran), drug production and trafficking.
5. Taliban:
   – annual turnover: USD 400 million,
   – main sources of funding: drug trafficking (mainly opium and heroin production), sponsorship fees and taxes, financial aid and donations.
6. Al-Qa'ida:
   – annual turnover: USD 150 million,
   – main sources of funding: financial aid and donations, kidnapping, ransom and drug trafficking.
7. Lashkar-e-Taiba (Army of the Righteous):
   – annual turnover: USD 100 million,
   – main sources of funding: financial aid and donations.
8. Al-Shabab:
   – annual turnover: approximately USD 70 million,
   – main sources of funding: kidnapping and ransom, illegal trafficking and piracy activities, sponsorship fees and taxes.
9. Real IRA:
   – annual turnover: USD 50 million,
   – main sources of funding: smuggling and illicit trafficking, aid and donations.
10. Boko Haram:
    – annual turnover: USD 25 million,
    – main sources of funding: kidnapping and ransom, fees and taxes, protection, bank robbery and looting.

After analysing this overview, the following regularity can be observed - all the listed methods of fundraising should be classified as criminal offences and are no different from those used by criminal organisations. Bank robberies (financial institutions), kidnappings for ransom and drug trafficking have been known for decades as methods of operation of both individual criminals and organised crime groups. Only the purposes for which these crimes are carried out are different.

Financing of activities from the personal assets of the attacker

It is easiest to identify the source of funding for an attack carried out by a single terrorist, referred to - mainly by the media - as a 'lone wolf', who is not connected to any community and who is not a member of any group that could provide him with support (e.g. logistical) during the execution of the attack.

It is also easier to identify the financing of attacks carried out by 19th century terrorists than by contemporary terrorists, due to the fact that most modern attacks are carried out by members of groups that often have millions of dollars at their disposal, and these groups have become financial enterprises (institutions) of sorts.

An example of an assassin who financed his attack himself is Antoni Berezowski. The cost of the assassination attempt and the source of the money are known - approximately. This former January Uprising insurgent (he took part in it as a 16-year-old) had been living in Paris since 1865, and when he learned that Tsar Alexander II was due to visit France in June 1867, he decided to assassinate him. At the time, he was working as a locksmith in the workshops of the Gouin brothers' Northern Railway and had few financial resources. On 5 June 1867, he bought a double-barrelled pistol for 5 francs (according to other sources, 9 francs). As he did not have enough money for bullets, he pawned his overcoat in a pawnshop and completed the armament with the 8 francs he received. Thus the cost of the assassination can be estimated at a dozen francs[9]. Berezowski, who was caught at the scene of the assassination, was sentenced to life imprisonment (exile) on the island of Nou in New Caledonia.

The cost of the assassination attempt on French President Marie-François Sadi Carnot, carried out in Lyon on 24 June 1894, is also known. Sante Geronimo Caserio, an Italian by origin, after spending five months in prison in 1892 on charges of being active in Milanese anarchist circles, travelled via Switzerland to France, where he settled in the small village of Cette (today's Séte) in Languedoc and began working in the learned profession of baker. However, after the death sentence was passed on Auguste Vaillant (the perpetrator of the National Assembly bombing of 9 December 1893) and he was not pardoned by the President, Caserio decided to take revenge. On 23 June 1894, he collected his pay (20 francs),

[9] Until 1873, the franc was based on silver parity. One franc contained 4.5 grams of pure silver.

left his job, bought back a knife with a fifteen-centimetre blade for 5 francs at a butcher's shop and went to Lyon, where Carnot was visiting in those days. The next day, near the buildings of the stock exchange and the Crédit Lyonnais, using the knife he had bought, he attacked the president going in his carriage to a gala held in his honour. He inflicted only one blow (versions vary here: to the heart, stomach or liver), which proved fatal. Caserio was apprehended and, after an investigation and a trial lasting only two days, he was sentenced to death. The sentence by beheading on the guillotine was carried out on 16 August 1894.

The two examples cited above perfectly illustrate the fact that considerable financial resources are not needed to carry out a terrorist attack. Today, however, it would be difficult to find exemplifications of such 'self-sufficient' assassins. Probably Theodore Kaczynski, an American with Polish roots, who was nicknamed the "Unabomber" by the FBI, can be regarded as such. Kaczynski gave up a promising career in science, abandoned civilisation in favour of a life in nature (he built a wooden house in the woods near the town of Lincoln, Montana, and farmed the land) and took up arms against what he called technological civilisation. For 17 years, he terrorised people in the scientific world and corporations by sending them trap letters. In all, he sent 16 of them: the first on 25 May 1978, the last on 24 April 1995. As a result of bombs placed in the letters, three people were killed and 29 injured. After a lengthy investigation, following a denunciation by his own brother, he was arrested and sentenced to life imprisonment in 1998.

Terrorists using their own financial resources were also Timothy McVeigh (perpetrator of the 19 April 1995 Oklahoma City attack) and Anders Breivik (who carried out two attacks in Norway on 22 July 2011), who are well known to the public because of the consequences of the attacks they carried out. In addition to these, one would more than likely have to add dozens of perpetrators of attacks involving driving a car into passers-by or attacking, for example, customers of shopping malls with a knife.

The finances of an organisation carrying out terrorist attacks

An organisation whose members carry out terrorist attacks must have the funds not only to carry out its task, but often also to help its members living in hiding. For this reason, when the organisation cannot count on

outside support, it resorts to common crimes to provide it with an inflow of cash.

Bank and other financial institution robberies

Simple internationally known method of obtaining money has been and continues to be robbery of banks or other places where the necessary funds can be obtained. According to the Encyclopaedia of Terrorism[10], during two months in 1972, The Red Army Faction (German: Rote Armee Fraktion, RAF) carried out six bank robberies, raising USD 185,000. These are not the only such actions showing the scale of this type of action. RAF leader Ulrike Meinhof, quoted there, was said to justify bank robberies in this way: Nobody thinks that a bank robbery in itself changes anything. It is justified because otherwise the financial problem could not be solved at all. It is tactically justified because it is a proletarian action. It is strategically justified because it is used to finance guerillas[11]. The words of former Brazilian army sergeant Pedro Lobo de Oliveira, who took part in the 1968 attack on the Banco Brasileiro de Descontinos in Sao Paulo, are quite different in this context:

> When I go to plant a bomb, I am aware that it will be obvious to the repressive apparatus as well as to the people, if I am killed or captured, that it was a revolutionary action. However, a bank robbery is something completely different. It causes psychological problems. A bank is robbed in order to loot the money in it. I felt the fear that the people would not understand why we needed the money, that they would not grasp the meaning of our action. For if we were arrested, it would be reported in the press: such and such, caught during a bank robbery. I asked myself: how will I prove to the people that the money from the robbery was for the revolution[12].

Members of the Combat Organisation of the Polish Socialist Party had no such scruples when they carried out, as they said, 'expropriations', robbing from postal wagons the money being transported from the Vistula

[10] *Encyklopedia terroryzmu* (Eng. Encyclopedia of terrorism), B. Zasieczna (ed.), Warszawa 2004.

[11] Ibid., p. 243.

[12] K. Karolczak, *Lewicowy terroryzm w Ameryce Łacińskiej* (Eng. Left-wing terrorism in Latin America), "Warsztat" 1984, no. 1, p. 46.

Country to the cities of the Russian Tsar. They did this 'for the revolution' and 'in the name of the revolution'. In an action near Rogowo on 8 November 1906, more than 30,000 roubles were stolen, 14,000 roubles were stolen near Sławków on 12 August 1907, and 200,812 roubles and 61 kopecks were stolen near Bezdany on 26 September 1908.

Kidnappings for ransom

Kidnapping for ransom has been one of the primary forms of criminal activity for many decades. It is a method that is simple to carry out and, as history has shown, very often effective. Awareness of this at some point reached terrorist groups, who decided to use it to raise funds for their activities.

The first such action was carried out by Latin American terrorists[13]. On 23 May 1971, an Argentine organisation called the People's Revolutionary Army (Spanish: Ejército Revolucionario Popular, ERP) abducted Stanley Sylvester, head of the Swift Meat Packing plant in Rosario (he was also the British Honorary Consul in the city). However, this was a non-standard abduction for ransom, as the kidnappers did not demand money for his release, but a distribution of food and clothing worth USD 62,500 to the poor population. The company agreed to this and Sylvester was released a week later.

On 22 March 1972, the ERP abducted Oberdano Sallustro, the executive director of FIAT's Buenos Aires factory. This time, too, the kidnappers demanded not money directly, but, among other things, the distribution of 'gift packages' worth one million dollars to poor students in schools throughout the country. This time, under pressure from the authorities, the demand did not materialise (in addition to the 'gift packages', members of the organisation demanded that 50 members of the group be released from prison and allowed to fly to Algeria, and that 250 FIAT workers in Córdoba be reinstated. After a police operation to free Sallustro, it emerged that he had previously been killed by his kidnappers.

Further abductions occurred in 1973: On 2 April, the victim was Anthony R. DaCruz, manager of the Eastman Kodak Company in Buenos

[13] All information is taken from the book: N. Antkol, M. Nudell, *No One Neutral. Political Hostage-Taking In the Modern World*, Ohio 1990, pp. 48–51. See *Los actos terroritas del E.R.P. y Montoneros*, Buen Día Noticia, 31 VII 2018, https://buendianoticia.com/nota/10960/los-actos-terroristas-del-erp-y-montoneros [accessed: January–May 2022].

Aires, who was released on 7 April after a ransom of USD 1.5 million had been paid; on 23 May, businessman Aaron Bellinson was abducted (ransom to be USD 1 million); on 6 June, Charles Lockwood was kidnapped (ransom USD 2 million); and on 18 June, John R. Thompson was kidnapped (ransom USD 3 million). It is noteworthy that the victims of the kidnappings were not Argentinians, but US and UK citizens who represented their companies in Argentina.

Al-Qa'ida also carried out abductions for ransom. And although after the attacks of 11 September 2001 United States tried to force its allies to respect the 'you don't negotiate with terrorists' position, after the 7 September 2004 kidnapping of two Italian women, Simona Pari and Simona Torretta, humanitarian aid workers (along with two Iraqis), the Italian government is believed to have paid a USD 5 million ransom. All four were released on 28 September 2004.

Kidnappings for ransom have become a primary source of income for Al-Qa'ida of the Islamic Maghreb (Arabic: Tanzim al-Qaida bi Bilad al-Maghribang), a group known as AQIM (Al-Qa'ida in the Islamic Maghreb), transformed in January 2007 from the Salafist Group of Prayer and Struggle (Arabic: Al.-Jama'a as-Salafiyya li ad-Dawa wa al-Kital, French: Groupe Salafite pour la Prédication et le Combat, GSPC). The organisation initially operated on the territory of six African countries (Algeria, Mali, Mauritania, Morocco, Niger and Tunisia) and in the following years also in Libya and Chad, and maintained contacts with jihadist groups in other countries (e.g. Nigeria). A Stratfor compilation of ransoms[14] received by AQIM for abductees (mainly foreign nationals) between 2008 and 2012 shows that AQIM's budget was enriched by almost USD 83 million.

Drug trafficking and smuggling

Another source of funding for the terrorist activities of AQIM and other existing organisations in West and North African countries, including the Defenders of the Faith (Arabic: Ansar ad-Din), the Movement for Unity and Jihad in West Africa (Arabic: Al-Jama'at at-Tawhid wa al-Jihad fi Ghabi Ifrakija) known as MUJAO (Mouvement pour l'Unicité et le Jihad en Afrique de l'Ouest) or Boko Haram is trafficking drugs from South America

[14] *Mali: Al Qaeda in the Islamic Maghreb's Ransom Revenue*, Stratfor, 15 X 2012, https://worldview.stratfor.com/article/mali-al-qaeda-islamic-maghrebs-ransom-revenue [accessed: 3 II 2014].

and smuggling them into Europe[15]. According to Algerian data from 2012, the value of cocaine smuggled through North Africa to Europe was EUR 1.6 billion, of which the armed groups were to receive EUR 310 million for their services (protection).

The Taliban have made the production and trafficking of drugs (mainly opium) their primary source of income[16], and this was already the case after the formal overthrow of their rule in Afghanistan. According to the US Special Inspector General for Afghanistan Reconstruction (SIGAR), illicit poppy cultivation and drug production accounts for nearly 60 per cent of the Taliban's annual revenue. According to the UN, the Taliban are able to reap profits of USD 100-400 million each year from the drug sector[17].

ISIL/ISIS/IS Finances

The Islamic State in Iraq and the Levant group, which has existed under this name since April 2013, is also known by the acronym ISIS (Islamic State of Iraq and Syria). The second 'S' in the acronym stands for 'Al-Sham', which can be translated as 'Syria' or even just Damascus, but in the context of the global jihad it referred to the entire Levant, considered at the time to be the Syrian part of Al-Qa'ida. It is understood that the grouping - whose origins were the Group of Unity of God and Jihad (Jama'at at-Tauhid wa-al-Jihad) regarded as an offshoot of Al-Qa'ida, formerly active in Iraq under

[15] See in more detail: E. Basar, *Drug Trafficking In Africa*, Civil-Military Fusion Centre Presents, December 2012, https://www.cimicweb.org/cmo/medbasin/Holder/Documents/r024%20CFC%20Monthly%20Thematic%20Report%20(07-DEC-12).pdf [accessed: 3 II 2014]; C. Freeman, *Revealed: how Saharan caravans of cocaine help to fund al-Qaeda in terrorists' North African domain*, The Telegraph, 26 I 2013, http://www.telegraph.co.uk/news/worldnews/africaandindianocean/mali/9829099/Revealed-how-Saharan-caravans-of-cocaine-help-to-fund-al-Qaeda-in-terrorists-North-African-domain.html [accessed: 2 IV 2014]; R.O. Idoumou, *Terrorists, traffickers forge union in African desert*, Magharebia, 24 II 2012, http://magharebia.com/en_GB/articles/awi/reportage/2012/02/24/reportage-01 [accessed: 3 II 2014].

[16] B. Chellaney, *Taliban turning Afghanistan into narco-terrorist state*, The Japan Times, 24 XI 2021, https://www.japantimes.co.jp/opinion/2021/11/24/commentary/world-commentary/taliban-narco-terrorism/ [accessed: 16 I 2022].

[17] *Afganistan jest największym na świecie producentem służącego do wytwarzania narkotyków maku* (Eng. Afghanistan is the world's largest producer of the drug poppy), Dziennik Gazeta Prawna, 25 VIII 2021, https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8231469,afganistan-producent-mak-narkotyki.html [accessed: 12 VI 2022].

Abu Musab az-Zarkawi and transformed into the Islamic State in Iraq after his death in 2006 - benefited from Al-Qa'ida funding[18].

The then leader of ISIS, Abu Bakr al-Baghdadi (a.k.a. Abu Dua), intended to unite all Syrian jihadist groups, which he partially succeeded in doing, as he gathered many small units under his command. Later, when referring to ISIS, the phrase 'So-called Islamic State' or 'Daesh', sometimes in a polonised version 'Da'isz', began to be used in public discourse. Both names were treated as pejorative terms in order to discredit the opponent. In 2013, according to US intelligence estimates, ISIS numbered around 5,000 fighters, mostly foreign, causing frequent clashes with other rebel branches (including Ahrar al-Sham, Ahfad al-Rasoul and Liwa Asifat al-Shamal) due to ISIS's attempt to dominate them. In June 2014, following al-Baghdadi's announcement of the renewal of the caliphate, the grouping changed its name to Islamic State (Arabic: ad-Dawlah al-Islāmiyah, IS). During this time, it has occupied increasing territory in Syria and Iraq. According to estimates by the US National Counterterrorism Center, NCTC, in autumn 2014 The Islamic State controlled most of the Tigris and Euphrates basin with an area of approximately 210,000 square kilometres, roughly the size of England[19]. As the territory over which the group ruled expanded, so did the organisation's revenues.

