TERRORISM

studies
analyses
prevention

TERRORISM
PREVENTION
Centre of Excellence

CENTRALNY OŚRODEK
SZKOLENIA I EDUKACJI ABW
im. gen. dyw. Stefana Roweckiego „Grota"

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

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 March 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!

The attacks on the World Trade Center and the Pentagon on 11 September 2001 marked a turning point in international relations and made the world community aware of the enormity of the dangers posed by terrorism. The intelligence and security services of NATO countries were obliged to reorient their counter-terrorist strategies.

The Internal Security Agency, whose 20th anniversary we are celebrating this year, is one of the most important pillars of the anti-terrorist system of the Republic of Poland. This has its basis in the provisions of the Act on Anti-Terrorist Activities, which came into force in 2016. The Agency's tasks are carried out by two specialised and closely cooperating organisational units: Counter-Terrorism Centre - which conducts operational and reconnaissance activities, and the Terrorism Prevention Centre of Excellence - which deals with counter-terrorist prevention in its broadest sense.

Terrorism, which for years has posed a serious threat to the internal security of many countries, continues to evolve. Therefore, the intelligence and security services must constantly increase their anti-terrorist potential and adapt it to new challenges. This is done, among other things, by strengthening cooperation between national counter-terrorist units and the academic world represented by researchers of the phenomenon of terrorism.

Since the tragic events of 2001, almost 300 thematic publications have been published in Poland, of which Polish scientists are authors or co-authors. Many of these have had a significant impact not only on the national counter-terrorist system, but also on regional security policy. Appreciating the importance of Polish research, on the 20th anniversary of the attacks on the WTC and the Pentagon, I made the decision to establish within the Internal Security Agency a scientific journal devoted to terrorism.

The periodical 'Terrorism - studies, analyses, prevention' is intended as a platform for exchanging scientific thought and experience. It brings together the academic world and representatives of institutions and services that for over 15 years have been working together under the Interministerial Team for Terrorist Threats, which is the coordination centre of the anti-terrorist system of the Republic of Poland. I would like the pages of the magazine to host a discussion on the direction in which the terrorist threat is developing, how intelligence and security services, anti-terrorist and counter-terrorist institutions as well as international bodies and bodies building the resilience of the Euro-Atlantic community to terrorist attacks should react. Terrorism prevention issues will also be a very important element of the new magazine. The success of any anti-terrorist system is measured by the effectiveness with which it prevents such attacks and the efficiency of state bodies in crisis situations.

Encouraging you to read the first issue, I would also like to invite you to contribute to the creation of the scientific journal 'Terrorism - studies, analyses, prevention' by sharing on its pages your theoretical and practical knowledge.

Head of the Internal Security Agency
Col. Krzysztof Wacławek

Ladies and Gentlemen!

The past experience of Western countries in the fight against terrorism shows that they are able to achieve an operational advantage over terrorists if they create an effective mechanism of coordination and cooperation in counter-terrorism, functioning at the level of international, interministerial and interinstitutional cooperation. Related research and scientific initiatives provide valuable support to the counterterrorism system. Their intensification is in the interest of all services and institutions responsible for national security.

One of such initiatives is a new scientific periodical "Terrorism - studies, analysis, prevention" created within the Internal Security Agency. Scientific and educational materials related to the challenges faced by Poland and other NATO member countries in the fight against terrorism will be presented on its pages. Topics covered will include: legal and organizational aspects of increasing the effectiveness of anti-terrorist systems, ways to build resistance to terrorist attacks, new technologies as tools in the hands of terrorists, historical issues related to terrorism and their translation into contemporary reality, educational activities for anti-terrorist security conducted in different social groups. Foreign affiliation of some of the members of the scientific board, reviewers and authors, as well as English-language translation of the journal will allow it to reach a wider audience.

In the first issue of the new periodical you will find articles devoted, among others, to: selected features of XXI century terrorism, legal aspects of the fight against terrorism in Poland and the EU, the 15th anniversary of the Interministerial Team for Terrorist Threats, radicalization leading to terrorism and methods of preventing this phenomenon applied in France, the use of cyberspace for terrorist activity, unmanned aerial vehicles used for terrorist attacks on objects of energy infrastructure, as well as the activity of the new unit of the anti-

terrorist division of the Internal Security Agency - Terrorism Prevention Centre of Excellence.

Inviting you to read the journal "Terrorism - studies, analysis, prevention", I hope that it will fulfil its mission of strengthening cooperation between the various communities involved in anti-terrorist protection activities and broaden the perspective of these issues. I also believe that it will systematically develop, gaining a large group of readers and supporters.

Editor-in-Chief of the journal
"Terrorism - studies, analysis, prevention"
Damian Szlachter, PhD

DOI: 10.4467/27204383TER.22.009.15425

ORCID: 0000-0003-4892-6112

KRZYSZTOF KAROLCZAK

Terrorism in the 21st century - selected aspects

Abstract

The article outlines selected aspects of terrorism in the 21st century. Taking into account the historical perspective, the modus operandi used by the perpetrators of attacks (suicide bomber, "lone wolf") is described, together with examples of the most spectacular attacks: decapitation, use of chemical weapons, attacks with vehicles. Two charts accompany the text: "Number of terrorist attacks in the world (2006-2019)" and "Most active groups carrying out attacks in the world in 2019 by number of attacks".

Keywords:

terrorism, terrorist attack, suicide bomber, decapitation, "lone wolf", chemical weapons, attacks using vehicles

The world entered the new millennium triumphant and hopeful. Francis Fukuyama's vision of the "end of history"[1], the victory of liberal democracy, was to mean the end of the Cold War and the division of the world into two opposing political and military blocs. The assumption of leadership in this new world order, which could not be questioned by anyone, by a single superpower - the United States of America - was to guarantee only a happy future.

[1] F. Fukuyama, *Koniec historii* (Eng. End of history), translated by T. Bieroń, M. Wichrowski, Poznań 1996.

The year 2001, the beginning not only of a new century, but also of a new millennium, was a breakthrough in the history of world terrorism. Whereas up until then it had been an international phenomenon at best (according to the maxim: international terrorism occurs when terrorists from one country carry out an attack on the territory of another in the interests of a third), after 11 September 2001 it became, due to its nature and scope, a global phenomenon. Of course, this was largely due to the fact that, for the first time since the Second World War, the United States, a global power, was attacked on its territory on that day. In addition, the World Trade Center and the Pentagon were attacked by the Al-Qaeda organisation, which, although it had previously carried out attacks in various parts of the world[2], had until then been a classic hierarchical organisation. However, it quickly evolved into a network organisation covering the entire globe.

Terrorism in the 21st century

Over two thousand years of documented history, terrorist methods have changed as technology has advanced, but it has been more a case of adding new tools to existing, proven ones. Assuming that the first terrorists were sicarios[3] operating in 1st century A.D. in Palestine, who carried out attacks (assassinations) with a short sword, dagger or *sica*[4],

[2] Among others, on 7 August 1998, in two capitals of East African countries, Nairobi (Kenya) and Dar es-Saalam (Tanzania), almost simultaneously (at an interval of several minutes), buildings of the US embassies were blown up - under the debris of the first one, 12 Americans, 32 citizens of other countries and 247 Kenyans were killed, and over 5000 Kenyans, 6 Americans and 13 citizens of other countries were wounded; in the second attack, 10 people were killed and 77 wounded. Incidentally, it was on the occasion of these attacks that the world public became aware of the activities of Osama bin Laden and al-Qaeda. The 20th century also ended with an assassination attempt on American soldiers, to which al-Qaeda confessed: On 12 X 2000, in the port of Aden (Yemen), the destroyer USS Cole was hit by a speedboat loaded to the brim with explosives, causing a large breach in the ship's side and the death of 17 sailors (39 were injured).

[3] Sicarios - the most extreme faction of Jewish Zelots fighting against the Roman occupiers; cf. W. Laqueur, *Terrorism*, London 1980, pp. 18-19.

[4] In modern Spanish *sicario* means paid killer, in Italian and Portuguese it means contract killer.

one could say that after two thousand years, history has come full circle, as today's terrorists also very often use a knife or a sword[5].

The modus operandi of terrorists in the 21st century

In the 21st century, terrorists use the same methods as their predecessors, adapting them to their needs and capabilities. Therefore, their most common modus operandi includes bombings, ramming vehicles into pedestrians and attacking bystanders with knives.

Suicide attacks

World terrorism in the first years of the 21st century has been dominated by suicide bombers (as were the attackers on 11 September 2001). Suicide bombers often wear explosives under their clothes (the term "shahid belt" has entered colloquial language), carry them in backpacks (as the London bombers did on 7 July 2005) or even hide them in the frames of bicycles. Often, to cause even more damage, suicide bombers drive vehicles filled with explosives.

The modern history of suicide bombing as a deliberate tactic of terrorists is relatively short - it can be dated back to the early 1980s. Analysts point to the dynamics of their increase: "Since 1983, suicide bombing has become the preferred terrorist tactic of insurgent groups from Sri Lanka to Chechnya to Afghanistan. One indicator of this growing preference is the number of attacks, which rose from 1 in 1981 to more than 500 in 2007"[6].

In the societies of Western civilisation, these attacks have caused shock because they are incompatible with the dogmas of the Christian religion. However, for followers of other religions, suicide is not forbidden, and by non-believers this problem is not considered at all (if at all, then in moral terms). What is more, even in Islam, which for many years did not allow women to engage in terrorist activities, at some point suicide bombings were permitted (the first such missions

[5] The myth of the sicarios has been referred to by ultra-orthodox Jews from the Sikrikim group, formed in 2005, who attack Israel's secular community.

[6] Cited after J. Kiras, "*suicide bombing*," *Encyclopedia Britannica*, 13 XI 2019, https://www.britannica.com/topic/suicide-bombing [accessed: 28 XI 2021].

were not undertaken by Muslim women, but by Tamil Tigresses; one of them, Thenmozhi Rajaratnam, killed former Indian Prime Minister Rajiv Gandhi in such an attack on May 21, 1991). In Russia, so-called black widows (*smiertniks*) have appeared - Chechens, and in Israel - shahidis, Palestinian women, members of the Army of Roses[7].

Despite the fact that children are given special care in every community, it is not uncommon for them to take part in armed conflicts or be used to carry out terrorist attacks, including suicide attacks.

In general, the number of suicide attacks represented a negligible percentage of terrorist attacks. Riaz Hassan in his article *What Motivates the Suicide Bombers? Study of a comprehensive database* gives a surprising answer states that in the years 1981-2006 there were 1200 suicide bombings, which constituted only 4% of all terrorist attacks and 14 599 people were killed in them, which constituted 32% of all victims[8]. Therefore, due to their spectacularity, terrorist organisations are very keen to use this method of action.