According to Western publicists, the Islamic State's income came from a number of sources. According to unofficial estimates, since the summer of 2014, the organisation's war budget was said to have grown from USD 800 million to USD 2 billion in one year, with one billion coming from Syrian and Iraqi oil, 430 million from robbing banks in Mosul and the provincial councils, 100 million from printing counterfeit money and 40 million from trading antiquities from Iraqi museums. British journalist Benjamin Hall writes about similar amounts in his book on ISIS: *The jihadists* (...) *have amassed a huge amount of money (at the end of 2014, their assets were valued at one billion three hundred million to two billion dollars*[20].

[18] From: *Encyklopedia PWN* (Eng. PWN Encyclopedia), https://encyklopedia.pwn.pl/haslo/Panstwo-Islamskie;5567242.html.

[19] See *What is 'Islamic State'?,* 2 XII 2015, BBC, http://www.bbc.com/news/world-middle-east-29052144 [accessed: 20 IX 2016].

[20] B. Hall, *ISIS. Państwo Islamskie* (Eng. ISIS. Islamic State), translated by: P. Wolak, Warszawa 2015, p. 190.

In contrast, the authors of the report Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)[21], published in February 2015 by the Financial Action Task Force (FATF), identified five main sources of funding for the Islamic State (both then and now they remain the same). Depending on the size of the share of the budget that this quasi-state had at the time, these were:

1) unlawful revenue derived from territories occupied by the Islamic State, obtained from bank looting, extortion, control of oil fields and refineries, theft of economic assets and unlawful taxation of goods and cash in transit through these territories (the tax was 2 per cent of the value of these goods or cash),
2) abductions for ransom (IS was able to obtain sums in the order of USD 30-50 million per year),
3) donations received from non-profit organisations,
4) material support received on an FTF (friend to friend) basis,
5) funds raised through modern communication networks (social networks)[22].

Such information on IS funding sources can be found in the official FATF document. Even more can be learned from Ana Swanson's article How the Islamic State makes its money featured in the Washington Post[23], and although it is "only" a news publication, it was published in one of the most prestigious daily newspapers. In addition to the sources mentioned, the article also mentions:

– the trafficking of antiquities located in IS-occupied areas, often from private collections. Some of them were destroyed, as shown in films broadcast mainly online and on various private and state television stations. However, it can be assumed that this constituted a kind of 'smokescreen' to hide the sale of antiquities and the treatment of them as an important source of income (at least during the first period of expansion). This is evidenced by the information provided to congressmen by Matthew Levitt of the Washington

[21] *Financing of the terrorist organisation Islamic State in Iraq and the Levant*, FATF, February 2015, www.fatf-gafi.org/topics/methodsandtrends/documents/financing-of-terrorist-organisation-isil.html [accessed: 1 VI 2022].

[22] Ibid., p. 12.

[23] A. Swanson, *How the Islamic State makes its money*, The Washington Post, 18 XI 2015, https://www.washingtonpost.com/news/wonk/wp/2015/11/18/how-isis-makes-its-money [accessed: 18 X 2016].

Institute for Near East Policy that IS gained over USD 100 million through these transactions in 2014. After the oil trade, antiquities were the second largest source of funding for the organisation;
- agricultural income obtained by IS to raise funds through legitimate means. They used one of the pillars of Islam, namely zakat (almsgiving), which is an obligation for every Muslim (it amounts to 10 per cent of income). Since around 40 per cent of all Iraqi grain is grown in areas under IS control, the proceeds amounted to around USD 200 million;
- the sale of material goods of Americans (mainly cars, but also home furnishings) seized in occupied areas;
- the trading or renting of properties (houses, flats) formerly belonging to representatives of the Iraqi establishment, people who fled IS-occupied areas or were killed;
- fees paid by foreigners who, in order to join the ranks of IS fighters, are forced to pay a kind of "buy-in";
- income from the sale of phosphates, cement, sulphur and, above all, their processed forms (acids). Despite the undervalued prices, IS has been able to generate around USD 300 million in annual profits from their sale;
- trafficking in human beings, primarily abducted women and girls (Yazidi and Turkmen Shia), sold as sex slaves.

From its inception, IS's authorities decided to become independent of the financial assistance it received from outside, although of course it did not despise it either. However, taking into account the experience of Al-Qa'ida, which benefited from such illegal subsidies, a quasi-government with ministries, including the Ministry of Oil, was created in this quasi-state. It was headed until his death by the Tunisian Abu Sayyaf (real name according to the Pentagon: Fathi Ben Awn Ben Jildi Murad al-Tunisi)[24], who was killed in May 2015 as a result of a US special forces operation. The Shura[25] decided that IS could become independent with the proceeds

[24] G. Chazan, S. Jones, E. Solomon, *Isis Inc: how oil fuels the jihadi terrorists*, Financial Times, 15 X 2015, https://www.ft.com/content/b8234932-719b-11e5-ad6d-f4ed76f0900a [accessed: 1 VI 2022].

[25] Shūra (Arabic: consultation) - a consultative council set up by Abu Bakr al-Baghdadi to lend credibility to the existence of the Islamic State. In early Islamic history it used to be a council of electors formed by the second caliph (ruler of the Muslim community), Umar I (634-644), to choose his successor. Subsequently, in Muslim states, the term shūrā

primarily from the oil trade and steps were initiated to implement these plans. Local specialists already working in the occupied oil fields were recruited (including Ajil and Allas in the north-eastern province of Iraq, Kirkuk or al-Jibsa in the Syrian province of Hassakeh and others located in the province of Deir ez-Zor), engineers and technicians from Saudi Arabia or Europe were brought in, offering them high salaries and security guarantees for them and their families. The smooth and uninterrupted extraction of oil and production of diesel was to be supervised by Amniyat, the ISIS secret police. It was tasked with patrolling the oil-producing areas, checking all transports and punishing the supervisors (often in a very brutal manner) if any irregularities occurred[26].

Thanks to the interrogation of Abu Hajjar, who was captured by US troops in June 2014 near Mosul, information was gained about the whereabouts of the then head of the ISIS Military Council Abu Abdulrahman al-Bilawi (which led to his liquidation), and in the process, more importantly, information was gained about the sources of IS funding. It emerged that as early as 2014, up to 40,000 barrels of oil per day were being produced from 11 IS-controlled oilfields in Iraq and Syria, which were being smuggled and sold illegally to Iran, Kurdistan, Turkey and Syria. The sale was generating revenue of around USD 1.2 million per day. The procedure was profitable even though the oil was sold at dumped prices, often 75 per cent lower than those prevailing on world markets[27].

What was unclear was the attitude of Turkey. It emerged that the sale of oil by IS to Turkey (which was at one point made public) was not only carried out with the tacit approval of the Turkish government, but that President Erdoğan's son Bilal was directly involved in the trade. According to media reports, he was a co-owner of the maritime transport corporation

has come to mean, depending on the state council or advisors to the sovereign (as in Saudi Arabia), the parliament (as in Pakistan) and the court with jurisdiction to settle the claims of citizens and the public against the government (as in Afghanistan). The word shūra is the title of the 42nd Sura of the Qur'an, in which believers are encouraged to conduct their affairs 'through mutual consultation'. From: *Encyclopaedia Britannica,* https://www.britannica.com/topic/shura [accessed: 1 VI 2022].

[26] G. Chazan, S. Jones, E. Solomon, *Isis Inc: how oil fuels…*

[27] Ch. Dalby, *Who Is Buying The Islamic State's Illegal Oil?*, 30 IX 2014, Oil Price, http://oilprice.com/Energy/Crude-Oil/Who-Is-Buying-The-Islamic-States-Illegal-Oil.html [accessed: 1 VI 2022].

BMZ Group Denizcilik, whose tankers distributed the illegally purchased oil to the targeted recipients[28].

State-sponsored terrorism

The methods of financing terrorist activities mentioned in this article very often imply the commission of criminal offences. However, since the 1970s, the term 'state-sponsored terrorism' has entered the scientific, or should we say political, language. This term was introduced in the USA to designate states that are considered hostile by the Washington administration. They can be held responsible for the existence (activities) of terrorist organisations and for repeatedly supporting acts of international terrorism. The annual reports of the US State Department list countries accused of sponsoring terrorism, with the list changing over 40 years. Currently it lists four countries[29]:

1) Syria - since 29 December 1979,
2) Iran - since 16 January 1984,
3) Democratic People's Republic of Korea - since 20 November 2017,
4) Cuba - since 12 January 2021.

Libya, Iraq, South Yemen and Sudan were also previously included on the list.

In the 1970s, the claim that the USSR and socialist countries supported various left-wing terrorist organisations was widely circulated in the West. There is no doubt that students at the Patrice Lumumba University of the Friendship of Nations in Moscow were individuals who later became terrorists, and among the most recognisable was Ilich Ramírez Sánchez, known as 'Carlos' or 'The Jackal'. Making such accusations can be compared to charging France with the crimes of the Khmer Rouge in Cambodia, because their leader Pol Pot studied at the Sorbonne. What is certain is that members of the RAF took refuge on East German territory after their 'retirement', as was proven after German reunification. However, this is

[28] Information on this has appeared in many media, see *Meet The Man Who Funds ISIS: Bilal Erdogan, The Son Of Turkey's President*, Mint Press News, 30 XI 2015, http://www.mintpressnews.com/211624-2/211624 [accessed: 15 X 2016].

[29] *State sponsors of terrorism*, U.S. Department of State, https://www.state.gov/state-sponsors-of-terrorism/ [accessed: 13 V 2022].

not tantamount to saying that the GDR had organised the terrorist activities of left-wing groups on German territory since 1968.

The methods of financing terrorist organisations and the attacks they carried out, presented in the article, are only selected examples. The author hopes that it will become the beginning of extensive research on this issue.

Bibliography

Antkol N., Nudell M., *No One Neutral. Political Hostage-Taking In the Modern World*, Ohio 1990.

Dietl W., Hirschmann K., Tophoven R., *Terrorism*, Warszawa 2009.

Encyklopedia terroryzmu (Eng. Encyclopedia of terrorism), B. Zasieczna (ed.), Warszawa 2004.

Hall B., *ISIS. Państwo Islamskie* (Eng. ISIS. Islamic State), translated by: P. Wolak, Warszawa 2015.

Karolczak K., *Lewicowy terroryzm w Ameryce Łacińskiej* (Eng. Left-wing terrorism in Latin America), "Warsztat" 1984, no. 1.

Karolczak K., *Terroryzm i polityka. Lata 2009–2013* (Eng. Terrorism and Politics. 2009-2013), Warszawa 2014.

Internet sources

Afganistan jest największym na świecie producentem służącego do wytwarzania narkotyków maku (Eng. Afghanistan is the world's largest producer of the drug poppy), Dziennik Gazeta Prawna, 25 VIII 2021 , https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8231469,afganistan-producent-mak-narkotyki.html [accessed: 12 VI 2022].

Basar E., *„Drug Trafficking In Africa", Civil-Military Fusion Centre Presents*, December 2012, https://www.cimicweb.org/cmo/medbasin/Holder/Documents/r024%20CFC%20Monthly%20Thematic%20Report%20(07-DEC-12).pdf [accessed: 3 II 2014].

Chazan G., Jones S., Solomon E., *Isis Inc: how oil fuels the jihadi terrorists*, Financial Times, 15 X 2015, https://www.ft.com/content/b8234932-719b-11e5-ad6d-f4ed76f0900a [accessed: 1 VI 2022].

Chellaney B., Taliban turning Afghanistan into narco-terrorist state, The Japan Times, 24 XI 2021, https://www.japantimes.co.jp/opinion/2021/11/24/commentary/world-commentary/taliban-narco-terrorism/ [accessed: 16 I 2022].

Dalby Ch., *Who Is Buying The Islamic State's Illegal Oil?*, Oil Price, 30 IX 2014, http://oilprice.com/Energy/Crude-Oil/Who-Is-Buying-The-Islamic-States-Illegal-Oil.html [accessed: 1 VI 2022].

Encyclopedia Britannica, https://www.britannica.com/topic/shura [accessed: 1 VI 2022].

Financing of the terrorist organisation Islamic State in Iraq and the Levant, FATF, February 2015, www.fatf-gafi.org/topics/methodsandtrends/documents/financing-of-terrorist-organisation-isil.html [accessed: 1 VI 2022].

Freeman C., *Revealed: how Saharan caravans of cocaine help to fund al-Qaeda in terrorists' North African domain*, The Telegraph, 26 I 2013, http://www.telegraph.co.uk/news/worldnews/africaandindianocean/mali/9829099/Revealed-how-Saharan-caravans-of-cocaine-help-to-fund-al-Qaeda-in-terrorists-North-African-domain.html [accessed: 2 IV 2014].

Funding of terrorist groups compared, Money Jihad, 21 I 2013, http://moneyjihad.wordpress.com/2013/01/21/funding-of-terrorist-groups-compared/ [accessed: 3 V 2022].

Idoumou R.O., *Terrorists, traffickers forge union in African desert*, Magharebia, 24 II 2012, http://magharebia.com/en_GB/articles/awi/reportage/2012/02/24/reportage-01 [accessed: 3 II 2014].

Los actos terroritas del E.R.P. y Montoneros, Buen Día Noticia, 31 VII 2018, https://buendianoticia.com/nota/10960/los-actos-terroristas-del-erp-y-montoneros [accessed: January–May 2022].

Mali: Al Qaeda in the Islamic Maghreb's Ransom Revenue, Stratfor, 15 X 2012, http://www.stratfor.com/analysis/mali-al-qaeda-islamic-maghrebs-ransom-revenue // https://worldview.stratfor.com/article/mali-al-qaeda-islamic-maghrebs-ransom-revenue [accessed: 3 II 2014].

Meet the Man Who Funds ISIS: Bilal Erdogan, the Son of Turkey's President, Mint Press News, 30 XI 2015, http://www.mintpressnews.com/211624-2/211624 [accessed: 15 X 2016].

State sponsors of terrorism, U.S. Department of State, https://www.state.gov/state-sponsors-of-terrorism/ [accessed: 13 V 2022].

Swanson A., *How the Islamic State makes its money*, The Washington Post, 18 XI 2015, https://www.washingtonpost.com/news/wonk/wp/2015/11/18/how-isis-makes-its-money [accessed: 18 X 2016].

Terrorism financing in Australia 2014, AUSTRAC website, https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/terrorism-financing-australia-2014 [accessed: 3 V 2022].

The World's 10 Richest Terrorist Organizations, Forbes, 12 XII 2014, http://www.forbes.com/sites/forbesinternational/2014/12/12/the-worlds-10-richest-terrorist-organizations/#336a6802ffae [accessed: 22 V 2022].

What is 'Islamic State'?, BBC, 2 XII 2015, http://www.bbc.com/news/world-middle-east-29052144 [accessed: 20 IX 2016].

DOI: 10.4467/27204383TER.22.029.16349

ORCID: 0000-0003-2763-9325

DAMIAN SZLACHTER

Terrorism in Poland and trends in its development. Survey results (summary report)

On 26 April 2022, the first survey on the perception of the phenomenon of terrorism and the anticipated, most likely trends in the development of terrorist threats in our country was conducted among the participants of the inaugural meeting of the new scientific periodical "Terrorism - studies, analyses, prevention" published by the Internal Security Agency.

The respondents were representatives of the academic and analytical community involved in terrorism studies and representatives of services and institutions belonging to the anti-terrorist community of Poland. The survey was anonymous, with 94 respondents, including 71 representatives of the state administration, 21 representatives of the academic community and 2 analysts cooperating with research centres.