Decapitation: a new/old method of psychological warfare

Beheading is not a new idea and, still less, was not invented by Islamic fundamentalists. As a means of carrying out a judicial death sentence, this method has been known for millennia. Decapitation was used by the authorities against political opponents and common criminals in ancient times (in China, in Middle Eastern countries), in the Middle Ages (in Europe), in modern times (still in Europe) and even today this punishment is used in Saudi Arabia. Only the tools changed: it could be an axe, sword or guillotine, but whatever the executioner used, it was carried out in public and played a double role - both as punishment for real (or imagined, as often happened during the French Revolution, for example) crimes and as a warning to others, who were to be made aware of what might await them if they opposed the authorities.

Islamic fundamentalists have returned to this method in the 21st century. Just a few months after the war on terror began, on 23 January 2002, the American journalist Daniel Pearl was abducted in Pakistan

---

[7] Cf. B. Victor, *Army of Roses. Inside the World of Palestinian Women Suicide Bombers*, London 2004.

[8] R. Hassan, *What Motivates the Suicide Bombers? Study of a comprehensive database gives a surprising answer*, „YaleGlobal", 3 IX 2009 [accessed: 28 XI 2021].

and then killed by his captors on 1 February. The video of the execution, posted on the Internet, was entitled *The Slaughter of the Spy-Journalist, the Jew Daniel Pearl*, and depicted the last seconds of the journalist's life, his statement in which he admitted his Jewish ancestry (which many analysts considered manipulated), and the scene of his decapitation. His body was found and identified on 16 May. The abduction and killing of the American was claimed by a hitherto unknown organisation, the National Movement for the Restoration of Pakistani Sovereignty, but the Pakistani authorities charged and arrested several members of al-Qaeda, including Sheikh Ahmed Saeed Omar, who even confessed to Pearl's murder and was sentenced to death (the sentence was not carried out)[9]. We should also always remember that the same death befell the Polish geologist Piotr Stańczak on 7 February 2009 in Pakistan, who had been abducted by the Taliban several months earlier.

Video footage of the decapitation of those abducted by Iraqi al-Qaeda appeared in 2004 on the Internet and was also broadcast by the Qatari television channel Al-Jazeera. The executor was said to be the group's leader Abu Musab al-Zarkawi (although this information was disputed by people who knew him), who replaced Osama bin Laden on the lists of the most dangerous terrorists. Al-Zarkawi is said to have personally decapitated Nicholas "Nick" Berg (7 May 2004) and Owen Eugene "Jack" Armstrong (20 September 2004). The Americans on 6 June 2006 carried out a bombing raid on al-Zarkawi's home, where he was hiding. Al-Zarkawi was killed, and executions of abducted hostages ceased to be a method used on a massive scale in the fight between Islamic fundamentalists and the West, although they occasionally occurred.

In 2014, thanks to the Islamic State, world public opinion was electrified by the use of decapitation once again as a method not only to eliminate the enemy, but also to intimidate and coerce the group's demands. Between 25 July 2014 and 10 August 2015, at least 300 people (foreign journalists, Syrian and Kurdish soldiers, humanitarian workers, Christian refugees from Ethiopia) were murdered in this way in 24 executions[10].

[9] Sheikh Omar recanted his confession in 2007 when Khalid Shaykh Muhammad confessed to killing Pearl.

[10] https://edition.cnn.com/2015/04/19/africa/libya-isis-executions-ethiopian-christians/ [accessed: 20 XI 2021].

Lone Wolf

According to the media, the new category of terrorists in the 21st century is made up of assassins who are not members of any group, who do not act on the orders of any of their commanders, who do not follow any specific global plan, but loners who prepare and carry out attacks on their own, without any outside help. Nothing could be further from the truth - although, of course, a single assassin's attack on a politician must be distinguished (there have been many such assassins in history, including our own, to mention Michał Piekarski and his attack on King Sigismund III Vasa with an axe) from a terrorist attack. The first "lone wolves" could include Antoni Berezowski, who carried out an unsuccessful assassination attempt on Tsar Alexander II in Paris on 6 June 1867, Sante Giovanni Caserio, associated with anarchist circles, the assassin of French President Marie-François Sadi Carnot (24 June 1894, Lyon), and Luigi Lucheni, the assassin of Empress Elisabeth of Austria (10 September 1896, Geneva), or finally Leon Czolgosz, who fatally shot U.S. President William McKinley in Buffalo on 6 September 1901.

There were also many such 'lone wolves' in the second half of the 20th century. Two Americans, Theodore Kaczynski "Unambomber" and Timothy McVeigh, among others, went down in the history of terrorism.

Theodore Kaczynski could perhaps be classed as a representative of the environmental movement or, to use 19th century terms, a Luddist, although he wrote about himself that he was protesting against modern technology[11]. For 17 years he sent letter-bombs to politicians, scientists and heads of corporations, which killed three people and wounded twenty-nine. He was arrested on 3 April 1996 and sentenced to life imprisonment;

Timothy McVeigh held far-right views and considered the government in Washington to be the Zionist Occupation Government (ZOG). He carried out the bombing of the federal government building in Oklahoma City (19 April 1995), which killed 168 people. He was arrested and sentenced to death.

"Lone wolf" was also the Austrian Franz Fuchs, who between 1993 and 1997, for xenophobic reasons, as the "Salzburger Eidgenossenschaft - Bajuwarische Befreiungsarmee" (Salzburg

[11] He presented his views in the manifesto *Industrial Society and Its Future*, first published on 19 IX 1995 by The New York Times and The Washington Post.

Confederation - Bajuwarische Befreiungsarmee) sent bomb letters to politicians (including the mayor of Vienna, Helmut Zilk), Green Party politicians and humanitarian activists. He was arrested, tried and in 1999 sentenced to life imprisonment (he committed suicide on 26 February 2000).

In the 21st century, "lone wolves" mainly attack random victims, although they do so, as they say, in the name of an idea. The most spectacular, tragic attack was carried out on 22 July 2011 by the Norwegian Anders Behring Breivik[12], an advocate of extreme right-wing views. He wrote and published online on the day of the attack the manifesto *2083 - A European Declaration of Independence*, which is a compilation of racist, xenophobic, anti-feminist and Islamophobic texts, but also directly taken from Theodore Kaczynski's *Manifesto*. Breivik first carried out a bomb attack on the prime minister's residence in Oslo (8 people were killed), and then moved to the island of Utøya, where he massacred participants of a Norwegian Labour Party youth camp with firearms. Sixty-nine people were killed. Arrested, despite many doubts about his mental state, Breivik was found sane and sentenced to the highest possible sentence, i.e. 21 years in prison (with the possibility of its unlimited extension).

In principle, this case could be treated as one of many attacks carried out by mentally disturbed people (Breivik was diagnosed with delusional disorder or narcissistic personality disorder, among other things, he believed himself to be the regent of Norway). This included Stephen Paddock's shooting on 1 October 2017 at a country music concert taking place outside the Luxor Las Vegas casino - 60 people were killed and 411 injured at the time. At the Century 16 Theater in Aurora, Colorado, during the premiere of *The Dark Knight Rises*, James Holmes injured 58 people with a gun on 20 July 2012. However, these attacks were not terrorist attacks. The fact that Breivik, by his own admission, carried out the attacks for political reasons, and his behaviour during the trial (making the gesture of a fascist salute) make it possible to classify the act as terrorist.

Such doubts are not raised by attacks carried out by Muslims who, although not affiliated with any jihadist group, carried out their individual actions emphasising their profession of faith (*Allah akbar*).

[12] In June 2017, he changed his name to Fjotolf Hansen.

Britain, for example, became the scene of two attacks carried out by fanatical followers of Islam in 2017, one of which can be attributed to a 'lone wolf'. Fifty-two-year-old British citizen Khalid Masood[13] drove the car he was driving onto the pavement of Westminster Bridge and Bridge Street on 22 March, injuring more than 50 people (four of them fatally) before crashing the vehicle into the fence of the Palace of Westminster. He got out, made his way into the Parliamentary courtyard, fatally wounded a police officer and was shot moments later.

Chemical weapons in the hands of terrorists

On 20 March 1995 members of the Japanese Buddhist sect Aum Shinri-Kyō (Supreme Truth) carried out a terrorist attack on the Tokyo underground using sarin, a poison gas. As a result, 13 people were killed and around 6 000 suffered the effects of gas poisoning, many of whom remain ill to this day and are even still hospitalised. It was the best known, most tragic terrorist attack using chemical weapons and was often presented as the first in history and later, in retrospect, as the only such attack. Although in the media such information was (and still is) very appealing and carrying, it is not true. Aum had made its first attempt to use sarin nine months earlier, on 27 June 1994, in the Kita-Fukashi district of Matsumoto city in Nagano prefecture. The gas sprayed there resulted in the death of seven and serious poisoning of more than 200 residents of the town[14]. American sources state, referring to testimonies of Aum members tried in the trials after the 1995 attack, that between 1990 and 1995 the sect carried out 17 attacks or attempted attacks using chemical and biological weapons: four times sarin, four times VX gas (a highly poisonous phosphorus and organosulphur chemical compound of the phosphonate type), phosgene and sodium cyanide, as well as four anthrax bacteria and

[13] T. Batchelor, *Khalid Masood. London attacker has no links to Isis or al-Qaeda, says Met Police*, „Independent", 17 III 2017, https://www.independent.co.uk/news/uk/home-news/khalid-masood-london-attack-isis-al-qaeda-no-links-police-a7652696.html [accessed:27 XII 2021].

[14] Information on this topic i.a. in.: D.E. Kaplan, A. Marshall, *The Cult at the End of the World*, New York 1996, pp. 137–146; D.W. Brackett, *Holy terror. Armageddon in Tokyo*, New York 1996, pp. 27–43.

three botulinum toxin (botulism)[15]. Today, Islamic fundamentalist groups are turning to chemical weapons.

Already in 2004, American special services alerted about the possibility of an attack on US territory, for which terrorists would use chemical weapons, even specifically pointing to chlorine, which is much more easily available than other poisonous gases (such as the sarin used by Aum), and can have comparable effects to them[16]. This was related to the chlorine tank fire in Atlanta (25 May 2004), which caused a toxic cloud to contaminate 5 miles^2 (13 km^2) of the suburb of Conyers and necessitated the evacuation of some 10,000 residents. Nine people were hospitalised with symptoms of gas poisoning[17]. Experts pointed out that although chlorine gas is easy to obtain due to its widespread use in water purification (e.g. by attacking tanker trucks or railway cars carrying it), it is just as dangerous to those attacked as it is to those who want to use it as a weapon. The American analysts did not take into account that for a suicide bomber this would not be an obstacle.

The authors of the cited analysis draw attention to the potential threat, but admit that al-Qaeda prefers to use classic explosives, such as those used in Madrid, because they are more effective than chemical weapons (193 people died in Madrid, 13 in Tokyo). They are also cheaper to produce: the cost of constructing the charges detonated in Madrid was estimated at USD 10 000, compared to the millions of dollars involved by Aum in its CBW programme[18]. And for this reason, the likelihood of terrorists using chemical weapons, like other weapons of mass destruction such as nuclear weapons, is theoretical rather than real.

In Rolf Mowatt-Larssen's 2010 work *Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality? A Timeline of Terrorists' Efforts*

[15] *Al Qaeda and the Threat of Chemical and Biological Weapons*, Stratfor Global Intelligence, 4 XII 2004, https://www.stratfor.com/analysis/al-qaeda-and-threat-chrmical-and-biological-weapons [accessed: 20 III 2015].

[16] *Chlorine as a Weapon?*, Stratfor Global Intelligence, 28 V 2004, https://www.stratfor.com/analysis/chlorine-weapon [accessed:16 III 2015].

[17] *Chlorine-tinged cloud of smoke forces evacuations east of Atlanta*", Associated Press, 25 V 2004, https://www.accessnorthga.com/detail.php?n=168143 [accessed: 22 III 2015].

[18] *Al Qaeda and the Threat of Chemical and Biological Weapons*, Stratfor Global Intelligence, 4 XII 2004, https://www.stratfor.com/analysis/al-qaeda-and-threat-chemical-and-biological-weapons [accessed: 20 III 2015].

to Acquire WMD[19] one may find information about al-Qaeda's preparations to produce weapons of mass destruction, mainly nuclear, but also chemical and biological. Already before the attacks of 11 September 2001, Midhat al-Mursi (alias Abu Khabab) organised training of members of the organisation in the use of such weapons in Afghanistan, while at the turn of 2002 and 2003 Abu Musab al-Zarkawi, bin Laden's deputy, planned to carry out attacks in Europe using ricin and cyanide. At the same time, a group operating in Bahrain was preparing a special device (Arabic: *mobtaker*, an invention) with which they wanted to spray hydrogen cyanide in the New York underground.

The year 2007 brought a series of attacks in Iraq in which chlorine-filled bombs were used. In three attacks on 16 March (two near Fallujah and one near Ar-Ramadi), 8 people were killed (including 6 US soldiers) and several hundred wounded[20]. Again near Ar Ramadi on 6 April, the detonation of a truck loaded with TNT and chlorine containers killed 27 people (this was the ninth such attack near Ar Ramadi)[21]. On 3 June, a truck filled with chlorine containers was blown up 200 metres from the entrance to the American base in Baquba (capital of Dijala province), causing gas poisoning of more than 60 soldiers.

It is interesting to note that even BEFORE this series of attacks, Stratfor analysts were asking the question, "*Chemical Strikes - the Beginning of a Trend?*"[22]. After all, a truck loaded with containers of chlorine exploded in Iraq's Ar-Ramadi on 30 January, and a similar attack took place in Al-Taji, north of Baghdad, on 20 February. These incidents were not reported by the media because they did not involve any casualties, but they allowed the authors to draw some general conclusions about the potential use of chlorine in terrorist attacks.

---

[19] R. Mowatt-Larssen, *Al Qaeda Weapons of Mass Destruction Threat. Hype or Reality? A Timeline of Terrorists' Efforts to Acquire WMD*, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge 2010, http://belfercenter.ksg.harvard.edu/files/al-qaeda-wmd-threat.pdf [accessed: 22 III 2015].

[20] *Iraq. Chlorine Attacks Kill 8, Injure Hundreds*, Stratfor Global Intelligence, 16 III 2007, https://www.stratfor.com/situation-report/iraq-chlorine-attacks-kill-8-injure-hundreds [accessed: 16 III 2015].

[21] *Iraq. Chlorine Truck Bomb Kills 27*, Stratfor Global Intelligence, 6 IV 2007, https://www.stratfor.com/situation-report/iraq-chlorine-truck-bomb-kills-27 [accessed: 16 III 2015].

[22] *Geopolitical Diary: Chemical Strikes – the Beginning of a Trend?*, Stratfor Global Intelligence, 21 II 2007, https://www.stratfor.com/geopolitical-diary/geopolitical-diary-chemical-stikes-begining-of-a-trend [accessed: 20 III 2015].

The final one was optimistic on the whole: although chlorine could indeed find use in bomb-making, it would not pose a real threat due to its low effectiveness as a lethal agent and the 'uncontrollability' of the poisonous cloud created by its spray.

And yet, after a few years, chlorine was reached for by another terrorist organisation: the Islamic State. ISIS is believed to have used chlorine charges on 15 September 2014 in the town of Duluja, north of Baghdad, while the Kurds fighting it in Iraq and Syria accuse it of using chlorine bombs at least twice against peshmerga (Kurdish fighters): on 23 January and 14 March 2015. Gen. Aziz Waisi, commander of the Zervani military police units, in an interview on 16 March 2015, complemented this information with another, saying that ISIS had used chlorine in fighting in the mountainous region of Sinjar[23]. Perhaps it was as a consequence of the January 24 incident that the Americans attacked, using drones, a convoy of cars travelling along a highway near Mosul and killed Abu Malik, the chief designer of chemical bombs for ISIS.

Terrorism in the 21st century - a new era?

Keeping to the definition of terrorism as a method of fighting to achieve political ends, which varies in time and place, the question must be asked: is this the next generation (wave) of terrorism? However, it is impossible to give a definitive answer, because the political game in which terrorism is used is not a zero-sum game. If we continue to consider terrorism as a method used exclusively by anti-state individuals/groups, then we are obviously not dealing with a new phenomenon. However, if the view is accepted that terrorism can also be used by state institutions, then the formal and legal approach to date needs to be reviewed and it should be recognised that, like war, this is another generation (wave) of terrorism.

Most attempts to define terrorism to date have firstly emphasised the use of physical violence as the sine qua non for any action to be considered terrorist (or at least as a threat), and from 1937 onwards

[23] *Update 3-Kurds report more chlorine attacks, Iraq pauses Tikrit offensive*, Reuters, 16 III 2015, http://www.reuters,com/article/2015/03/16/mideast-crisis-iraq-idUSL6N0WI1OA20150316 [accessed: 20 III 2015].

(Geneva Convention), their anti-state character[24]. Such legal regulations resulting from political calculation allowed those in power to legitimise their actions not only with the actual threat of politically motivated terrorist crime, but simply to fight the opposition. Any attempt to place terrorism differently within the legal system was doomed to failure, and sometimes those proposing such solutions were even accused of supporting terrorism. It is only in recent years that a new perspective on terrorism has emerged, recognising not only its anti-state nature. In the *Encyclopedia of Applied Ethics*[25], published in 2012, its authors write, among other things, in the entry "Terrorism":

> Terrorism is defined as a destructive method of political action which uses violence to cause fear for political ends. While some political goals may be achieved only through the use of terrorism, terrorists often kill or injure noncombatants or the innocent in order to maximize terror and to seek widespread publicity for their actions. Contemporary terrorism is often conceived in terms of war. While terrorism may be perpetrated by individuals against a state, states can enact policies of terrorism against their own citizens or subjects of another nation or country.

In the second half of the 20th century, Western European countries faced separatist terrorism (Great Britain - Irish Republican Army, IRA, Spain - Basque Country and Freedom, ETA) and ideological (left-wing and right-wing) grounds. The 1970s and 1980s saw the heyday of such groups as the Rote Armee Fraktion or Wehrsportgruppe Hoffmann in West Germany, Brigade Rosso or Ordine Nero in Italy, and many others. There was not a country in Western civilisation in those years whose security was not threatened by terrorism. After the attacks of 11 September 2001, the societies of Western countries were intimidated by the terrorism of Islamic fundamentalists. But not

---

[24] Article 2 of the *Convention on the Prevention and Punishment of Terrorism* of 16 XI 1937 considered an "act of terrorism" to be "a criminal act directed against a State with the intention or hope of creating a state of fear in the minds of individuals, groups of individuals or society as a whole", quoted in *Convention for the Prevention and Punishment of Terrorism. Opened for Signature AT Geneva, November 16, 1937*, in *Control of Terrorism: International Documents*, Y. Alexander, M.B. Browne, A.S. Nanes (ed.), preface by R.S. Cline, New York 1979, pp. 20-21.

[25] *Encyclopedia of Applied Ethics. Second Edition*, R. Chadwick, D. Callahan, P. Singer (ed.), Oxford 2012.

because it was born then (in the Middle East, Islamic organisations such as the Muslim Brotherhood, Hamas and Hezbollah, which refer to jihad, have existed and been active for decades), but because it knocked directly on their doors. Until then, Europeans and Americans had at best learned from the media about attacks carried out, for example, in Beirut on the US embassy (18 April 1983 - 63 people were killed), on US and French army barracks (23 October 1983 - 241 US and 58 French soldiers were killed) or others if they involved them. Attacks on all the others were at best noted, and sometimes omitted altogether from news services. However, on 11 September 2001 they became convinced that terrorist attacks by Islamic fundamentalists posed a direct threat to them, and the following years documented this clearly. Since that day and the declaration of war on terrorism by U.S. President George W. Bush, all terrorist attacks, no matter in which part of the world they took place, have been attributed to al-Qaeda. And other Islamic fundamentalist organisations were said to be linked to al-Qaeda (estimates put the number at several dozen[26]), operating in dozens of countries[27].

[26] According to the U.S. State Department, prior to the September 2001 attacks, groups cooperating with the Base included: the Reform Advisory Council (Sudan/Afghanistan), Asbat al-Ansar (Lebanon), Ansar al-Islam/Fighters of Islam (Iraqi Kurdistan), Harakat ul-Ansar/Mujahedin (Pakistan), Al-Badar (Pakistan), Armed Islamic Group/GIA (Algeria), Saafi Group for Proselytism and Struggle/GPSD (Algeria), Talaa'l al-Fateh (Egypt), Groupe Roubaix (France), Harakat ul Jihad (Pakistan), Jaish Mohammed (Pakistan), Jamiat- Ulema-e-Pakistan (Pakistan), Jamiat Ulema-e-Islam (Pakistan), Hezbollah (Lebanon), Hezb ul-Mujahideen/Party of the Holy Warriors (Pakistan), Al-Gama'a al-Islamiyya (Egypt), al-Hadith (Pakistan), Hamas (Palestinian Authority), Bayt al-Imam (Jordan), Islamic Holy War (Palestinian Authority), Islamic Movement of Uzbekistan (Uzbekistan), al-Jihad (Bangladesh), al-Jihad (Egypt), al-Jihad Group (Yemen), Laskar e-Toiba (Pakistan), Lebanese Guerrilla League (Lebanon), Libyan Islamic Group (Libya), Moro Islamic Liberation Front (Philippines), Guerrilla Movement (Kashmir), Abu Sajjaf (Philippines), Al-Ittihad al-Islamiya/Islamic Unity (Somalia), Jemaah Islamiyah (Indonesia), Union of the Ulema of Afghanistan (Afghanistan) - data after: Y. Alexander, M.S. Swetnam, *Sowers of death. Osama bin Laden and other heads of al-Qaida*, translated by J. Kozłowski, Warsaw 2001, p.49 and own sources.