The paper questionnaire consisted of 11 questions - 5 semiopen questions (questions: 1, 2, 3, 5, 6), 2 closed questions (questions: 7, 8) and 4 multiple-choice questions (questions: 4, 9, 10, 11). In the multiplechoice questions, respondents were asked to rank their answers according to a 4-point or 5-point scale given in the instructions to the question each time.

The results obtained were statistically analysed and then presented as figures. The numbers in the figures have been rounded to two digits after the decimal point.

Key findings from the results of the survey:

- 62,76% of respondents consider ISIS (DAESH) as the organisation posing the greatest threat to the security of EU countries, Al-Qa'ida came second with 15,96% of the votes, the Russian special services were mentioned in third place with 11,70% of the votes.
- 61,70% of respondents consider ISIS (DAESH) as the organisation posing the greatest threat to the security of eastern EU countries, the Russian special services came second with 17,02% of the votes, Al-Qa'ida was mentioned in third place with 9,57% of the votes.
- 53,19% of respondents consider ISIS (DAESH) to be the organisation posing the greatest threat to the security of the Republic of Poland, the special services of the Russian Federation ranked second with a score of 17,02% of votes, Atomwaffen was mentioned in third place with a score of 14,89% of votes.
- Among the types of facilities that remain of interest to terrorists planning their activities within the EU, respondents listed the following locations in the top three:
  - critical infrastructure facilities (39,36% of votes),
  - public open spaces (32,98% of the votes),
  - tourist infrastructure and sports facilities (14,89% of the votes).
- Among the technologies currently posing the greatest challenge to the services, authorities and institutions tasked with ensuring the ICT security of services, devices or facilities that could be the target of terrorist attacks in cyberspace, respondents listed in the top three:
  - highly advanced automation technology for control processes (35,11% of votes),
  - artificial intelligence (26,60% of votes),
  - cloud-based data storage (22,34% of votes).
- Among the tools, devices or technologies that are currently the greatest challenge for services, authorities and institutions to ensure the physical security of people and objects that could be targeted by terrorist attacks, respondents listed in the top three:
  - unmanned aerial vehicles (69,15% of votes),
  - improvised explosive devices (10,64% of the votes),
  - 3D printing (8,51% of the votes).
- 47,87% of respondents thought that in a three-year perspective Poland would be an attractive country for international terrorists

planning their activities in the EU, with 19% of respondents holding the opposite view.
- 90,43% of respondents considered that terrorist activity carried out as part of hybrid activities undertaken on the territory of Poland by a foreign state should be expected in the three-year perspective.
- Among the facilities located in the Republic of Poland whose level of threat of a terrorist attack in a three-year horizon is rated as the highest by respondents, the top three were:
  – critical energy infrastructure facilities (36,17% of votes),
  – public transport system (34,04% of votes),
  – military bases used as part of NATO's eastern flank (19,15% of votes).
- Among the terrorism research topics that should be given the highest priority, respondents listed the following areas in the top three:
  – the process of radicalisation leading to terrorism (30,85% of votes),
  – detection and blocking of terrorist propaganda (23,40% of votes),
  – countering the financing of terrorism (19,15% of votes).
- Among initiatives that build anti-terrorism cooperation between academia and government institutions and services, respondents listed the following proposals in the top three:
  – joint research and development projects (45,74% of votes),
  – creation of formalised forums for the exchange of knowledge and experience (39,36% of votes),
  – publication of joint guides on security education (2,77% of votes).

Statistical elaboration

Breakdown of survey respondents by the community they represent:
- 22% - representativse of the academic community,
- 76% - representatives of state administration,
- 2% - analysts cooperating with a research centre.

Question 1. Which terrorist organisation poses the greatest threat to the security of the countries of the European Union? (choose one answer)

a. Al-Qa'ida,
b. ISIS,
c. Hezbollah,
d. Atomwaffen,
e. Other.

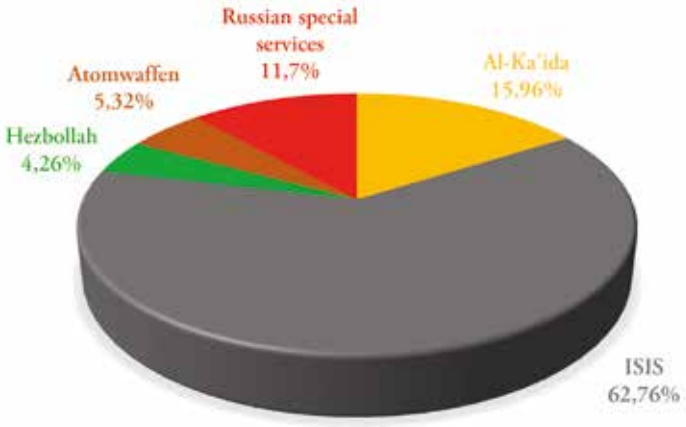

Figure 1. Terrorist organisations posing the greatest threat to the security of EU countries.

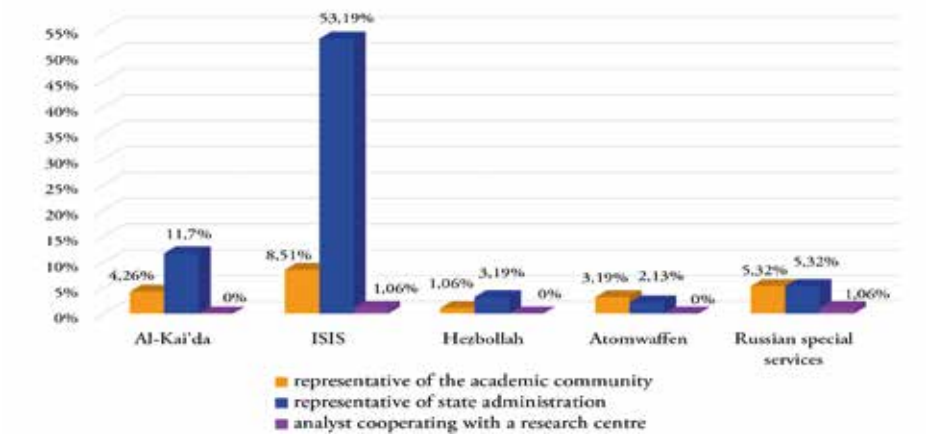

Figure 1a. Terrorist organisations posing the greatest threat to the security of EU countries - distribution of responses according to the community represented by the respondent.

Question 2. Which terrorist organisation poses the greatest security threat to the eastern part of the European Union? (choose one answer)

a. Al-Qa'ida,
b. ISIS,
c. Hezbollah,
d. Atomwaffen,
e. Other.

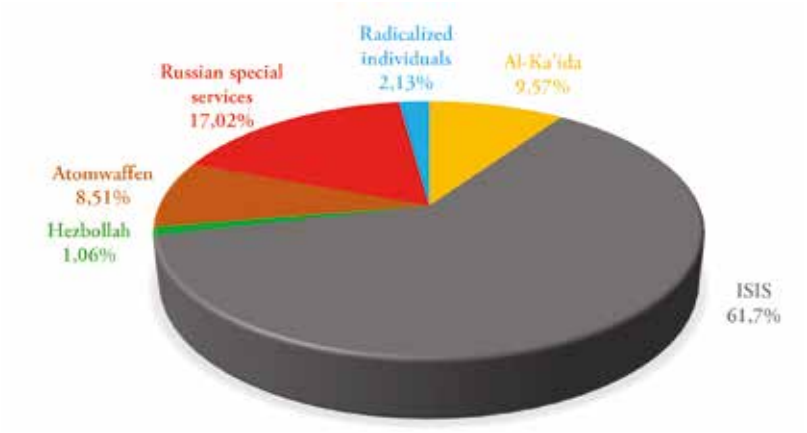

Figure 2. Terrorist organisations posing the greatest security threat to the eastern part of the EU.

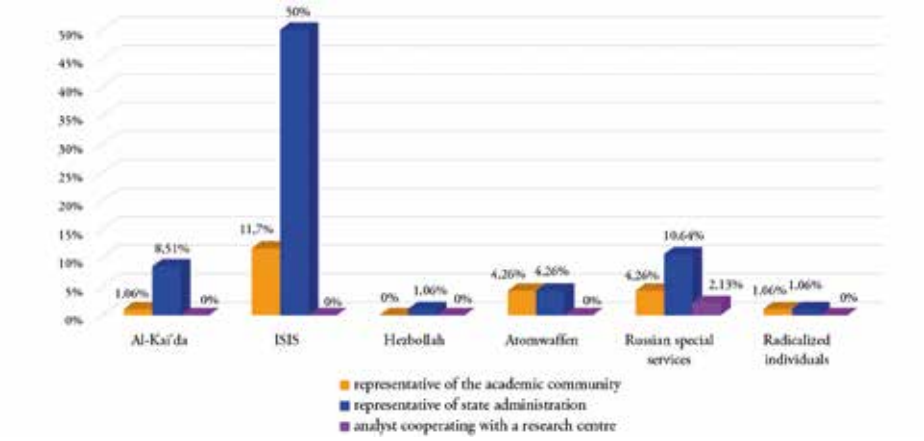

Figure 2a. Terrorist organisations posing the greatest threat to the security of the eastern part of the EU - distribution of answers according to the community represented by the respondent.

Question 3. Which terrorist organisation poses the greatest threat to the security of the Republic of Poland? (choose one answer)

a. Al-Qa'ida,
b. ISIS,
c. Hezbollah,
d. Atomwaffen,
e. Other.

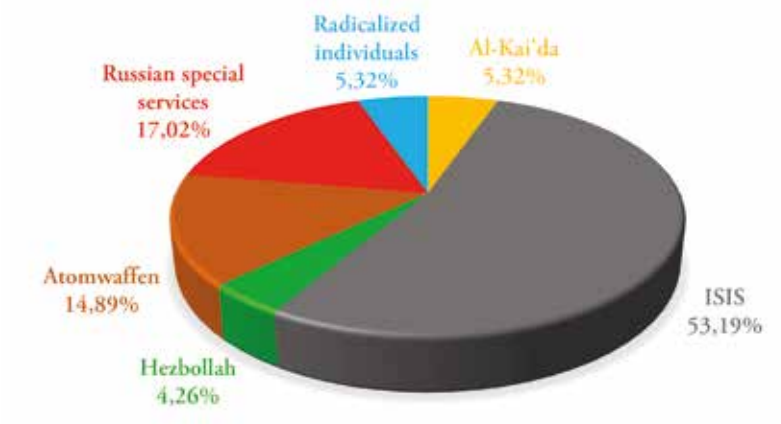

Figure 3. Terrorist organisations posing the greatest threat to Poland's security.

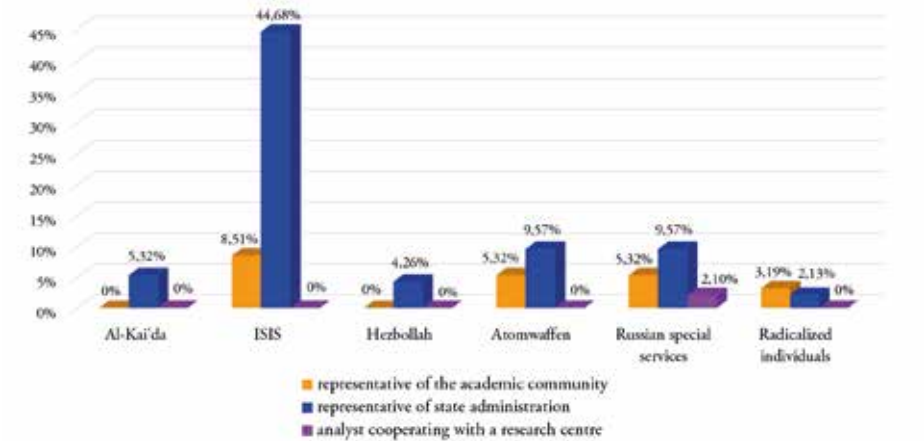

Figure 3a. Terrorist organisations posing the greatest threat to the security of the Republic of Poland - distribution of answers according to the community represented by the respondent.

Question 4. What sites are of interest to terrorists planning their activities within the European Union today? (rank on the right hand side from 1 to 5, with 1 indicating the greatest level of interest)

a. Government office buildings,
b. Critical infrastructure facilities,
c. Public open spaces,
d. Military bases,
e. Tourism infrastructure and sports facilities.

Facilities marked with number 1

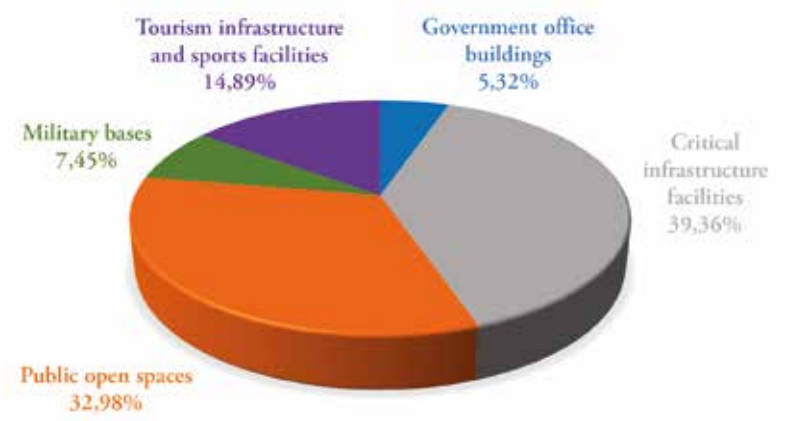

Figure 4. Proportion of each type of site of interest to terrorists planning their activities in the EU, in the group of sites marked with 1 (highest level of interest).

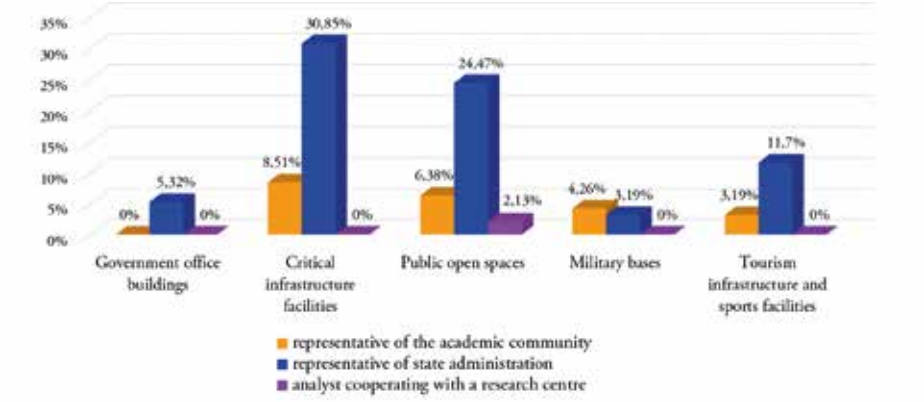

Figure 4a. Proportion of each type of site of interest to terrorists planning their activities in the EU, in the group of sites marked with the number 1 – distribution of answers according to the community represented by the respondent.

Facilities marked with number 2

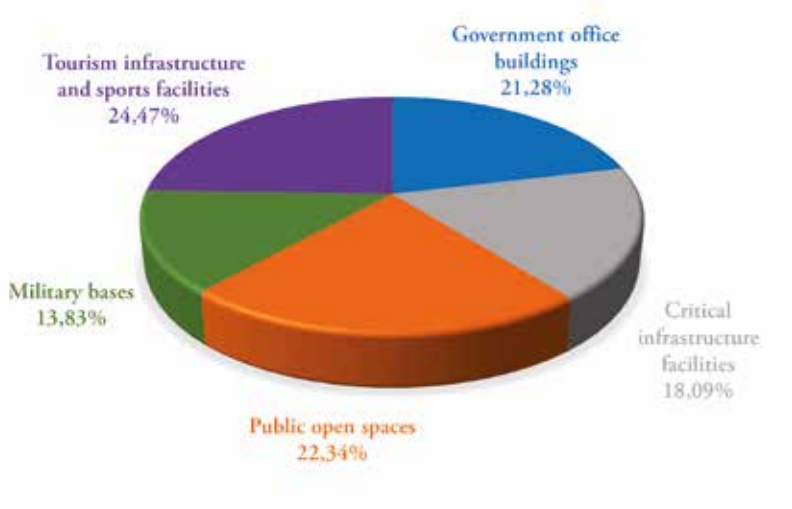

Figure 4b. Proportion of each type of site of interest to terrorists planning their activities in the EU, in the group of sites marked with the number 2.

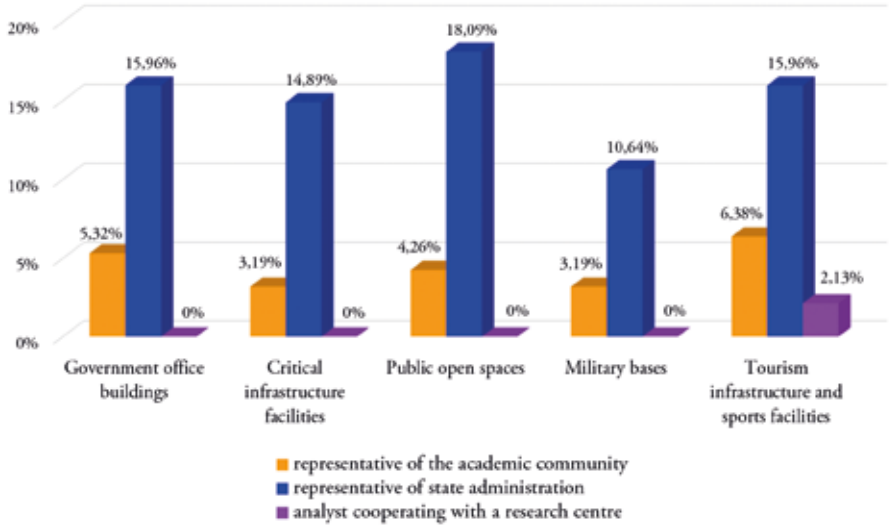

Figure 4c. Proportion of each type of site of interest to terrorists planning their activities in the EU, in the group of sites marked with the number 2 – distribution of answers according to the community represented by the respondent**.**

Facilities marked with number 3

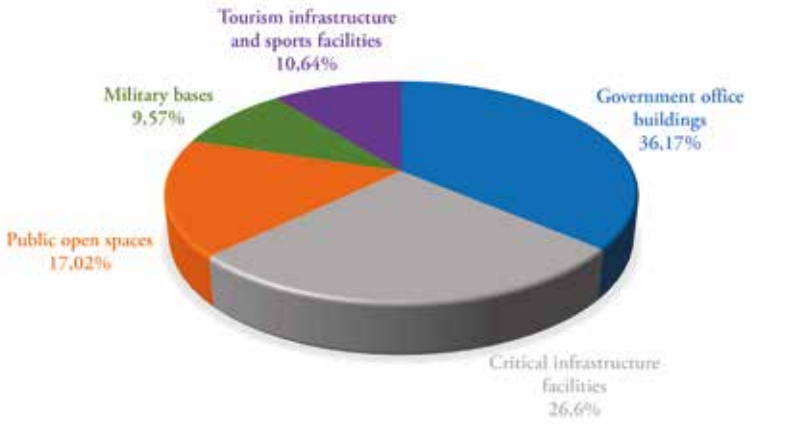

Figure 4d. Proportion of each type of site of interest to terrorists planning their activities in the EU, in the group of sites marked with the number 3.

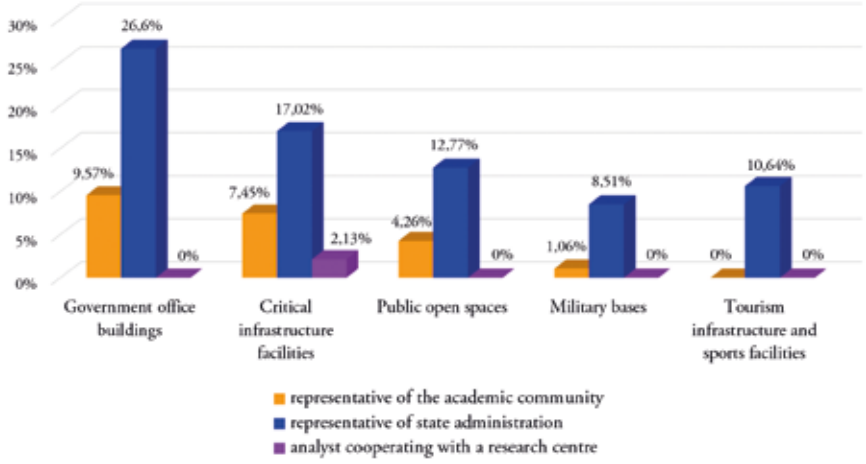

Figure 4e. Proportion of each type of site of interest to terrorists planning their activities in the EU, in the group of sites marked with the number 3 – distribution of answers according to the community represented by the respondent.

Facilities marked with number 4

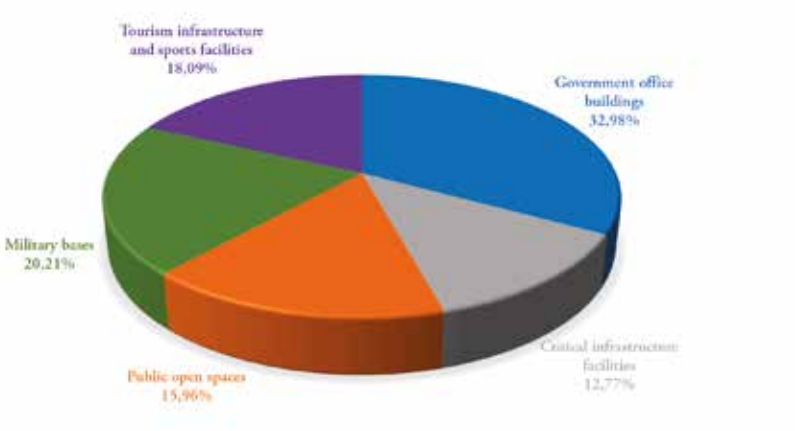

Figure 4f. Proportion of each type of site of interest to terrorists planning their activities in the EU, in the group of sites marked with the number 4.

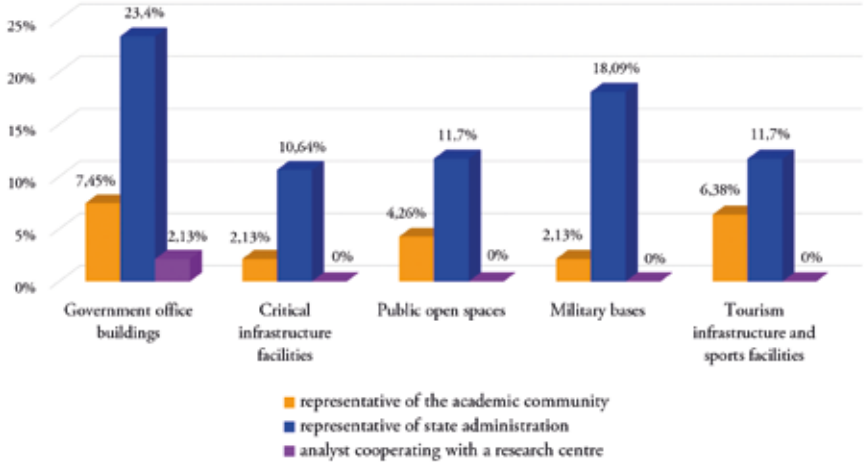

Figure 4g. Proportion of each type of site of interest to terrorists planning their activities in the EU, in the group of sites marked with the number 4 – distribution of answers according to the community represented by the respondent.

Facilities marked with number 5

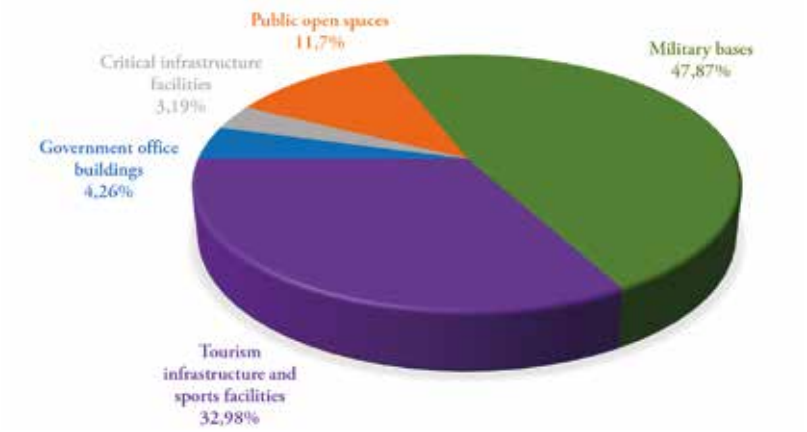

Figure 4h. Proportion of each type of site of interest to terrorists planning their activities in the EU, in the group of sites marked with the number 5.

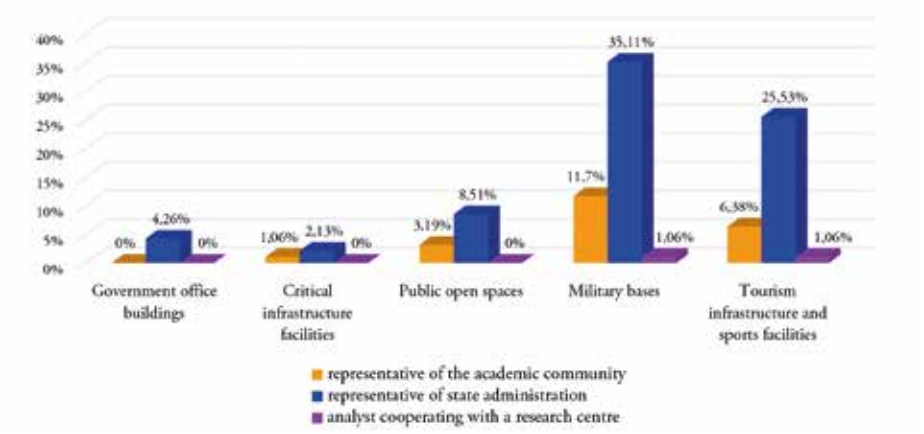

Figure 4i. Proportion of each type of site of interest to terrorists planning their activities in the EU, in the group of sites marked with the number 5 – distribution of answers according to the community represented by the respondent.

Question 5. What technologies are today's biggest challenges for services, authorities and institutions to ensure the ICT security of services, devices or facilities that could be targeted by terrorist attacks in cyberspace? (choose one answer)

a. Artificial intelligence,
b. Cloud-based data storage,
c. Highly advanced automation technology for control processes,
d. Development of 5G data transmission standards,
e. Other.

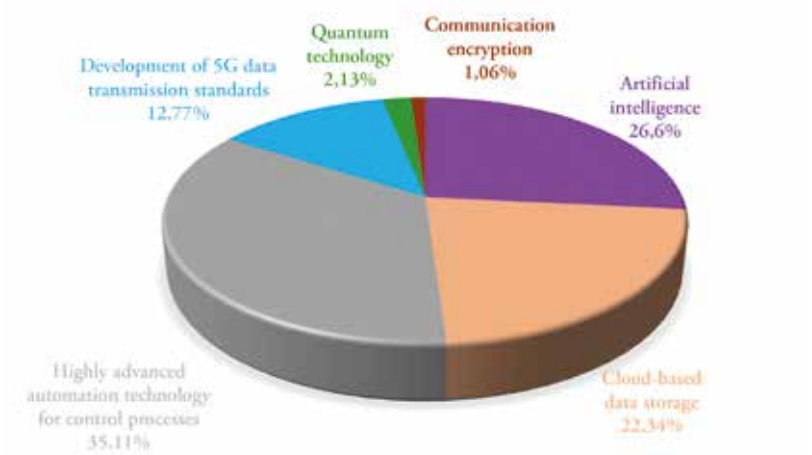

Figure 5. Technologies that pose the greatest challenge today for services, authorities and institutions tasked with ensuring the ICT security of services, devices or facilities that could be targeted by terrorist attacks in cyberspace.

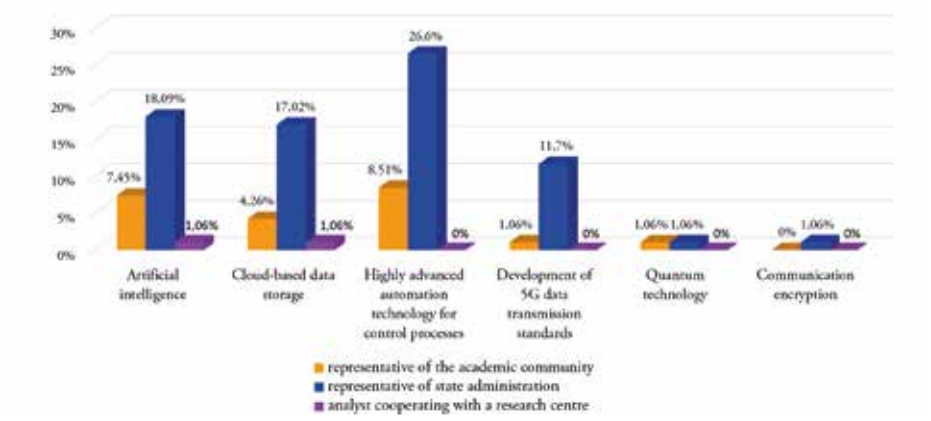

Figure 5a. Technologies that pose the greatest challenge today for services, authorities and institutions tasked with ensuring the ICT security of services, devices or facilities that could be targeted by terrorist attacks in cyberspace – distribution of answers according to the community represented by the respondent.

Question 6. What are the most challenging tools, devices or technologies today for the services, authorities and institutions tasked with ensuring the physical security of persons and facilities that may be targeted by terrorists? (choose one answer)

a. Unmanned aerial vehicles,
b. 3D printing,
c. Vehicles as weapons,
d. Improvised explosive devices,
e. Cold steel weapons made of composites,
f. Other.

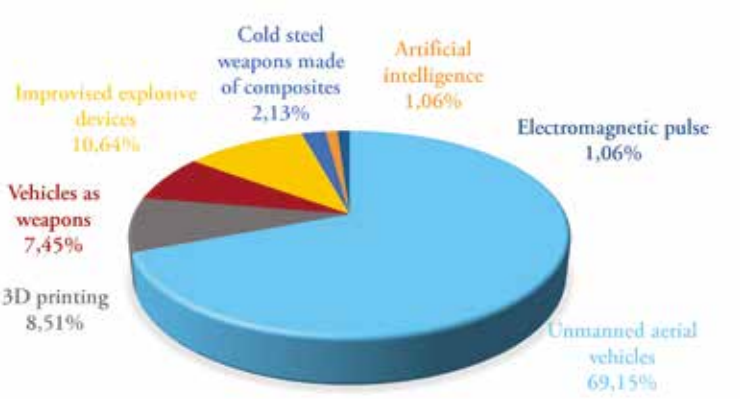

Figure 6. Tools, devices or technologies that pose the greatest challenge today to the services, authorities and institutions tasked with ensuring the physical security of persons and objects that could be the target of terrorist attacks.