[27] Middle East - Egypt, Iraq, Iran, Israel, Jordan, Kuwait, Lebanon, Morocco, Palestinian Authority, Saudi Arabia, Sudan, Syria, Tunisia, Turkey, United Arab Emirates, Yemen; Asia - Afghanistan, Bangladesh, China, India (Kashmir), Indonesia, Malaysia, Myanmar, Pakistan, Philippines; Europe - Albania, Belgium, Bosnia and Herzegovina, Croatia, Denmark, France, Germany, Italy, former Yugoslavia (Kosovo), Luxembourg, Netherlands, Spain, Sweden, Switzerland, United Kingdom; Commonwealth of Independent States (former USSR) - Azerbaijan, Russian

The milestones in the history of attacks in Europe in the 21st century and attributed to al-Qaeda were the attacks in Madrid on 11 April 2004, which killed 193 people and wounded more than 2 000, and the coordinated suicide attacks in London on 7 July 2005, which targeted the public transport system, killing 52 people and wounding more than 700. This was followed by a few years of pause in the attacks by Islamic terrorists on Europe, but with the rise of the Islamic State came the next wave of attacks. It was then that there was the attack in France on 7 January 2015 on the editorial board of the satirical magazine Charlie Hebdo (as retaliation for the posting of caricatures of Mohammed, 12 people were killed) and the attacks on 13 November of that year in Paris, which left 130 people dead and more than 350 injured (in terms of one-off casualties the biggest event in France since World War II)[28]. In 2016. Europeans were shocked by further attacks: on 22 March 2016 in Belgium - two at Brussels Zaventem Airport and one at the Maelbeek/Maalbeek metro station in Brussels (bombs killed 35 and injured 316), and on 14 July in Nice. There Mohamed Lahouaiej-Bouhlel drove into a crowd walking on the Promenade des Anglais, killing 86 and injuring 458. Later, there were many smaller-scale attacks, although the number has fallen since the beginning of 2020. This was not due to counter-terrorism efforts, but to the COVID-19 coronavirus pandemic, which caused potential terrorists problems if only logistically. Does this mean that the threat of terrorist attacks has diminished, because there can be no question of it disappearing altogether? From a European perspective such a thesis could perhaps be put forward, but in the case of other regions of the world it appears to be false. Admittedly, the available sources do not yet take into account the aggregate data for 2020-2021, but if we follow the reports of news agencies, we do not observe any radical decreases in the number of attacks. In the past, there were years in which the number of attacks fell by 50% compared to previous years (e.g. according to Statista,

Federation, Chechnya, Tajikistan, Uzbekistan; Africa - Algeria, Comoros, Djibouti, Eritrea, Ethiopia, Kenya, Libya, Mauritania, Nigeria, Senegal, Somalia, South Africa, Sudan, Tanzania, Uganda, Zaire; North and South America - Canada, United States of America, Argentina, Brazil, Paraguay, Uruguay - 67 (!) countries in total - data after: Y. Alexander, M.S. Swetnam, *Sowers of death...*, p.50.

[28] Description of attacks eg. https://www.britannica.com/event/Paris-attacks-of-2015 [accessed: 20 III 2015].

in 2012 there were 6771 attacks, and in 2006 - 14 371), which still does not give cause for optimism. Territorial temporal shifts in the frequency of attacks can also be observed, but the Middle East, North Africa, the Sahel, the Indian subcontinent are still the most vulnerable areas in the 21st century.

The annual Country Reports on Terrorism 2017[29] published in September 2018 by the State Department states that:

> Despite our successes, the terrorist landscape became more complex in 2017. ISIS, al-Qaeda and their partners have proven resilient, determined and adaptable, and have adapted to increased counter-terrorism pressure in Iraq, Syria, Afghanistan, Libya, Somalia, Yemen and elsewhere. [Terrorist organisations] have become more dispersed and clandestine, have begun to use the internet to inspire remote attacks by their followers, and as a result have become less vulnerable to conventional military action. Moreover, the return or arrival of new fighters engaged in combat abroad has contributed to the growth of experienced, developed and interconnected terrorist networks that can plan and execute attacks[30].

A few months later, completely ignoring the warnings of experts, in confirmation of the successes of the war on terror and the defeat of ISIS, U.S. President Donald Trump announced the withdrawal of US troops from Syria and Iraq[31], which, of course, was met with a wave of criticism and resulted in the symbolic resignation of General James Mattis as Secretary of Defence. In the report cited above, State Department analysts warned that ISIS had not abandoned its activities despite losing territory. It has resorted to new methods of exploiting its sympathisers spread around the world and using unconventional techniques to carry out attacks.

> The group encouraged sympathisers to use all available weapons - such as large vehicles - against soft targets and public spaces. Increasingly, the responsibility for deciding where, when and how to carry out an attack dissipated to homegrown terrorists inspired

[29] *Country Reports on Terrorism 2017*, United States Department of State Publication, Bureau of Counterterrorism, Washington 2018.

[30] Ibid., p. 8.

[31] These plans have already been confirmed by U.S. President Joe Biden in 2021.

> or seconded by ISIS to conduct operations far from the war zone. In 2017, we saw such attacks in Manchester, UK; Barcelona, Spain; Sinai, Egypt; Marawi, Philippines; New York and many other places[32].

Similarly, threats from ISIS were defined by another State Department Report:

> In 2019, Europe continued to face multiple terrorist threats and unrest (...). Despite the complete loss of geographic territory, ISIS continued to operate, inciting attacks on symbolic European targets and public spaces and recruiting individuals from European countries. Most of these incidents took place in Western Europe and Russia and consisted of simple actions carried out by easy-to-execute methods using commonly available tools and vehicles to injure or kill pedestrians[33].

And there is no indication that the threat of terrorist attacks by jihadist groups will diminish in the third decade of the 21st century.

Post scriptum (statistics)

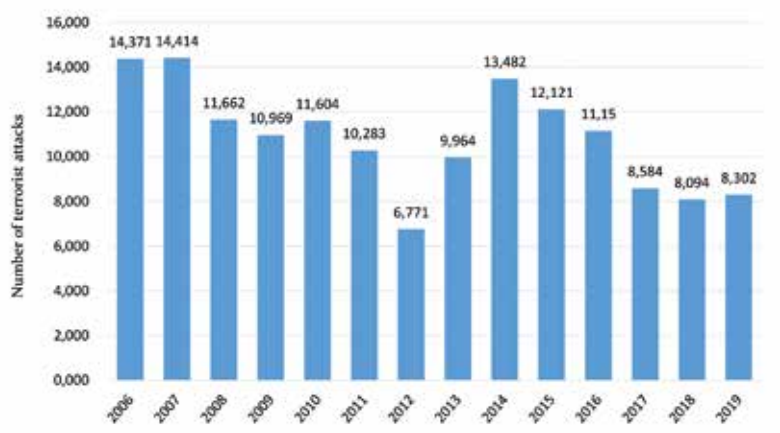


Fig. 1. Number of terrorist attacks worldwide (2006-2019).

Source: https://www.statista.com/statistics/202864/number-of-terrorist-attacks-worldwide/.

[32] Ibid.

[33] *Country Reports on Terrorism 2019*, United States Department of State Publication, Bureau of Counterterrorism, Washington 2019, p. 60.

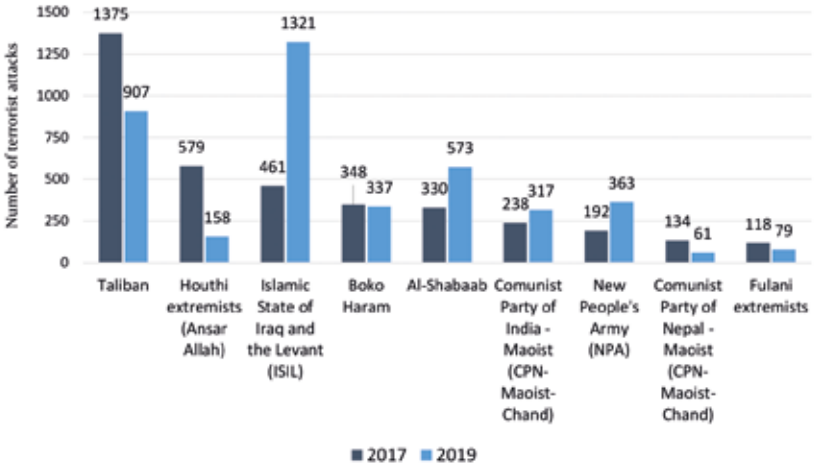


Fig. 2. Most active groups carrying out attacks in the world in 2019 by number of attacks.

Source: https://statista.com/statistics/937553/terrorism-most-active-perpetrator-groups-worldwide/.

Bibliography

Alexander Y., Swetnam M.S., *Siewcy śmierci. Osama bin Laden i inni szefowie al-Qaidy* (Eng. Sowers of death. Osama bin Laden and other heads of al-Qaeda), translated by J. Kozłowski, Warszawa 2001.

Brackett D.W., *Holy terror. Armageddon in Tokyo*, New York 1996.

Country Report on Terrorism, United States Department of State Publication, Bureau of Counterterrorism, Washington, 2005–2019.

Encyclopedia of Applied Ethics. Second Edition, R. Chadwick, D. Callahan, P. Singer (ed.), Oxford 2012.

Convention for the Prevention and Punishment of Terrorism. Opened for Signature AT Geneva, November 16, 1937, w: *Control of Terrorism. International Documents*, Y. Alexander, M.B. Browne, A.S. Nanes (ed.), foreword R.S. Cline, New York 1979.

Fukuyama F., *Koniec historii* (Eng. End of history), translated by T. Bieroń, M. Wichrowski, Poznań 1996.

Hassan R., *What Motivates the Suicide Bombers? Study of a comprehensive database gives a surprising answer*, „YaleGlobal", 3 VIII 2009.

Kaplan D.E., Marshall A., *The Cult at the End of the World*, New York 1996.

Karolczak K., *Terroryzm. Nowy paradygmat wojny w XXI wieku* (Eng. Terrorism. A new paradigm of war in the 21st century), Warszawa 2010.

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

Laqueur W., *Terrorism*, London 1980.

Laqueur W., *The New Terrorism. Fanaticism and the Arms of Mass Destruction*, London 2001.

Patterns of Global Terrorism, United States Department of State Publication, Bureau of Counterterrorism, Washington, 2001–2004.

Victor B., *Army of Roses. Inside the World of Palestinian Women Suicide Bombers*, London 2004.

Internet sources

Al Qaeda and the Threat of Chemical and Biological Weapons, Stratfor Global Intelligence, 4 XII 2004, https://www.stratfor.com/analysis/al-qaeda-and-threat--chrmical-and-biological-weapons [accessed: 20 III 2015].

Chlorine as a Weapon?, Stratfor. Global Intelligence, 28 V 2004, https://www.stratfor.com/analysis/chlorine-weapon [accessed:16 III 2015].

Chlorine-tinged cloud of smoke forces evacuations east of Atlanta, Associated Press, 25 V 2004, https://www.accessnorthga.com/detail.php?n=168143 [accessed: 22 III 2015].

Geopolitical Diary. Chemical Strikes – the Beginning of a Trend?, Stratfor Global Intelligence, 21 II 2007, https://www.stratfor.com/geopolitical-diary/geopolitical-diary-chemical-stikes-begining-of-a-trend [accessed: 20 III 2015].

Iraq: Chlorine Attacks Kill 8, Injure Hundreds, Stratfor Global Intelligence, 16 III 2007, https://www.aljazeera.com/ [dostęp: 16 III 2015].

https://www.bbc.com/news/world.

https://edition.cnn.com/.

https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/terrorism.

https://www.reuters.com/.

https://www.stratfor.com/situation-report/iraq-chlorine-attacks-kill-8-injure-hundreds [accessed: 16 III 2015].

Iraq. Chlorine Truck Bomb Kills 27, Stratfor Global Intelligence, 6 IV 2007, https://www.stratfor.com/situation-report/iraq-chlorine-truck-bomb-kills-27 [accessed: 16 III 2015].

Kiras J., „*suicide bombing*" entry, in: Encyclopedia Britannica, 13 XI 2019, https://www.britannica.com/topic/suicide-bombing [accessed: 28 XI 2021].

Mowatt-Larssen R., *Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality? A Timeline of Terrorists' Efforts to Acquire WMD*, Cambridge 2010, http://belfercenter.ksg.harvard.edu/files/al-qaeda-wmd-threat.pdf [accessed: 22 III 2015].

Update 3-Kurds report more chlorine attacks, Iraq pauses Tikrit offensive, Reuters, 16 III 2015, http://www.reuters.com/article/2015/03/16/mideast-crisis-iraq-idUSL6N0WI1OA20150316 [accessed: 20 III 2015].

DOI: 10.4467/27204383TER.22.010.15426

ORCID: 0000-0002-6685-8769

PIOTR BURCZANIUK

Legal aspects of combating terrorism in the Polish legal system against the background of challenges shaped by European legislation

Abstract

The article deals with the legal aspects of the fight against terrorism in the national legal system in the context of the challenges shaped by European legislation. The analysed issue is interesting due to the lack of broader and current analyses conducted in the field of legal sciences, devoted to the presentation and explication of legislation covering the subject matter of the fight against terrorism. This study is an attempt to fill this research gap.

In order to provide a comprehensive overview of the topic and to achieve the objectives set out in the article, the study is divided into six main parts. In the introduction, the thesis and its objectives are outlined, then sequentially: an analysis of the formation of legal regulations of domestic law aimed at counter-terrorism is made; the importance of the Act on anti-terrorist activities in the normative system of counter-terrorism in Poland is discussed, taking into account the perspective and experience of five years of its implementation; the current legal status of the European Union in the area of terrorism is presented; the perspectives and regulatory challenges of Polish law in the background of legislative activities of EU bodies are described; the considerations carried out are summarized, outlining the perspectives and regulatory challenges facing the domestic legislator in the background of the directions of the projected legislative solutions in the European Union.

Keywords:

Polish anti-terrorist legislation, European anti-terrorist legislation, Act on anti-terrorist activities, anti-terrorism, fight against terrorism

Introduction

In legal doctrine, as a result of the analysis of the types and scope of legal solutions adopted in selected countries and targeted at combating the phenomenon of terrorism, two main models are identified, i.e. the so-called formal anti-terrorist legislation and substantive anti-terrorist legislation. As P. Chomentowski points out, (...) *in the first case, we are talking about states that have one or more legislative acts in their legal system, which directly and exclusively concern the whole area of the fight against terrorism. The second case is that of a whole system of provisions on the procedures and means used in the fight against terrorism, scattered throughout various laws*[1].

Taking this dualistic division of counter-terrorism regulations as a starting point, it should be pointed out that the primary purpose of this article is to attempt a synthetic description of the scope of regulations that make up the Polish anti-terrorism system against the background of the changes that occurred in it due to the adoption of the Act of 10 June 2016 on anti-terrorist activities, which de jure replaced the material model with a formal model. However, the discussion of these regulations is not possible without reference to European Union legislation, which, as in the case of EU regulations, by the effect of direct applicability co-creates the national system or, as in the case of directives, sets the direction of national legislative actions. Finally, a reference to the legislative sources of the EU is necessary in order to grasp the ongoing or planned changes in these regulations, the scope of which increasingly touches upon the issue of threats to state security called "asymmetric" or "hybrid". The discussion of these issues will be devoted to individual parts of this study.

Historical background

As emphasised by M. Gołaszewska, (...) *the term 'terrorism' has not been legally defined in the Polish legal system.* (...) *it is rather a term of a scientific*

[1] P. Chomentowski, *Polski system antyterrorystyczny. Prawno-organizacyjne kierunki ewolucji* (Eng. Polish anti-terrorist system. Legal and organisational directions of evolution), Warszawa 2014, p. 47.

nature, depicting a state of social threat caused by an act of a terrorist nature[2]. In view of the above, it should be noted that the problem of terrorism in the domestic legal system was addressed by the legislator relatively late, as only by the Act of 27 September 2002[3]. It was not until the Act of 27 September 2002, which amended the *Act of 16 November 2000 on counteracting the bringing into financial circulation of property values originating from illegal or undisclosed sources*[4] (as of 1 December 2002), that it was supplemented with the phrase "and on counteracting financing of terrorism". As it was indicated in the justification to the draft amending act:

> (...) the proposed change in the title of the Act is related to the fact that the subject project covers the issue of counteracting the financing of terrorism. The introduction of regulations relating to this issue is one of the elements aimed at implementing the provisions of UN Security Council Resolution 1373 (2001) on combating international terrorism and the recommendations of the Financial Action Task Force on Money Laundering operating under the auspices of the OECD (FATF). The proposed solutions only relate to the issue of the General Inspector passing on to the obliged institutions information on persons who are reasonably suspected of aiding or participating in the perpetration of terrorist acts and create the possibility of initiating a procedure to block funds held in an account[5].

This Act thus introduced the first *quasi* definition of "terrorism" into the Polish legal system, recognising as "terrorist acts" offences against

---

[2] 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*, P. Burczaniuk (ed.), Warszawa 2021, pp. 46-47.

[3] *Act of 27 September 2002 amending the Act on counteracting the introduction into financial circulation of property values originating from illegal or undisclosed sources* (Journal of Laws of 2002, no. 180 item 1500).

[4] The original text was published in the Journal of Laws of 2000, No. 116, item 1216.

[5] *Explanatory Memorandum to the Government's Draft Act on amending the Act on counteracting the introduction into financial circulation of property values originating from illegal or undisclosed sources*, http://orka.sejm.gov.pl/proc4.nsf/opisy/338.htm [accessed: 22 XI 2021].

peace, humanity and war crimes, offences against public security and offences under Articles 134 and 136 of the *Act of 6 June 1997 - Penal Code*[6], hereinafter referred to as the "Penal Code". This definition was shaped objectively, referring to specific types of prohibited acts covered by the Penal Code, which, significantly, did not define the concept of a terrorist offence at that time.

In the substantive criminal law, changes in this respect were introduced by the legislator only in 2004, when by virtue of the Act of 16 April 2004[7] the Penal Code was supplemented from 1 May 2004 with the definition of a terrorist offence, understood as a prohibited act punishable by imprisonment of at least 5 years, committed with the aim of: 1) seriously intimidating a number of persons, 2) forcing a public authority of the Republic of Poland or another state or an authority of an international organisation to undertake or abandon certain actions, 3) causing serious disturbances in the system or economy of the Republic of Poland, another state or an international organisation - as well as a threat to commit such an act. Furthermore, changes have been introduced to the wording of Article 258 of the said Code which penalizes participation in an organized criminal group, extending it to a group or association aiming at committing a terrorist offence, differentiating responsibility depending on the involvement, i.e. establishment, leadership or participation in such a group. As indicated in the explanatory memorandum to the amending act, it was aimed at:

> (...) the adaptation of Polish law to the requirements of the legal instruments of the European Union, adopted in 2001-2002, under the so-called 'new acquis'. The Framework Decision of 13 June 2002 on combating terrorism obliges Member States to adopt a uniform definition of terrorist offences. The aim here is not merely to achieve a theoretical and systemic effect. The fact that an offence is classified as a terrorist offence has the effect of increasing the penalty for that offence[8].

[6] Current wording of the Act published in Journal of Laws of 2020, item 1444.

[7] *Act of 16 April 2004 amending the Act - Penal Code and certain other acts* (Journal of Laws of 2004, No. 93, item 889).

[8] *Explanatory Memorandum to the Government Draft Act on amending the Act - Penal Code and some other* acts, http://orka.sejm.gov.pl/proc4.nsf/opisy/2407.htm [accessed: 22 XI 2021].

Due to the fact that Member States were obliged to implement the legal solutions provided for in the above-mentioned Framework Decision by the end of 2002, this translated into the necessity of their adoption by Poland upon accession to the Union.

As T. Batory points out, (...) *when decoding offences of a terrorist nature on the basis of the provisions of the Penal Code, taking into account the typification of offences in the special part of this Code, it should be indicated that the following offences are involved: Art. 118 (Extermination), Art. 118a (Assassination against the population), Art. 119 (Violence and unlawful threat), Art. 120 (Means of mass destruction), Arts. 127 and 128 (Coup d'état), Art. 134 (Attempt on the life of the President), Art. 140 (Terrorist attack), Art. 148 (Assassination), Art. 163 (Causing dangerous events), Art. 164 (Imminent danger), Art. 165 (Other dangers), Art. 165a (Financing a terrorist crime), Art. 166 (Piracy), Art. 167 (Dangerous devices or substances), Art. 170 (Maritime robbery), Art. 173 (Catastrophe), Art. 174 (Danger of catastrophe), Art. 252 (Taking hostage), Art. 255a (Dissemination of content which may facilitate the commission of a criminal offence), Art. 258 § 2 and § 4 (Organised group and criminal association), Art. 259a (Crossing the border of the Republic of Poland to commit a terrorist offence)*[9].

On the basis of the analysis of the amendments to the two Acts mentioned above, a basic conclusion should be drawn, that the introduction of the problem of combating terrorism into the national legislation was not the result of internal analyses and legislative proposals, but a direct consequence of the need to adapt the Polish legal system to the requirements arising from membership in the United Nations and the ongoing process of integration with the European Union.

In this context, a similar character is acquired by a major reform[10] of the system of counteracting the use of the financial system for

[9] 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 Wewnętrznego*, P. Burczaniuk (ed.), Warszawa 2021, pp. 73-74.