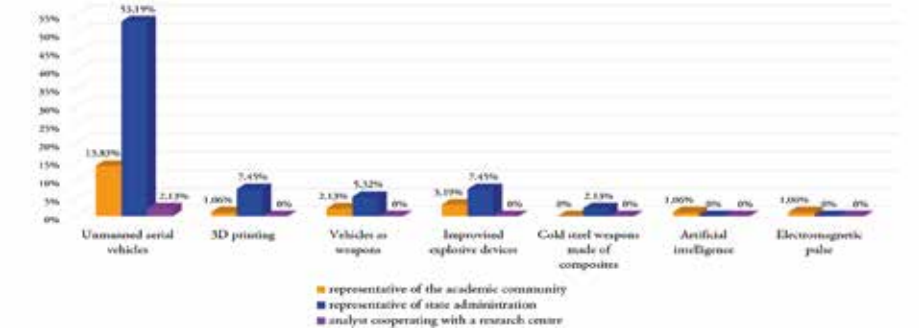

Figure 6a. Tools, devices or technologies that pose the greatest challenge today to the services, authorities and institutions tasked with ensuring the physical security of persons and objects that could be the target of terrorist attacks – distribution of answers according to the community represented by the respondent.

Question 7. In a 3-year perspective, will Poland be an unattractive country for international terrorists? (choose one answer)

a. Yes,
b. No,
c. Difficult to say.

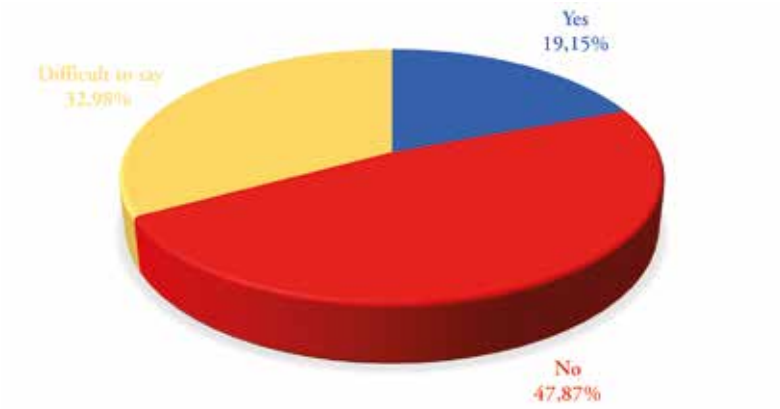

Figure 7. Poland as an unattractive country for international terrorists in the next 3 years.

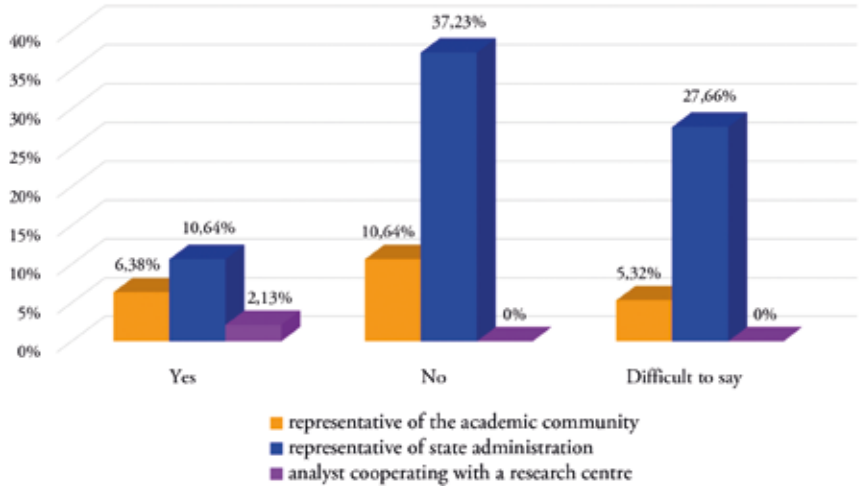

Figure 7a. Poland as an unattractive country for international terrorists in the next 3 years – distribution of answers according to the community represented by the respondent.

Question 8. In a 3-year horizon, should we expect to see the use of terrorist activity as part of hybrid activities undertaken on Polish territory by a foreign state? (choose one answer)

a. Yes,
b. No,
c. Difficult to say.

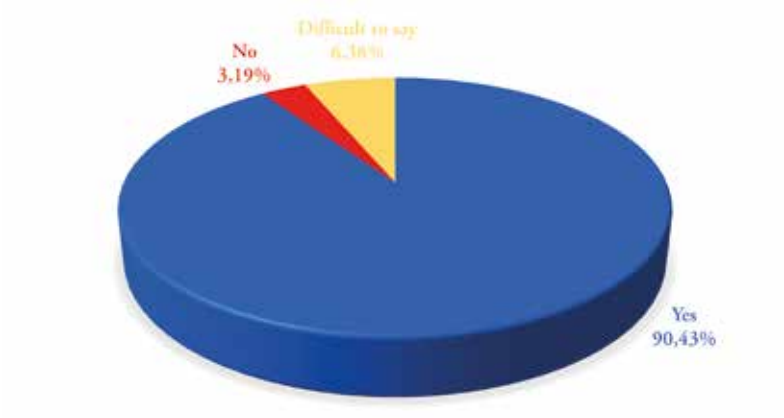

Figure 8. The likelihood of terrorist activity being used as part of hybrid activities undertaken by a foreign state on Polish territory in the next 3 years.

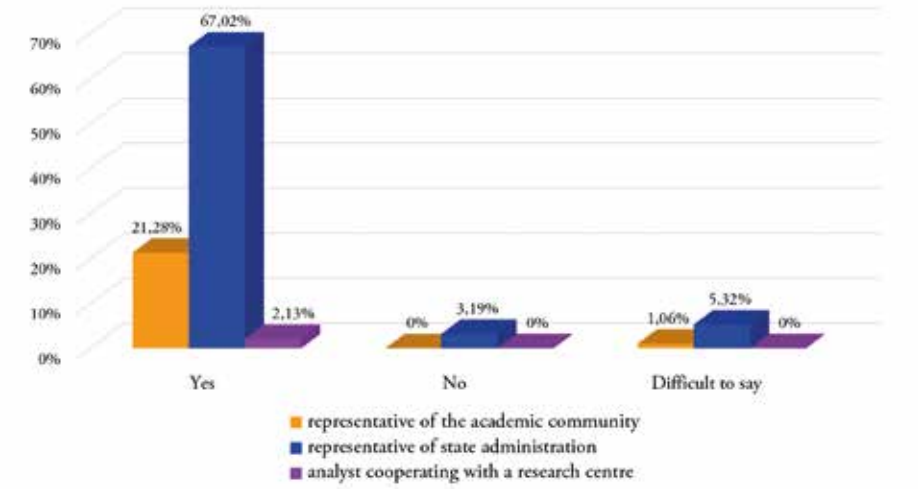

Figure 8a. The likelihood of terrorist activity being used as part of hybrid activities undertaken by a foreign state on Polish territory in the next 3 years – distribution of answers according to the community represented by the respondent.

Question 9. In a 3-year perspective, how will the level of threat of a terrorist attack on the indicated sites in Poland evolve? (rank on the right hand side from 1 to 5, with 1 indicating the greatest level of threat)

a. Military bases used as part of NATO's eastern flank,
b. Critical energy infrastructure facilities,
c. Public transport system,
d. Seats of constitutional state bodies,
e. Tourism infrastructure and sports facilities.

Facilities marked with number 1

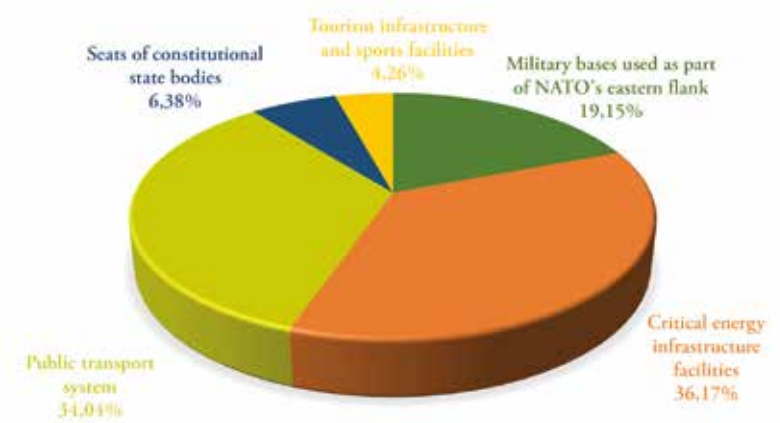

Figure 9. Share of each type of facility in the Republic of Poland at risk of a terrorist attack in the next 3 years in the group of facilities marked with the number 1 (highest level of threat).

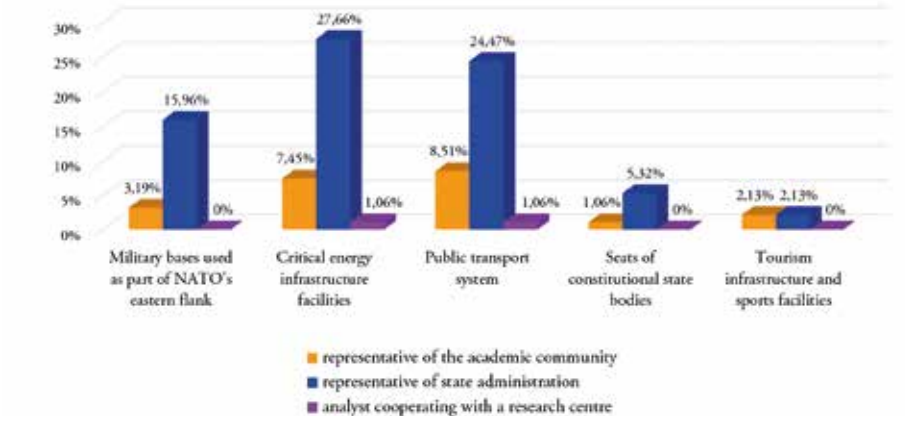

Figure 9a. Share of each type of facility in the Republic of Poland at risk of a terrorist attack in the next 3 years in the group of facilities marked with the number 1 (highest level of threat) – distribution of answers according to the community represented by the respondent.

Facilities marked with number 2

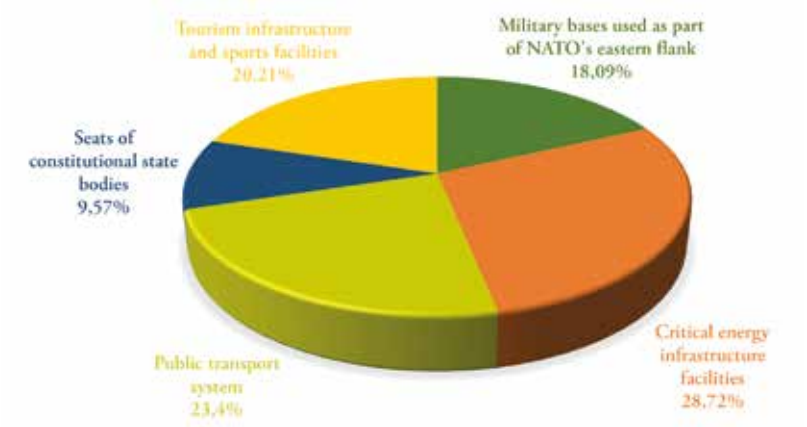

Figure 9b. Share of each type of facility in the Republic of Poland at risk of a terrorist attack in the next 3 years in the group of facilities marked with the number 2.

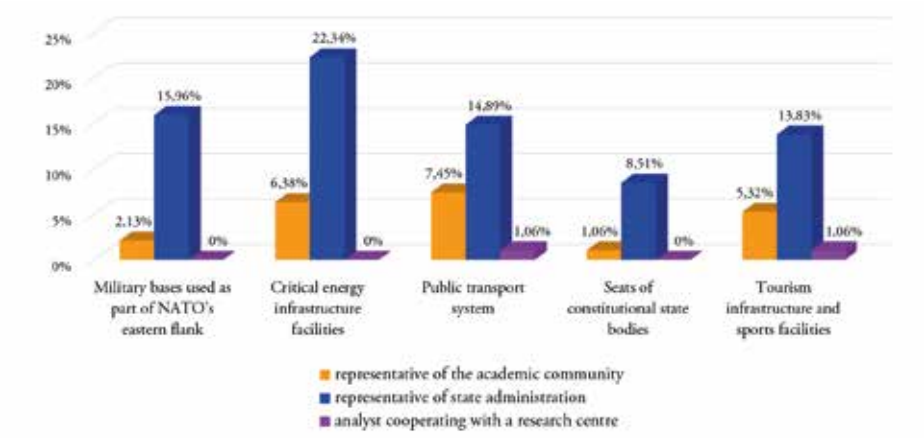

Figure 9c. Share of each type of facility in the Republic of Poland at risk of a terrorist attack in the next 3 years in the group of facilities marked with the number 2 – distribution of answers according to the community represented by the respondent.

Facilities marked with number 3

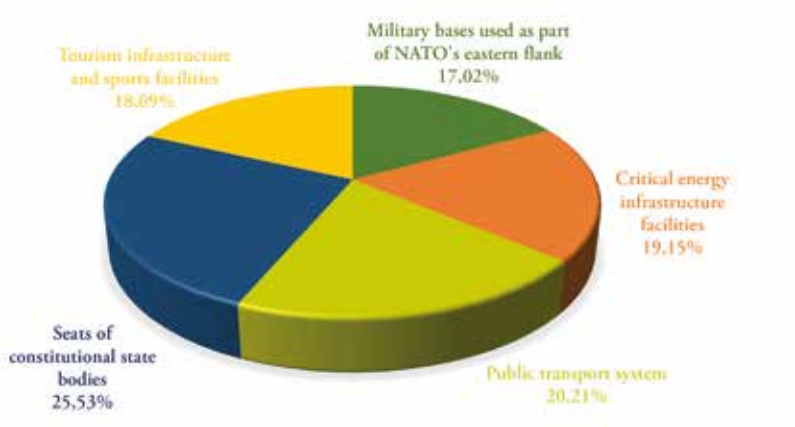

Figure 9d. Share of each type of facility in the Republic of Poland at risk of a terrorist attack in the next 3 years in the group of facilities marked with the number 3.

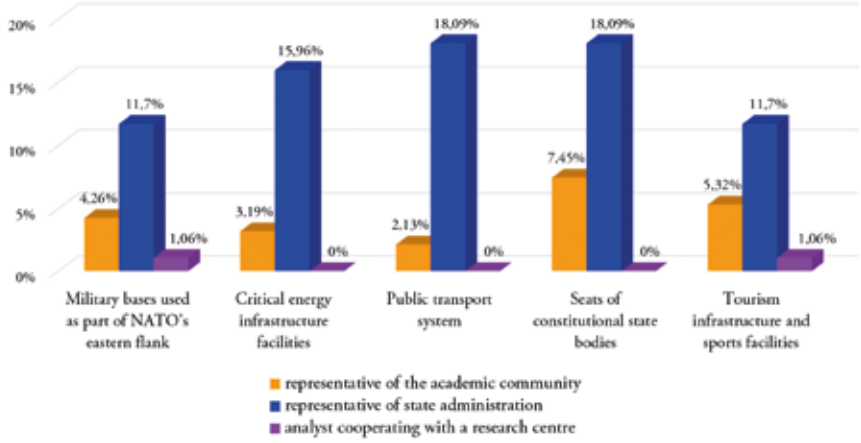

Figure 9e. Share of each type of facility in the Republic of Poland at risk of a terrorist attack in the next 3 years in the group of facilities marked with the number 3 – distribution of answers according to the community represented by the respondent.