[10] Amended by the *Act of 25 June 2009 amending the Act on counteracting the introduction into financial circulation of property values originating from illegal or undisclosed sources and counteracting the financing of terrorism, and amending certain other acts* (Journal of Laws of 2009, No. 166, item 1317).

the purpose of money laundering and terrorist financing, carried out in 2009, taking into account in the national legal regulations the requirements introduced by Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005[11] and Commission Directive 2006/70/EC of 1 August 2006 establishing implementing measures for Directive 2005/60/EC[12]. Pursuant to this reform, in the first of the analysed Acts, the definition of the term "terrorist act" was repealed and the term "financing of terrorism" was introduced as a prohibited act - introduced as a new one - in Article 165a of the Penal Code. As indicated in the explanatory memorandum to the reform law, (...) *the requirement to criminalize the financing of terrorism is provided for in the International Convention for the Suppression of the Financing of Terrorism, which has been ratified by Poland* (...). *The issue of terrorist financing is also addressed by Directive 2005/60/EC. In this respect, the above regulation is not only aimed at full implementation of the Directive, but also at unifying the application of international standards*[13]. Analysing the changes in the branch of criminal law aimed at counteracting terrorism, it should be noted that by virtue of the amendment[14] which entered into force on 14 November 2011, the legislator added to the Penal Code, in Article 255a, a new type of offence aimed at disseminating content which may facilitate the commission of an offence of a terrorist nature. The introduction of these changes, as before, resulted from the need to implement EU regulations, in this case Council Framework Decision 2008/919/JHA of 21 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism, extending the catalogue of "offences connected with terrorist activity" to include the offences of incitement to commit a terrorist offence, recruitment for terrorism and training for terrorism.

[11] OJ EU L 309/13 of 24 XI 2005.

[12] OJ EU L 214/29 of 4 VIII 2006.

[13] *Explanatory Memorandum to the Government's Draft Act on amending the Act on counteracting the introduction into financial circulation of property values originating from illegal or undisclosed sources and on counteracting the financing of terrorism and amending some other laws,* http://orka.sejm.gov.pl/proc6.nsf/opisy/1660.htm [accessed: 22 XI 2021].

[14] *Act of 29 July 2011 amending the Act - Penal Code, the Act - Penal Procedure Code and the Act on Liability of Collective Entities for Acts Prohibited under Penalty* (Journal of Laws of 2011, No. 191, item 113).

In addition to the two legislative acts analysed above, an important place in the national legal regulations on the phenomenon of terrorism was taken by the Act on crisis management, adopted on 26 April 2007, which defined the authorities competent in matters of crisis management and their tasks, including in the prevention, prevention and elimination of consequences of terrorist events. Importantly, by virtue of the amendment[15] of this Act, which entered into force on 19 September 2009, the scope of its legal definitions was extended to include the notion of an 'event of a terrorist nature', under which a situation arising as a result of an act specified in Article 115 § 20 of the Penal Code or a threat of such an act, which could lead to a crisis situation, was understood. In addition, Article 12a was added to the Act, which regulated cooperation in preventing, preventing and removing the effects of terrorist incidents between public administration bodies and owners and subsidiaries of critical infrastructure facilities, installations or equipment. Under this provision, the role of government administration bodies competent in recognising, preventing and combating threats was emphasised, including the special role of the Head of the Internal Security Agency, who was given statutory authority to give recommendations on the protection of critical infrastructure to bodies and entities threatened by acts of a terrorist nature, as well as to transfer to those entities the necessary information to counteract such threats, also obtained in the course of operational activities[16].

It should be added that the issue of terrorist threats was also noticeably taken up by the legislator in the regulations on states of emergency. The *Act on the state of emergency of 21 June 2002*[17] in its original wording, in art. 2 indicated that the justification for the request to the President of the Republic of Poland to impose a state of emergency was the occurrence of a situation of a particular threat to the constitutional system of the state, security of citizens or public order, including those caused by terrorist actions, which

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

[16] Cf. *Explanatory Memorandum to the Government's Draft Act on Amendments to the Crisis Management Act,* http://orka.sejm.gov.pl/proc6.nsf/opisy/1699.htm [accessed: 22 XI 2021].

[17] Original text published in Journal of Laws of 2002, No. 113, item 985.

could not be removed by the use of ordinary constitutional means. Similarly, the *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*[18] in Article 2 of its original version provided the basis for the President of the Republic of Poland to introduce, at the request of the Council of Ministers, martial law in a part or in the entire territory of the state in the event of an external threat to the state, including one caused by terrorist actions, an armed attack on the territory of the Republic of Poland or when an international agreement imposes an obligation of joint defence against aggression.

The subject matter of terrorist threats is also important in the constitutional legislation of the legal protection authorities, in particular in the *Act on the Police of 6 April 1990*, the *Act on the Border Guard of 12 October 1990*, the *Act on the Internal Security Agency and the Foreign Intelligence Agency of 24 May 2002*, hereinafter referred to as the "Act on the ABW and the AW", as well as in other acts of law covering selected aspects concerning a given type of threats[19], approaching the problem of counter-terrorist activities from the perspective of the scope of tasks entrusted to a given service and the powers granted to it, as well as the principles of cooperation and exchange of information.

Detailed operating procedures, in turn, were included in internally binding legal acts and more informal documents created both at the level of the Council of Ministers or individual ministries and services and institutions, as well as in agreements of an administrative nature between them. Significant tasks related, inter alia, to the development of draft standards and procedures in the field of combating terrorism and applying to relevant ministers in order to take legislative action to improve the methods and forms of combating terrorism have been performed by the existing since 25 October 2006 Interministerial Team for Terrorist Threats[20], acting as an auxiliary body of the Council of Ministers.

[18] Original text published in Journal of Laws of 2002, No. 156, item 1301.

[19] A detailed list of basic laws regulating the scope of tasks performed with regard to particular types of terrorist threats by relevant entities was attached as Annex No. 1 to the *National Anti-Terrorist Programme for 2015-2019* (MP of 2014, item 1218).

[20] Appointed by *Order No. 162 of the Prime Minister of 25 October 2006 on the creation of the Interministerial Team for Terrorist Threats*.

An analysis of the historical development of national legislation aimed at countering terrorist threats, as outlined above, allows the conclusion that it has followed a substantive model, creating a system of provisions scattered across various laws and other normative and non-normative acts.

It should be pointed out that the described development of legal regulations of the anti-terrorist system was accompanied by a long-standing debate, *(...) whether counter-terrorism can constitute a statutory subject matter, and if so, whether counteracting this threat to security can be included in one comprehensive law*[21]. Among the attempts to develop such a law, attention should be drawn to the work of the Task Force for Systematising National Regulations and Legal Solutions Relating to Counter-Terrorism[22], which has developed a preliminary draft of assumptions for a draft law on the collection and processing of information for the purpose of identifying threats of a terrorist nature. Taking into account the recommendations of this Team, a Task Force was appointed to develop detailed assumptions for the draft act on identifying, preventing and combating terrorism[23]. *Within this body, however, it was not possible to develop the envisaged objectives, and at the political level it was decided to terminate work in this area*[24].

Due to the failure of legislative activities of the above-mentioned Groups, work began on a strategic document of a non-normative nature, relating to the prevention of and response to terrorist threats, which resulted in the adoption of the *National Anti-Terrorism*

---

[21] K. Indecki, P. Potejko, *Wstęp* (Eng. Introduction), in: *Terroryzm. Materia ustawowa?*, K. Indecki, P. Potejko (ed.), Warszawa 2009, p. 4.

[22] Appointed by *Decision No. 5 of the Chairman of the Interministerial Team for Terrorist Threats of 10 June 2008*.

[23] Appointed by *Decision No. 6 of the Chairman of the Interministerial Team for Terrorist Threats of 12 January 2009*.

[24] 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*, W. Zubrzycki, K. Jałoszyński, A. Babiński (ed.), Szczytno 2016, p. 280.

Programme for 2015-2019[25], which presents in particular the diagnosis of the phenomenon of terrorism and the anti-terrorist system of the Republic of Poland, the main objective and specific objectives of the programme and the mechanisms for its implementation.

Another decision to undertake work on a law comprehensively regulating the issues of conducting anti-terrorist activities and cooperation between authorities competent to conduct such activities was taken on 2 December 2015 at a meeting of the Interministerial Team for Terrorist Threats, while the draft developed by the Ministry of Interior and Administration in cooperation with the Internal Security Agency began government legislative work in April 2016. The draft law, which was finally adopted on 10 June 2016, changing the model of anti-terrorist legislation from a material model to a formal model, took into account the experience gathered by the teams working in 2008-2009 and created in connection with the functioning of the National Anti-Terrorist Programme.

The special significance of the Act on anti-terrorist activities in the normative system of counter-terrorism in Poland

The Act on anti-terrorist activities[26] entered into force on 2 July 2016, just before the summit of the North Atlantic Alliance member states taking place on 8-9 July 2016 in Warsaw and the World Youth Day scheduled for 26-31 July 2016. World Youth Day in Krakow, which events - as was often pointed out during legislative work - influenced the acceleration of work on the Act.

As is indicated in the doctrine:

> (...) after many years of a kind of 'legal chaos' in anti-terrorist activities - also in Poland - the need to strengthen the tools for counteracting and combating terrorist threats, as well as for responding to these threats, was perceived. (...) For many years, experts dealing with public security have pointed out that the Polish services in the event of an attack do not act as quickly

[25] *Resolution 252 of 9 December 2014 on the "National Anti-Terrorism Programme for 2015-2019"* (MP of 2014, item 1218).

[26] Original text was published in Journal of Laws 2016, item 904.

> and efficiently as their counterparts in London, Paris or Brussels. The reason for this was the lack of clear rules and procedures for responsibility for a given area of activity and the resulting chaos and dilution of responsibility[27].

In order to counteract this, the Polish legislator passed a law whose primary objective became:

> (...) to increase the effectiveness of the Polish anti-terrorist system, and thus increase the security of all citizens of the Republic of Poland, by:
> 1) strengthening the mechanisms for coordination of activities;
> 2) clarifying the tasks of individual services and bodies and the principles of cooperation between them;
> 3) ensuring the possibility of effective action in the event of a suspicion of a crime of a terrorist nature, including in the area of preparatory proceedings
> 4) providing response mechanisms adequate to the type of threats occurring;
> 5) adapting criminal provisions to the new types of terrorist threats[28].

As was clearly emphasised in the justification to the draft law:

> (...) the regulation has the character of integrating the activities of the entities of the Polish anti-terrorist system with a clear indication of responsibility in individual areas. Application of the systemic approach to the problem of terrorist threats in the Act will allow for using the potential of all services, bodies and institutions with statutory authority to carry out anti-terrorist actions. The regulation will also have a direct impact on the speed

[27] A. Tyburska, B. Jewartowski, *Ustawa antyterrorystyczna wobec zjawiska współczesnego terroryzmu* (Eng. The Act on anti-terrorist activities and the phenomenon of contemporary terrorism), in: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (ed.), Szczytno 2016, p. 263.

[28] *Explanatory Memorandum to the Government's Draft Act on Anti-Terrorist Actions and Amendments to Certain Other Laws*, https://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=516 [accessed: 24 XI 2021].

and correctness of the decision-making process at the strategic level[29].