Facilities marked with number 4

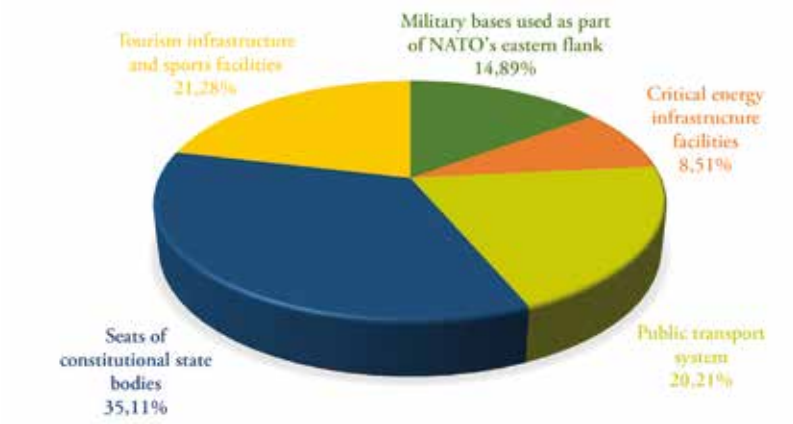

Figure 9f. Share of each type of facility in the Republic of Poland at risk of a terrorist attack in the next 3 years in the group of facilities marked with the number 4.

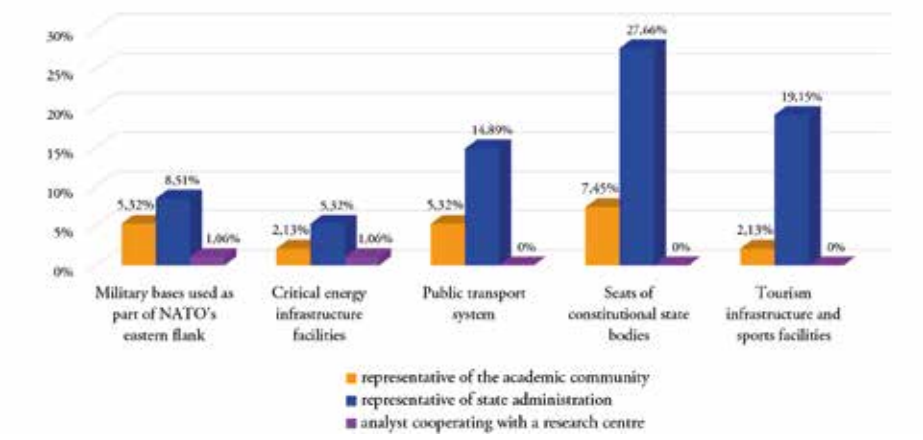

Figure 9g. Share of each type of facility in the Republic of Poland at risk of a terrorist attack in the next 3 years in the group of facilities marked with the number 4 – distribution of answers according to the community represented by the respondent.

Facilities marked with number 5

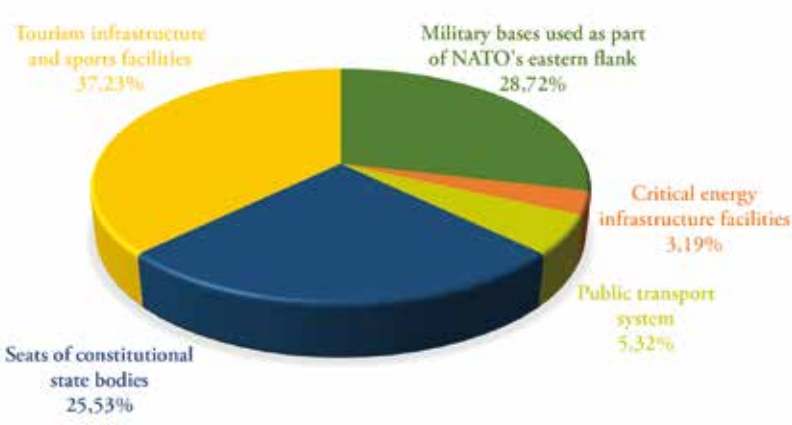

Figure 9h. Share of each type of facility in the Republic of Poland at risk of a terrorist attack in the next 3 years in the group of facilities marked with the number 5.

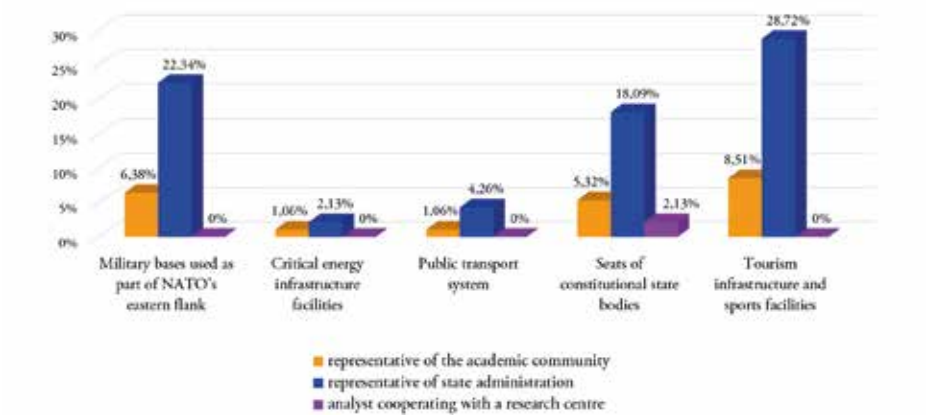

Figure 9i. Share of each type of facility in the Republic of Poland at risk of a terrorist attack in the next 3 years in the group of facilities marked with the number 5 – distribution of answers according to the community represented by the respondent.

Question 10. How should the topics of terrorism research be prioritised in Poland? (rank on the right hand side from 1 to 5, with 1 being the highest priority)

a. The process of radicalisation to terrorism,
b. Countering recruitment to terrorism,
c. Detection and blocking of terrorist propaganda,
d. Detection technologies for devices used to carry out terrorist attacks,
e. Countering the financing of terrorism.

Research topics marked with number 1

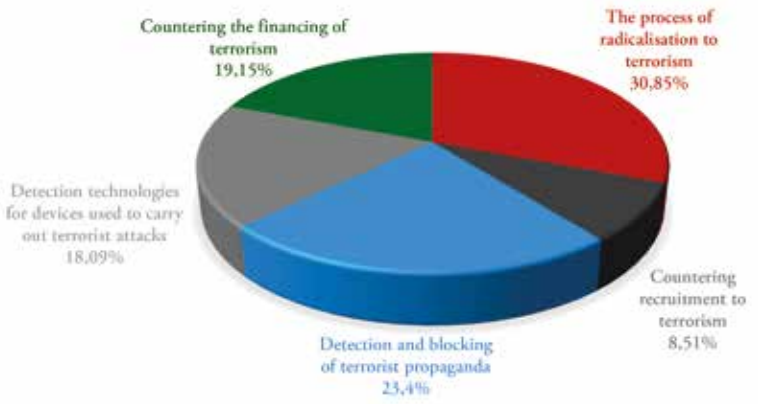

Figure 10. Share of individual terrorism research topics among those marked with number 1 (highest priority).

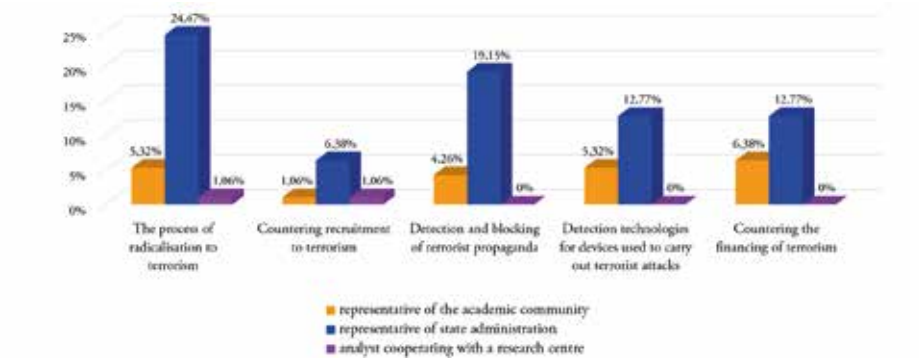

Figure 10a. Share of individual terrorism research topics among those marked with number 1 (highest priority) – distribution of answers according to the community represented by the respondent.

Research topics marked with number 2

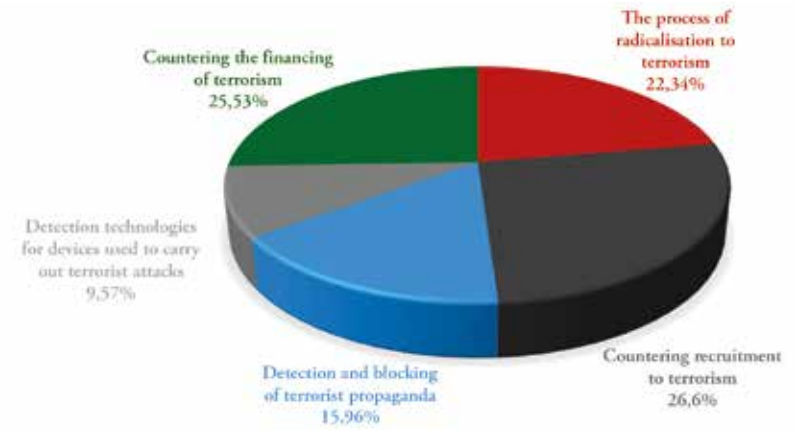

Figure 10b. Share of individual terrorism research topics among those marked with number 2.

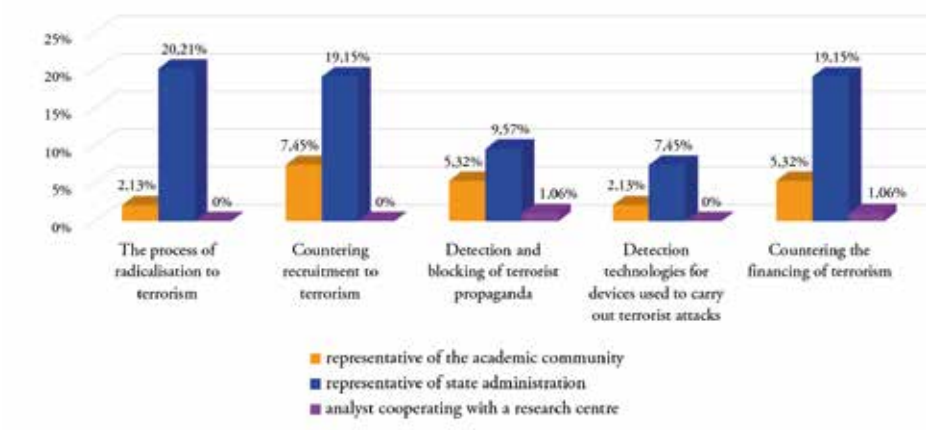

Figure 10c. Share of individual terrorism research topics among those marked with number 2 – distribution of answers according to the community represented by the respondent.

Research topics marked with number 3

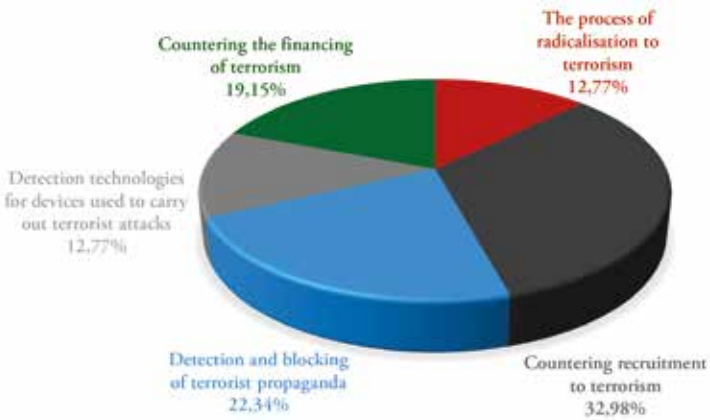

Figure 10d. Share of individual terrorism research topics among those marked with number 3.

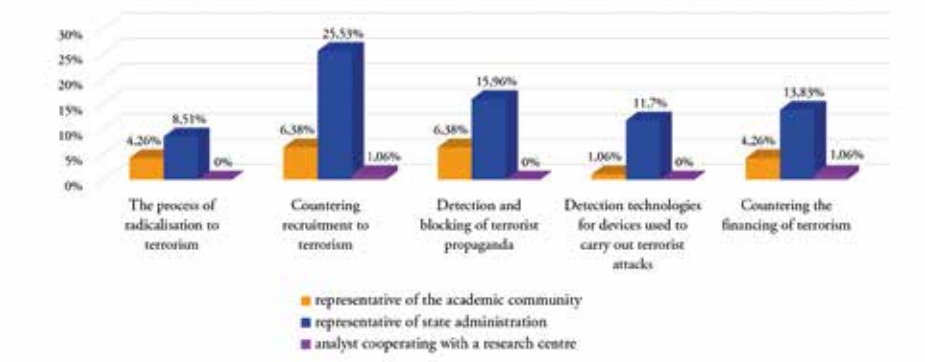

Figure 10e. Share of individual terrorism research topics among those marked with number 3 – distribution of answers according to the community represented by the respondent.

Research topics marked with number 4

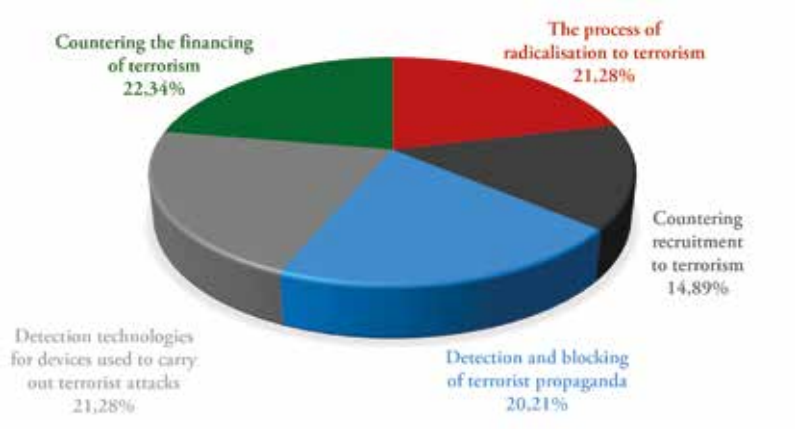

Figure 10f. Share of individual terrorism research topics among those marked with number 4.

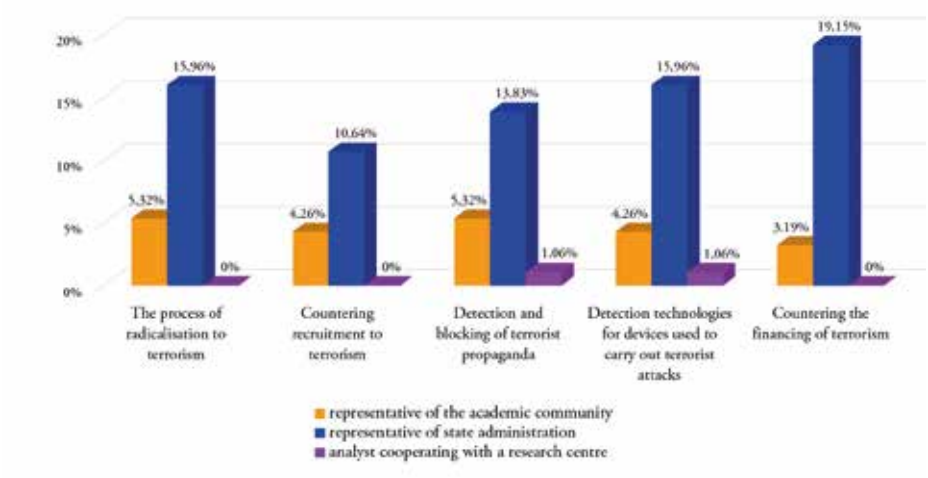

Figure 10g. Share of individual terrorism research topics among those marked with number 4 – distribution of answers according to the community represented by the respondent.