Structurally, the Act has been divided into 7 chapters. Chapter 1 contains the most important legal definitions of such notions for the functioning of the Act as:

- "counter-terrorist activities", understood as activities of public administration bodies consisting in prevention of terrorist events, preparation for taking control over them by means of planned undertakings, response in case of occurrence of such events and removal of their consequences, including restoration of resources intended for response to them (Article 2, item 1 of the Act);
- "counter-terrorist actions", understood as actions against perpetrators, persons preparing or assisting in the perpetration of a terrorist offence referred to in Article 115 § 20 of the Penal Code, conducted in order to eliminate the direct threat to life, health or freedom of persons or property with the use of specialised forces and resources and specialised tactics of action (Article 2, item 2 of the Act);
- "place of a terrorist event", understood as the open or enclosed space in which a terrorist event has occurred or in which its effect has occurred or is expected to occur, and the space in which threats related to a terrorist event exist (Article 2, item 6 of the Act)
- "terrorist event", understood as a situation that is suspected to have arisen as a result of a terrorist offence as referred to in Article 115(20) of the Penal Code, or a threat of such an offence.

The main substantive content of the Act is contained in Chapters 2 and 4, which are structurally based on the separation of two main stages of undertaking counter-terrorist activities. The first of them, regulated in chapter 2, is the stage of prevention of terrorist events, in which responsibility and a coordinating role is assigned to the Head of the Internal Security Agency. As essential elements of the activities of this stage, the legislator considered firstly, imposing an obligation on public administration bodies, owners

[29] Ibid.

and possessors of facilities, installations, devices of the infrastructure of public administration or critical infrastructure - to cooperate with bodies, services and institutions competent in matters of security and crisis management in the performance of anti-terrorist activities, and in particular to immediately provide the Head of the Internal Security Agency with information concerning threats of a terrorist nature to the infrastructure of public administration or critical infrastructure in their possession, including threats to the functioning of energy, water and sewage systems and networks, as well as heating systems and data communications systems important from the point of view of national security. At the same time, the Head of the ABW received a number of new powers, including in particular:

- issuing orders to authorities and entities which are endangered by these events, aiming at counteracting the threats, their removal or minimisation, as well as providing them with information necessary for achieving this goal (Art. 4 of the Act);
- coordination of analytical and information activities undertaken by special services and coordination of the exchange of information (its collection, processing and analysis) provided by the Police, Border Guard, the Marshal's Guard, the State Protection Service, the State Fire Department, the General Inspector of Financial Information, the National Revenue Administration, the Military Police and the Government Centre for Security, concerning events of a terrorist nature and data on persons connected with terrorist activities, which are classified in accordance with the socalled catalogue of incidents of a terrorist nature, specified in the *Regulation of the Minister of Internal Affairs and Administration of 22 July 2016 on the catalogue of incidents of a terrorist nature*[30] (Art. 5 of the Act);
- coordination of operational and exploratory activities concerning incidents of a terrorist nature, undertaken by special services and the Police, Border Guard, National Revenue Administration and Military Police, as well as issuing recommendations to these services aimed at removing or minimising the terrorist threat that has occurred (Art. 8 of the Act);

[30] Journal of Laws 2017, item 1517, as amended.

- maintaining a list of persons connected with terrorist activities and providing information from that list, also in the form of current analyses of the state of the threat of a terrorist event (Art. 6 of the Act)
- managing covert operations with regard to foreigners in the scope of obtaining and recording the contents of conversations conducted with the use of technical means, images or sounds of persons from premises, means of transport or places other than public places, the contents of correspondence and data contained on computer data carriers, telecommunication terminal equipment, information and data communications systems (Art. 9 of the Act)
- free access to data and information collected in public registers and records, as well as to images of events recorded by image-recording devices placed in public premises, along public roads and other public places (Art. 11 of the Act)
- empowering officers of the Internal Security Agency, the Police and the Border Guard to take fingerprints, record facial images and collect DNA material (Art. 10 of the Act).

Moreover, the Act introduces solutions facilitating secondment of employees or officers 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 the ABW, which is of utmost importance from the perspective of organisation and operation of the Counter-Terrorism Centre of the ABW[31], i.e. the statutory organisational unit of the ABW, responsible for recognising terrorist threats and performing its tasks in close cooperation with other state services and institutions and international organisations[32].

It should be added that the Act introduced, in Chapter 3, the possibility for the Prime Minister to introduce one of the four alert levels and CRP alert levels, which are characterised by the value of universally applicable information directed, in addition to bodies,

[31] *Order No. 163 of the Prime Minister of 26 September 2018 on granting the statute of the Internal Security Agency* (MP of 2018, item 927).

[32] Cf. *Zwalczanie terroryzmu* (Eng. Combating Terrorism), https://www.abw.gov.pl/pl/zadania/zwalczanie-terroryzmu/5,Zwalczanie-terroryzmu.html [accessed 24 XI 2021].

services and institutions, also to other organisational units and society. This system has been largely transposed from the previously applicable Annex No. 1 to the *Order No. 18 of the Prime Minister of 2 March 2016 on the list of undertakings and procedures of the crisis management system*[33]. *The use of a catalogue of alert degrees results from Poland's obligations as a member of the North Atlantic Treaty Organisation (NATO)*[34].

The second stage of undertaking counter-terrorist activities, regulated in Chapter 4 of the Act, was considered to be the stage involving preparation for taking control of terrorist events by means of planned undertakings, response in the event of the occurrence of such events and restoration of resources intended for responding to such events, in which responsibility and coordination role was assigned to the minister in charge of internal affairs. The legislator defined the notion of a person in charge of counter-terrorist activities undertaken by competent services or bodies within the framework of their statutory competence on the place of an event of a terrorist nature, who becomes a representative of the Police Commander-in-Chief (or a representative of the Minister of National Defence - in the case of an event on the territory of military areas). The leader of anti-terrorist activities so appointed has gained the right, when justified by the situation on the site of an event of a terrorist nature, to, inter alia ordering the evacuation of persons or property from the place of a terrorist event and its surroundings to a designated place, facility or area, and stopping or limiting vehicle traffic or rail traffic in the place of a terrorist event and its surroundings, or demanding free use of real estate or free takeover for use of movable property, including objects and equipment, or demanding assistance from institutions, organisations, entrepreneurs and natural persons or giving instructions to them. Furthermore, within this stage, the Act has established the possibility of prohibiting gatherings or mass events in the area or facility covered by the alert level, on the principles laid down in Article 21. The legislator has also provided for the possibility of using the Armed Forces of the Republic of Poland to assist police units in the event of the introduction of the third or fourth alert level, on the principles laid down in Article 22. Special use of firearms means the possibility to use firearms against a person

[33] MP of 2016, item 233.

[34] *Explanatory Memorandum to the Government's Draft Act on Anti-Terrorist Actions and Amendments to Certain Other Laws*, https://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=516 [accessed: 24 XI 2021].

carrying out an attack or taking or holding a hostage, which may result in death or a direct threat to life or health of this person if it is necessary to counteract a direct, unlawful and violent attack on human life or health or to release a hostage and the use of firearms in a way causing the least possible harm is insufficient and counteracting such an attack or releasing a hostage in another way is impossible.

In Chapter 5 of the Act, the legislator introduced special provisions concerning the pre-trial stage of criminal proceedings, concerning the special mode of performing procedural actions, searching premises or detaining a person suspected of terrorist offences, as well as drafting a decision on presenting charges and ordering pre-trial detention.

The Act also introduced numerous changes in the competences and pragmatic provisions of legal protection bodies, which are mainly a consequence of the directional solutions introduced in the Act based on the separation of two main stages of undertaking anti-terrorist activities. In particular, it should be noted that as part of these changes, a new type of offence was added to the Penal Code, by means of Article 259a, in the form of an offence of crossing the border of the Republic of Poland in order to commit a terrorist offence and, by means of Article 259b, the institution of extraordinary mitigation of punishment or conditional suspension of the execution of punishment in relation to the perpetrator of the above offence who voluntarily abandoned the commission of, inter alia, a terrorist offence[35]. Furthermore, by virtue of amendment provisions included in the Act, the Act on the ABW and the AW has been substantially amended, i.a:

- by extending the ABW competence by identification, prevention and detection of threats to the security of information and communication systems vital for the continuity of the functioning of the state, as specified in Art. 5 sec. 1 item 2a of the ABW and the AW Act;
- by introducing the ABW's authorisation to conduct the so-called secret cooperation with a perpetrator of an espionage offence or a suspect of a terrorist offence;

[35] The wording of Article 259a and Article 259b was amended as of 22 June 2021 by virtue of Article 1, point 2 of the *Act of 20 April 2021 amending the Act - Penal Code and some other acts* (Journal of Laws of 2021, item 1023). They removed the phrase "on the territory of another state" and changed the penalty for the offence under Article 259a to imprisonment from 3 months to 5 years.

- by giving the ABW the power to access bank secrecy (Art. 34a of the Act on the ABW and the AW);
- by adding a series of ABW powers in the area of information and communication security, i.e:
  a) assessing the security of ICT systems (Article 32a of the ABW and the AW Act);
  b) providing, at the request of the Head of the ABW, information on the construction, functioning and principles of operating ICT systems by the entities referred to in art. 5 sec. 1 item 2a of the ABW and AW Act (art. 32b of the ABW and the AW Act);
  c) blocking the availability of specified IT data or IT services in the ICT system, connected with an event of a terrorist nature (Article 32c of the ABW and the AW Act);
  d) keeping of a register of events violating the security of IT systems (Article 32d of the ABW and the AW Act);
  e) issuing recommendations by the Head of the ABW with a view to improving the security level of IT systems (art. 32e of the ABW and the AW Act).

It should be pointed out that since the date of enactment of the Act on anti-terrorist activities, it has been amended six times, and the amendments were aimed primarily at adjusting it to reorganisation and changes in individual services.

The Act on anti-terrorist activities shaped in this way has received a positive reception and international evaluation, including, among others, being presented in 2018 by Jukka Savolainen, Director of Resilience at the European Centre of Excellence against Hybrid Threats in Helsinki (Hybrid CoE), as an exemplary case in terms of legislative solutions that can serve as a model solution 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. *Undoubtedly, positive evaluations of the Act on anti-terrorist activities on international forums and its impact on the shaping of European legislation is an undoubted success and a reason for satisfaction for the authors of the Act*[36].

Summing up the description of legal solutions introduced by the Act on anti-terrorist activities, it should be emphasised once

[36] S. Żaryn, *Polska antyterrorystycznym wzorem* (Eng. Poland as an anti-terrorist model), Portal wgospodarce.pl, https://wgospodarce.pl/opinie/58189-polska-antyterrorystycznym-wzorem [accessed: 25 XI 2021].

again that it changed the national model of anti-terrorist legislation from a dispersed substantive model to a concentrated formal model. In such a way, this law has become, together with the new Law on Anti-Money Laundering and Financing of Terrorism passed on 1 March 2018[37], the source of Polish regulations that directly shape the legal core of the counter-terrorism area.

European law and terrorism - state of play

Counter-terrorism is an important issue covered by European Union legislation. However, specifying and analysing the scope of the impact of this legislation is not easy, in particular due to the nature of the sources of European Union law.