Research topics marked with number 5

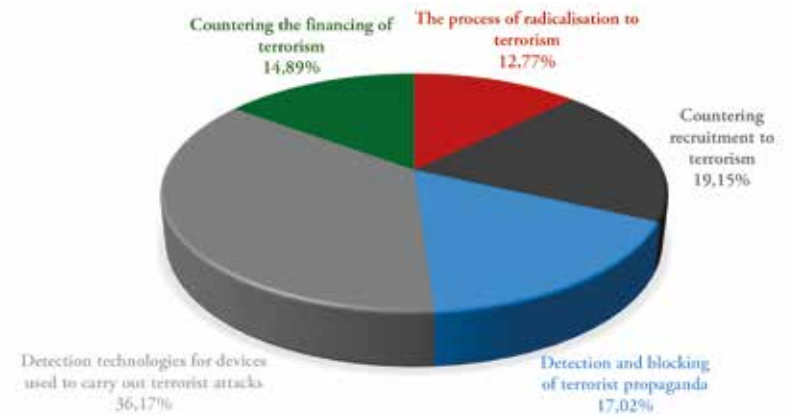

Figure 10h. Share of individual terrorism research topics among those marked with number 5.

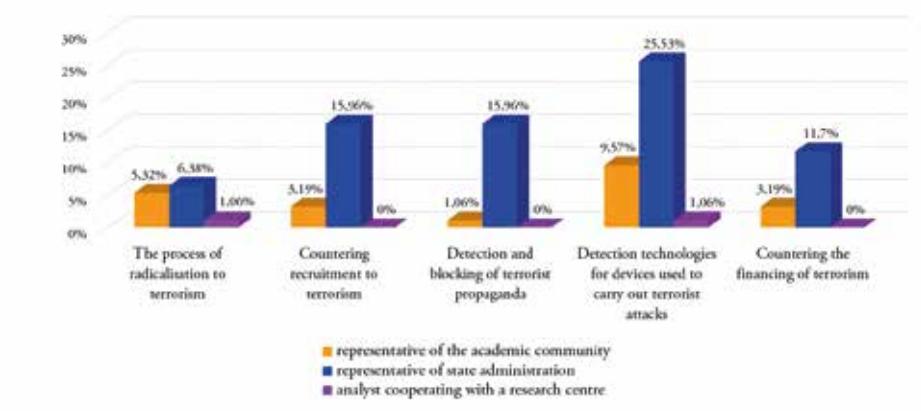

Figure 10i. Share of individual terrorism research topics among those marked with number 5 – distribution of answers according to the community represented by the respondent.

Question 11. Which initiatives that build anti-terrorist cooperation between academia and government institutions and services should be particularly developed? (rank on the right hand side from 1 to 4, with 1 being the most important initiative)

a. Patronage of university conferences,
b. Creation of formalised forums for the exchange of knowledge and experience,
c. Joint research and development projects,
d. Publication of joint guides on security education.

Initiatives marked with number 1

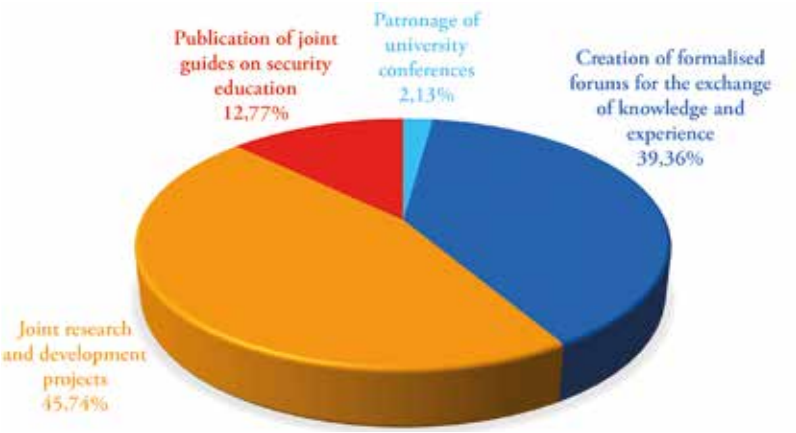

Figure 11. Share of individual initiatives building anti-terrorist cooperation between academia and government institutions and services in the group of initiatives marked with number 1 (the most important initiative).

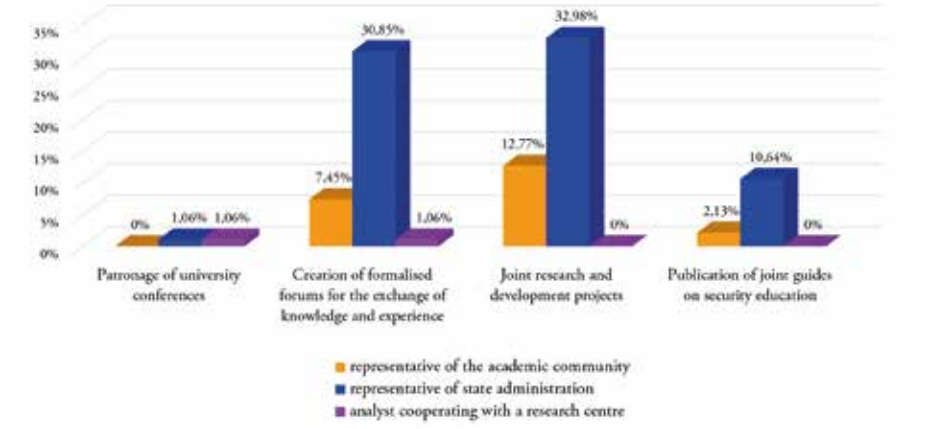

Figure 11a. Share of individual initiatives building anti-terrorist cooperation between academia and government institutions and services in the group of initiatives marked with number 1 (the most important initiative) – distribution of answers according to the community represented by the respondent.

Initiatives marked with number 2

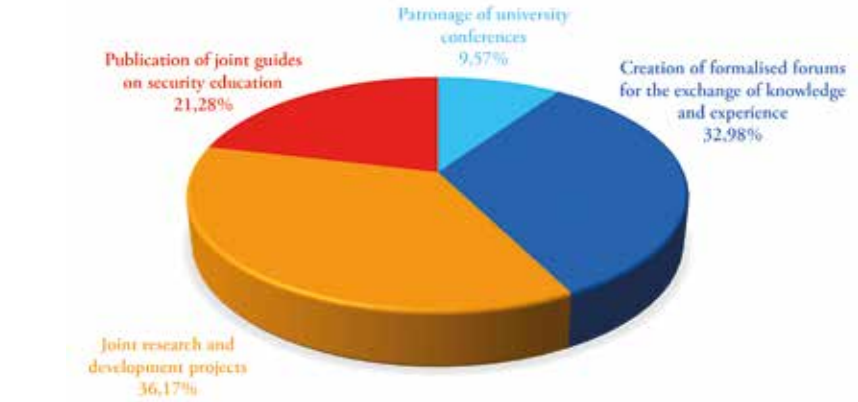

Figure 11b. Share of individual initiatives building anti-terrorist cooperation between academia and government institutions and services in the group of initiatives marked with number 2.

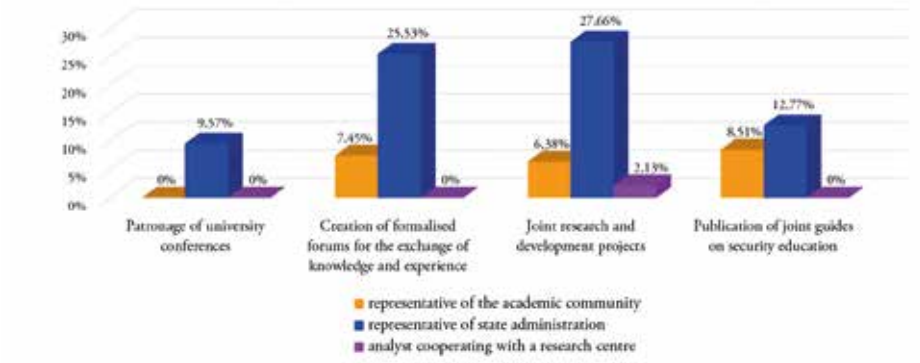

Figure 11c. Share of individual initiatives building anti-terrorist cooperation between academia and government institutions and services in the group of initiatives marked with number 2 – distribution of answers according to the community represented by the respondent.

Initiatives marked with number 3

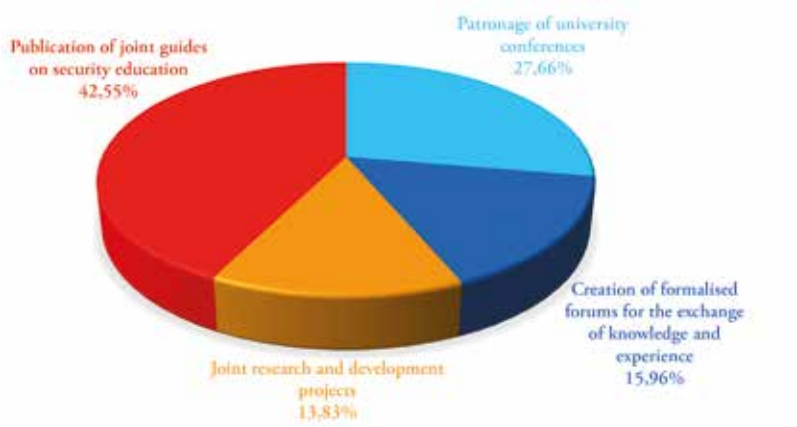

Figure 11d. Share of individual initiatives building anti-terrorist cooperation between academia and government institutions and services in the group of initiatives marked with number 3.

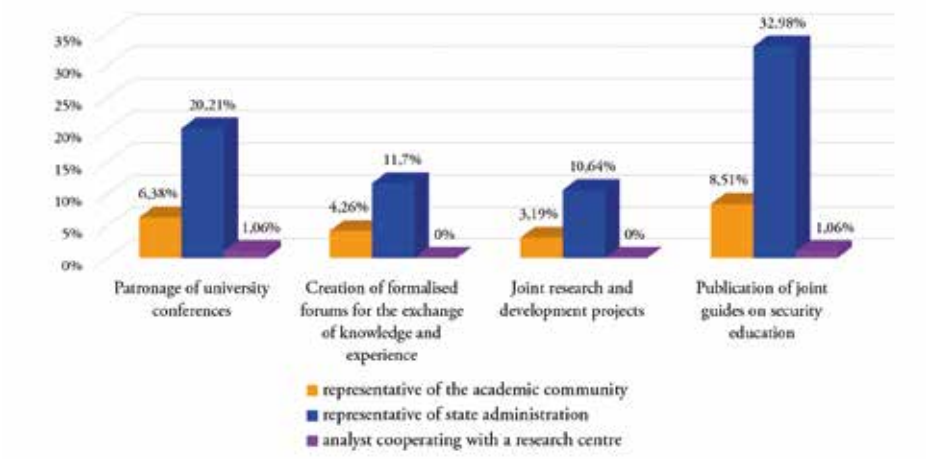

Figure 11e. Share of individual initiatives building anti-terrorist cooperation between academia and government institutions and services in the group of initiatives marked with number 3 – distribution of answers according to the community represented by the respondent.

Initiatives marked with number 4

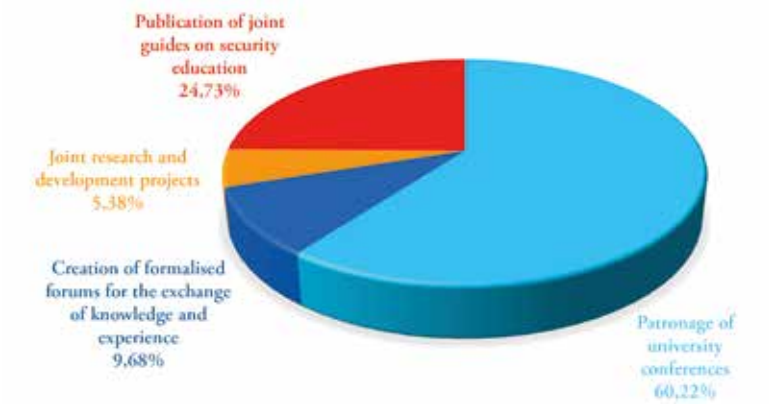

Figure 11f. Share of individual initiatives building anti-terrorist cooperation between academia and government institutions and services in the group of initiatives marked with number 4 (93 respondents, no answer from 1 respondent).

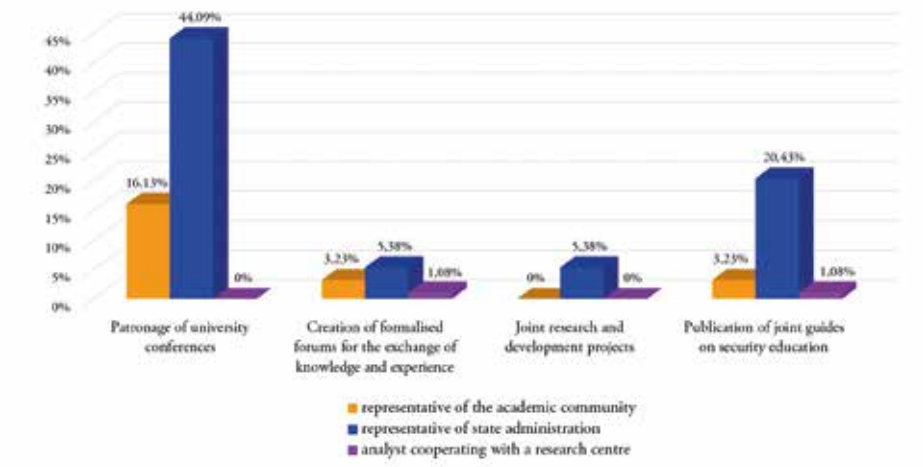

Figure 11g. Share of individual initiatives building anti-terrorist cooperation between academia and government institutions and services in the group of initiatives marked with number 4 – distribution of answers according to the community represented by the respondent.

DOI: 10.4467/27204383TER.22.030.16350

ORCID: 0000-0003-4649-589X

ANNA ROŻEJ-ADAMOWICZ

Book review: Tomasz R. Aleksandrowicz, *Prognozowanie zagrożeń terrorystycznych. Aspekty metodologiczne* (Eng. Forecasting terrorist threats. Methodological aspects)[1]

Raising public awareness plays an important role in effective terrorism prevention. Appropriately prepared organisations and services should impart the necessary knowledge and teach life-saving behaviours when a threat arises. In this way, the level of fear can be reduced and the ability of members of society to resist negative phenomena and the actions of others can be increased. Education should be multi-faceted, for different age and social groups. It should be based on sound knowledge, derived both from scientific knowledge and from experience.

The links between science and practice and the role of terrorism prevention are repeatedly mentioned by Tomasz Aleksandrowicz in his scientific monograph *Forecasting terrorist*

[1] T.R. Aleksandrowicz, *Prognozowanie zagrożeń terrorystycznych. Aspekty metodologiczne* (Eng. *Forecasting terrorist threats. Methodological aspects*), Warszawa 2022, Difin.

threats. Methodological aspects, which is the first attempt on the Polish arket to face the title issue. The aim behind this publication is to present the methodology of forecasting terrorist threats, i.e. basic methods, techniques and tools used in this process. The author, a professor at the Police Academy in Szczytno and a respected expert in the field of terrorism research, describes these issues against the background of national and international solutions, based on the experience of countries that have a long track record in identifying and combating terrorism, and the findings contained in his book organise the knowledge of these solutions. The primary research method used in his work is system analysis.

It is worth mentioning at this point that foresight is now an essential part of the functioning of states, organisations and individuals alike. Indeed, effective security strategies cannot rely solely on reactive measures, but must focus on anticipating threats. The main thesis of Tomasz Aleksandrowicz's book is that a properly developed forecast allows us to determine with high probability the possibility of a terrorist threat, but it is always an estimation of such a possibility, not a cognitive certainty.

The reviewed monograph covers 128 pages and consists of an introduction, seven chapters, a conclusion, an appendix and an extensive bibliography containing many valuable and, above all, up-to-date studies, which is worth emphasising due to the nature and dynamics of the studied processes. The author has carefully thought through the layout of the publication, which is coherent and logical. In the introduction, he has precisely defined the aim and subject of the research, the scope of the issues raised, the assumptions and limitations of the research, presented his position on the studied subject, and described the structure of the monograph. Chapters I-III are divided into subchapters covering specific issues. In the subsequent parts of the book, their separation was not justified due to the issues raised in them. The book is written in accessible language, at times colourful, as the author does not shy away from references to fiction, which may be of additional value to the reader. It is worth emphasising that the reviewed publication is thematically linked to Tomasz Aleksandrowicz's previous work on terrorism, its recognition and combating, which also speaks for its high level.

The author of the monograph has undertaken a very demanding task. This is because there is no doubt that forecasting is the most difficult part

of information analysis. It should be made clear that making a forecast is based on several categories of information and data. First of all, this is data coming from areas that can be subjected to cognition - this can be analysed, conclusions can be drawn from it, classic analytical questions can be answered: what? What is the result? This is the so-called hard data, which can be called strong signals about future developments. The second category is weak signals, which are identified with difficulty. These are such events (processes) that constitute novelty and are either outside the sphere available to our cognition or ignored. In English, the term *slow-burning issues* is sometimes used to refer to them, as they are almost imperceptible and their impact can only be noticed a long time after the first symptoms appear. In the future, however, these weak signals can have a significant impact. In forecasting, it is also necessary to be aware of the areas of ignorance and their extent and to try to estimate them. It is also important to remember that there is information and data that we do not want to know about. The reasons for this reluctance can range from political (having to make socially unpopular decisions) to psychological (cognitive dissonance). A forecast is therefore never a certainty - its validity can only be verified after a certain period of time, *post factum*. However, a well-prepared one makes us less surprised by the future. The effectiveness of a forecast, understood as the accurate determination of what will happen in the future, is not - especially in the area of security - the only criterion for its evaluation. On the basis of the forecast, decisions are often taken that prevent the occurrence of the risks it warns against. This means that it was both right and effective.

Attention is drawn, among others, by Andrzej Dawidczyk, a specialist in strategic analyses using qualitative and quantitative methods, to the fact that classical forecasting is based on the analysis of only that area of reality which we have been able to learn. In this way, we obtain a fragment of the picture of the future limited by our habits, accepted paradigms, hidden assumptions, determined by established canons of thought. According to Dawidczyk, there is also the aforementioned area outside the sphere of observation, inaccessible to cognition, in which processes take place that have a direct and sometimes decisive influence on future developments[2]. In studies on information analysis theory, such a situation

[2] A. Dawidczyk, *Analiza strategiczna w dziedzinie bezpieczeństwa państwa. Wybrane metody* (Eng. Strategic analysis in state security. Selected methods), Warszawa 2020.

has been described as a problem of analysis in the absence of sufficient data, and analysts have been urged to look for what is not there. The realisation that there was a need for such an intellectual search was called information awareness. Similarly, David Omand, a former British intelligence agent and security author, notes that our knowledge of the world around us is always fragmented, incomplete and we sometimes make errors of judgement. This is because we do not have all the information we need and, moreover, we feel reluctant to recognise that new data should change the picture of reality already developed. We also have difficulty understanding our opponent's motivations, which is linked to a lack of knowledge of the culture in which they operate and the beliefs they have developed[3]. Bobby W., an analyst in the CIA's Analysis Department, states that (...) *there is no such forecasting technique that is able to determine the timing of a trend-changing fact (timing of nonlinearity)*[4]. An intelligence analyst can formulate a prediction about the increased sophistication of Al-Qaeda's plans and the increased tension in the Middle East, but he cannot predict when terrorist-hijacked planes will hit the World Trade Center towers or when the self-immolation of a street vendor in Tunisia will cause civil unrest. The processes leading to changes in activity are gradual, but when a phenomenon starts to go beyond the pattern observed so far, this represents a previously unpredictable tipping point. To the forecasting difficulties indicated, one must add the widespread information warfare, elements of which are disinformation and misleading, including for those trying to predict future developments.

A great asset of Tomasz Aleksandrowicz's book is that the author addresses one of the most difficult and complex analytical themes, which includes forecasting terrorist threats. The starting point for his considerations is the claim that terrorists always have an advantage over the state, as they can attack at a time, in a manner and against a target of their choice, while the state is unable to defend every potential target against every type of attack at all times. This is especially true in democratic states, as terrorists use the basic attributes of democracy, such as freedom of speech, access to information, freedom of movement or the right to privacy, to prepare and carry out their attacks. These attributes unfortunately favour the existence and development of terrorism. The perpetration of a terrorist

[3] D. Omand, *How Spies Think. Ten Lessons in Intelligence*, London 2020.

[4] W. Bobby, *The Limits of Prediction – or How I Learned to Stop Worrying about Black Swans and Love Angels*, "Studies in Intelligence" 2019, vol. 63, no 4.

attack in North Korea, for example, is unlikely due to the total surveillance of everyone on its territory. Freedom and democracy come at a cost - in this case the price is the threat of terrorist attacks.

In the introduction to the book, the author formulates an extremely interesting research problem, based on (...) *resolving the dilemma of whether it is possible to forecast terrorist threats and what should be the methodology for developing such forecasts* (p. 9). He writes that the primary objective of his research is (...) *to develop a methodology for forecasting terrorist threats. The thesis that the author is tempted to prove is that it is possible to forecast terrorist threats using an appropriate methodology in the process of developing them* (p. 9). This justifies the adopted structure of the study - from the systematisation of theoretical issues in the field of forecasting (the author analyses them in the context of security science), through the analysis of the subject of forecasting, i.e. contemporary terrorism, to the proposal of a forecasting methodology in the subject at three levels: strategic, operational and tactical.

Writing about the specificity of security sciences (chapter one), the author of the monograph maintains his view, formulated much earlier, of the multifaceted nature of this discipline (this is also reflected in the literature he cites). His deductions on this subject lead him to correctly establish the object and purpose of the research. The author sees their meaning in the effective provision of state security, which is precisely what the forecasting of terrorist threats is supposed to serve. It can be concluded that the inclusion of the considered issues within the framework of security science is largely justified, however with reservations, which are discussed later in the review.

The author captures the science of security in a way that invites discussion, circling between a broad view and the need to embed it in a more concretised layer of purpose (scientific purpose). In fact, after considering the interdisciplinarity of the security sciences, he formulates the view that (...) *the basic criterion differentiating the security sciences from other scientific disciplines is the object of research, which - despite its signalled broadness - can be reduced to the subject's security environment and its response to the resulting opportunities, challenges, threats and risks* (p. 34). In doing so, he places the considerations in the strategic thinking and action stream, referring to the most important categories ordering security research derived by theorists from the military sciences (challenges, threats, etc.). In doing so, he points out that this kind of research should be in close relation to practice

(chapter two), which is obvious in the context of the constant need to improve security systems. This approach seems appropriate for the search for an appropriate methodology for forecasting threats, not only those of terrorism. It is important that Tomasz Aleksandrowicz recognises and uses the achievements of other authors (e.g. Andrzej Dawidczyk, Mirosław Sułk) describing various methods and their applications in research on security in its various dimensions. According to the reviewer, in future editions of the book, it would be worthwhile to include in the references the latest position by Andrzej Dawidczyk and Justyna Jurczak entitled *Metodologia bezpieczeństwa w przykładach i zastosowaniach* (Eng. Safety methodology in examples and applications), (Warszawa 2022, Difin).

An extremely interesting part of the theoretical introduction to the subject of the study is the one devoted to the American school of intelligence analysis. Here, the author refers both to his own numerous studies on the subject, as well as to the rich literature on the subject and primary sources (documents, accounts). This part of the monograph is an introduction to the author's proposal of forecasting methodology, as it contains a very comprehensive overview of the methods and techniques and approaches used in it.

The next (third) chapter, which presents an analysis of terrorist threats as an object of forecasting, should be considered as equally valuable. The author moves freely in this area, citing the findings of authorities and the results of recent research, and above all verifying his own assessments and theses contained in earlier studies. This part of the publication complements the knowledge based on Tomasz Aleksandrowicz's original approach to the issue in question.

The fourth chapter is devoted to general findings on terrorist threat forecasting. In it, the author describes the practice of identifying and counteracting these threats, related not only to the activities of the services and special units, but also of the administration responsible for state security. Remaining in the analytical trend developed in the USA, he also includes in the analysis domestic legal and organisational solutions. This is a great asset of the monograph.

Chapters five, six and seven are devoted to forecasting at the strategic, operational and tactical levels, respectively.

The description of the strategic level includes a model of the base of terrorist events (attacks) on a global scale. The author refers to existing solutions of this type and indicates the need for a uniform template

for data description. At the strategic level, the fundamental directions of the state's counter-terrorism policy are set and the knowledge needed for forecasting at the operational level is drawn (p. 92), a conclusion that can be considered valid. The primary objective of terrorist threat forecasting at the strategic level is to answer the fundamental questions: does such a threat exist? Could we be forced to face it in the foreseeable future? From what directions might the threat emerge? What might its nature be? What state responses does it require at the strategic level? This is therefore a classic multi-factor analysis and forecast, the results of which form the basis for policy decisions not only related to the projected threat to the state in question, but also arising from the state's legal, international and alliance obligations, such as participation in multilateral conventions, bilateral agreements, accords, alliances, or indicating the need to join such or intensify international cooperation in this regard. In the sphere of domestic policy, the findings of the strategic forecast may (and should) constitute the basis for decisions on the construction of the anti-terrorist system, its shape, components and directions of development, and if such a system already exists - on the directions of its improvement taking into account the changes indicated in the forecast.

The starting point for the construction of a terrorist threat forecast at the strategic level is the creation of a database of attacks on a global scale over a specific time period, which allows the trend in threats to be identified. Of course, it is possible to use publicly available databases, e.g. START, the Global Terrorism Index (GTI) or the EU Terrorism Situation and Trend Report (TE-SAT), but attention must be paid to the methodology used in them, i.e. which incidents of violence are qualified as a terrorist attack by the creators of each database. Such a database must contain not only information about the attacks carried out, but also many other records and be relational in nature, i.e. allow searches according to set criteria.

The operational level and forecasting at this level, described in the next chapter, relate to a specific security entity. In this section, the author presents national procedures on the basis of documents, quoting them extensively. This is, in the reviewer's opinion, a legitimate procedure in the context of the purpose of the study.

Forecasting at the tactical level is also described with reference to documents and selected theses taken from national literature. The author emphasises the link between this forecasting and operational reconnaissance, thus stressing the practical dimension of the activity

in question. The starting point for creating terrorist threat forecasts at the tactical level is several categories of data. These are primarily the findings of the forecast at the strategic level, i.e. regarding the main directions of the threats, the preferred targets of attacks and modus operandi, the political time (e.g. elections, strikes and civil unrest, mass events). Based on this information, criteria for the selection of the target, time and modus operandi of the perpetrators can be developed and adapted to local circumstances. When creating a forecast at the tactical level, the data contained in the operational forecast should be used. It allows for the selection of potential targets (objects) of attacks and, therefore, at the same time for the targeting of activities consisting in the recognition of these objects by counter-terrorist services in terms of the characteristics of the terrain, the layout of the premises, the manner of protection, technical security or procedures. It is also necessary to take into account data from ongoing operational reconnaissance, which relates to identified preparations for an attack or an attack already carried out (precisely: in progress), e.g. in the case of hostage-taking.

At this point, it is worth mentioning Tomasz Bajerowski and Anna Kowalczyk's concept of realised risk. According to them (...) *there is a need to supplement risk assessment methods with an analysis of the feasibility (possibility of realisation) of crisis events, where feasibility (possibility) is the deterministic weight of a random phenomenon*[5]. They propose a formula for estimating the risk (using a mathematical method) of specific phenomena or events that includes the feasibility (possibility) of their realisation, with a particular focus on phenomena that are almost improbable, but possible and capable of producing extreme effects. In doing so, the authors distinguish between two concepts: the probability and the feasibility (possibility) of an event occurring.

It should be noted that there is a feedback loop between terrorist threat forecasts at strategic and operational levels. The findings of the strategic forecast are sometimes complementary to the operational forecasts, if only when links between different entities (e.g. individuals or companies implicated in terrorist activities) are demonstrated and the operational forecast shows that they are involved in the identified situation.

[5] T. Bajerowski, A. Kowalczyk, *Feasibility (Possibility) and Probability in Risk and Crisis Management*, reproduced typescript in the author's possession.

In summary, the concept of terrorist threat forecasting described in the monograph boils down to a synthesis of general forecasting methods existing in science with guidelines for the accumulation of knowledge in the field in question. A threat recognition system designed in this way (partly based on already existing national solutions) is a valuable contribution to the development of security theory and an important contribution to the analysis of existing solutions at strategic, operational and tactical levels. Many of the findings, assumptions and concepts contained in Tomasz Aleksandrowicz's monograph provide a good starting point for further scientific debate, which is another value of this book.

The publication should be of interest primarily to students and researchers in the field of security sciences, as well as those involved in analytical work, crisis management and planning of anti-terrorist and counter-terrorist activities in law enforcement agencies and intelligence institutions belonging to the national counter-terrorism system, which consists of members of the Interministerial Team for Terrorist Threats. Tomasz Aleksandrowicz's book can also be used as a textbook in courses on terrorist threat analysis organised in academic circles and in state administration. It is worth considering an English-language publication so that the Polish perspective on global threat forecasting can complement the literature available in Euro-Atlantic training structures.

About the authors

Piotr Burczaniuk, PhD - Assistant Professor in the Department of Theory and Philosophy of Law at the Faculty of Law and Administration of Cardinal Stefan Wyszynski University in Warsaw; legal adviser, member of the Regional Chamber of Legal Advisers in Lublin; member of the Polish Legislation Society, expert on legislation. Author of publications on the theory and philosophy of law, constitutional law and business law. His scientific activity is related to the creation and application of law.

Mariusz Cichomski - lawyer, sociologist, graduate of doctoral studies at the University of Warsaw. For several years he has been professionally engaged in issues related to terrorism, organised crime, supervision over the activities of services and legislation.

Ilona Idzikowska-Ślęzak - political scientist, since 2008 professionally connected with the Ministry of Interior and Administration. Currently she heads the department responsible for issues related to terrorism, organised crime and the organisation of the State Protection Service.

Krzysztof Izak - retired officer of the Internal Security Agency.

Krzysztof Karolczak, PhD - political scientist, graduate of the Faculty of Journalism and Political Science of the University of Warsaw, doctor of humanities in the field of political science. Until 2008 a researcher at the Institute of Political Science of the Faculty of Journalism and Political Science of the University of Warsaw. A lecturer at the Helena Chodkowska University of Management and Law in Warsaw, the Bolesław Prus University of Humanities in Warsaw (rector), Collegium Civitas and the Diplomatic Academy of the Ministry of Foreign Affairs. Author of books: *Encyklopedia terroryzmu* (Eng. Encyclopedia of Terrorism) (1995), *Terroryzm. Nowy paradygmat wojny w XXI wieku* (Eng. Terrorism. A new paradigm of war in the 21st century) (2010), *Terroryzm i polityka. Lata 2009–2013* (Eng. Terrorism and Politics. Years 2009-2013) (2014).

Michał Piekarski, PhD - Assistant Professor in the Department of Security Studies of the Institute of International Studies, University of Wrocław. He analyses the phenomenon of „hybrid warfare" in Europe, contemporary terrorism, issues of national maritime security, and issues of Polish strategic culture.

Anna Rożej-Adamowicz, PhD - Vice President of the Management Board of Inseqr sp. z o.o. Expert in conducting projects related to cyber security. Security officer. She specialises in assessing threats and constructing security policies for IT systems that process classified information. Academic lecturer and author of numerous publications in the field of ICT systems security and management.