It should be recalled that the sources of EU law include, in the first place, the so-called primary law, consisting of the treaties concluded by the Member States, among them both the founding treaties of the European Communities and the European Union (i.e. the Treaty of Paris of 1951, the Treaties of Rome of 1957 and the Maastricht Treaty of 1992) and the so-called revision treaties, i.e. the agreements concluded between Member States amending and supplementing the founding treaties, as well as the accession treaties (on the accession of individual states to the EU). It should be added that primary law also includes the annexes (in the form of protocols) attached to these agreements, general principles of law and the Charter of Fundamental Rights of the European Union. Secondary law, created by the Union's institutions on the basis of primary law, includes, in line with Article 288 of the Treaty on the Functioning of the European Union[38], regulations, directives, decisions, recommendations and opinions. These legal acts differ, in particular, in their force and scope: a regulation is of general

[37] Original text announced in the Journal of Laws of 2018, item 723. The primary purpose of the Act was to align Polish legislation with the provisions of *Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC*, and the revised recommendations of the Financial Action Task Force (FATF).

[38] Journal of Laws 2004, No. 90 item 864/2.

application and binding in its entirety and directly applicable in all Member States. A Directive, on the other hand, is binding, as to the result to be achieved, upon each Member State to which it is addressed, but leaves to the national authorities the choice of form and methods. A decision is binding in its entirety but is individual and specific, which means that each of them is addressed to a precise group of addressees and deals with precise matters or situations, whereas recommendations (suggesting certain actions) and opinions (containing certain assessments) have no binding force.

In light of the above, it should be noted that the European Union's counter-terrorism legislation is, firstly, differentiated by the nature of the source of law in which it is regulated, which directly translates into the extent of its impact. Secondly, there is a thematic dualism in the way in which terrorism is regulated in the European Union, with individual issues either being dealt with in a separate, thematically distinct piece of legislation, or issues being dealt with in conjunction with other security legislation.

When analysing primary legislation, it must be pointed out that the Treaty on European Union[39] refers directly to the problem of terrorism in only one place, indicating in Article 42, in conjunction with Article 41 (systematically located in section 2 on Common Security and Defence Policy), that the EU may undertake, in accordance with the principles of the United Nations Charter, missions outside its territory to preserve peace, prevent conflicts and strengthen international security. Such missions, in which it may use civilian and military means, include joint disarmament operations, humanitarian and rescue missions, military advice and assistance missions, conflict prevention and peace-keeping missions, military crisis management missions, including peacemaking and post-conflict stabilisation operations. Importantly, under the Treaty, all these missions may contribute to the fight against terrorism, including by supporting third countries in combating terrorism in their territories.

The Treaty on the Functioning of the European Union, on the other hand, deals with terrorism in much greater detail, both in Part Three, which is devoted to the Union's internal policies and actions, and in Part Five, which sets out the legal basis for the Union's external action.

[39] Journal of Laws 2004, No. 90 item 864/30.

In this respect, under Title V of Part Three of the Treaty on an Area of Freedom, Security and Justice, it is provided in Article 75 that, where necessary to achieve the objectives referred to in Article 67 (the so-called 'EU obligations') in preventing and combating terrorism and related activities, the European Parliament and the Council, acting by means of regulations in accordance with the ordinary legislative procedure, shall define a framework for administrative measures with regard to capital movements and payments, such as the freezing of funds, financial assets or economic gains belonging to, or owned or held by, natural or legal persons, groups or non-state entities. The Council, on a proposal from the Commission, shall adopt measures to implement this framework. These acts must contain the necessary provisions on legal safeguards. Significantly, on the basis of this delegation, Union bodies have issued 75 secondary acts of regulation introducing restrictive measures against selected countries, including Iran, Iraq, Congo, Belarus, Liberia, Somalia, Lebanon, Uzbekistan, among others.

Within the same Title V of Part Three of the Treaty, Article 83 indicates that the European Parliament and the Council, acting by means of directives in accordance with the ordinary legislative procedure, may establish minimum rules with regard to the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them jointly. The Treaty has included terrorism among these crimes, along with trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime. On the basis of the delegation in question, the Union bodies issued, inter alia, *Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA*[40], which is one of the most important pieces of EU secondary legislation in the field of terrorism.

This delegation also gave rise to *Council Decision (EU) 2018/889 of 4 June 2018 on the conclusion, on behalf of the European Union,*

[40] OJ EU L 88/6 of 31 III 2017.

Council of Europe Convention on the Prevention of Terrorism[41], which approved, on behalf of the Union, the Council of Europe Convention on the Prevention of Terrorism of 16 May 2005[42], for matters falling within the competence of the Union and *Council Decision (EU) 2018/890 of 4 June 2018 on the conclusion, on behalf of the European Union, of the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism*[43].

The same part of the Treaty became the setting for the rules of police cooperation in the EU, of which the establishment of Europol (European Union Agency for Law Enforcement Cooperation) is an element. Its task, under Article 88 of the Treaty, is to support and strengthen action by Member States' police authorities and other law enforcement services and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy.

Finally, in Part Five of the Treaty on the external action of the Union, there is Article 222 which establishes a so-called solidarity clause whereby the Union and its Member States act jointly in a spirit of solidarity if any Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. In this regard, the Union shall mobilise all the instruments at its disposal, including the military resources made available to it by the Member States, in order, firstly, to prevent terrorist threats on the territory of the Member States; secondly, to protect democratic institutions and the civilian population from any terrorist attack; thirdly, to assist a Member State on its territory, at the request of its political authorities, in the event of a terrorist attack. Moreover, as added in paragraph 2, if a Member State has been the target of a terrorist attack or the victim of a natural or man-made disaster, other Member States shall assist it at the request of its political authorities. To this end, the Member States shall coordinate their action within the Council. At the same time, paragraph 3 specified that, acting on a joint proposal from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy, the Council shall

[41] OJ EU L 159/1 of 22 VI 2018.

[42] OJ EU L 159/3 of 22 VI 2018.

[43] OJ EU L 159/15 of 22 VI 2018.

adopt a decision laying down the conditions for the Union to apply this solidarity clause. Such a decision was issued on 24 June 2014[44].

Turning the present considerations towards EU derived law, it should be pointed out that one of the most important - if not the most important - EU normative act touching on the issue of terrorist threats is, indicated above, *Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA*. The Directive entered into force on 20 April 2017, replacing, as its title indicates, *Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism*, which was considered to be the basis for Member States' actions to combat terrorism in the field of criminal justice. The new Directive, as indicated in its Article 1, established minimum rules concerning the definition of criminal offences and sanctions in the field of terrorist offences, offences relating to a terrorist group and offences linked to terrorist activities, as well as measures to protect, assist and support victims of terrorism. As indicated in recitals 6 to 8 of the new Directive:

> (...) Taking account of the evolution of terrorist threats to and legal obligations on the Union and Member States under international law, the definition of terrorist offences, of offences related to a terrorist group and of offences related to terrorist activities should be further approximated in all Member States, so that it covers conduct related to, in particular, foreign terrorist fighters and terrorist financing more comprehensively. These forms of conduct should also be punishable if committed through the internet, including social media. Furthermore, the cross-border nature of terrorism requires a strong coordinated response and cooperation within and between the Member States, as well as with and among the competent Union agencies and bodies to counter terrorism, including Eurojust and Europol. To that end, efficient use of the available tools and resources for cooperation should be made, such as joint investigation teams and coordination meetings facilitated by Eurojust. The global character of terrorism necessitates an international answer, requiring the Union and its Member States to strengthen cooperation with relevant third countries. A strong coordinated response and cooperation is also necessary

[44] OJ EU L 192/53 of 1 VII 2014.

> with a view to securing and obtaining electronic evidence. This Directive exhaustively lists a number of serious crimes, such as attacks against a person's life, as intentional acts that can qualify as terrorist offences when and insofar as committed with a specific terrorist aim, namely to seriously intimidate a population, to unduly compel a government or an international organisation to perform or abstain from performing any act, or to seriously destabilise or destroy the fundamental political, constitutional, economic or social structures of a country or an international organisation. The threat to commit such intentional acts should also be considered to be a terrorist offence when it is established, on the basis of objective circumstances, that such threat was made with any such terrorist aim. By contrast, acts aiming, for example, to compel a government to perform or abstain from performing any act, without however being included in the exhaustive list of serious crimes, are not considered to be terrorist offences in accordance with this Directive.

Pursuant to Article 28 of the Directive, its provisions should be implemented at the level of the relevant laws, regulations and administrative provisions of the Member States by 8 September 2018. In Poland, this Directive was implemented by the *Act of 20 April 2021 amending the Act - Penal Code and certain other acts*[45]. As indicated in the justification to the bill in question:

> (...) in view of the fact that Poland had previously implemented, inter alia, Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ EU L 164 of 22 June 2002, p. 3), concerning the same area, the vast majority of the provisions of Directive 2017/541 should be regarded as implemented. For example, in Article 115 § 20 of the Penal Code there is already a definition of a terrorist offence, in Article 165a the financing of a terrorist offence is criminalised, and in Article 258 § 2 and 4 activities within a terrorist criminal group are criminalised. As an aside, it should be mentioned that Directive 2017/541 is cross-cutting in nature and touches not only on the area of criminal law, but also on related topics such as the protection of the rights of victims of terrorism. Here too, however, the vast majority of the implementation work has already been done on the occasion

[45] Journal of Laws 2021, item 1023.

of the implementation of earlier EU instruments, such as Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime and replacing Council Framework Decision 2001/220/JHA (Official Journal of the EU L 315 of 14 November 2012, p. 57). Moreover, some of the postulates contained in the Directive do not require legislative measures, but only organisational ones[46].

The common legal framework set out by the discussed Directive 2017/541 provides a reference for the exchange of information and cooperation between national competent authorities of Member States carried out in the EU on the basis of:

- *Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States*[47]*;*
- *Council Framework Decision 2002/465/JHA of 13 June 2002 on Joint Investigation Teams*[48]*;*
- *Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences*[49]*;*
- *Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union*[50], which lays down the rules under which Member States' law enforcement authorities may exchange existing information and intelligence effectively and expeditiously for the purpose of conducting criminal investigations or intelligence operations concerning serious crime, including organised crime and terrorism;
- *Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism*

[46] *Explanatory Memorandum to the Government Draft Act on Amendments to the Act - Penal Code and certain other acts*, https://www.sejm.gov.pl/Sejm9.nsf/PrzebiegProc.xsp?nr=867 [accessed: 2 XII 2021].

[47] OJ EU L 190/1 of 18 VII 2002.

[48] OJ EU L 162/1 of 20 VI 2002.

[49] OJ EU L 253/22 of 29 IX 2005.

[50] OJ EU L 386/89 of 29 XII 2006.

and cross-border crime[51], which contains provisions in Chapter 4 on the conditions for the supply of information for the prevention of terrorist offences;
– *Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013*[52].

At the same time, at the level of the Union, the need for an effective exchange between the competent authorities of the Member States and Union agencies of information that the competent authorities consider relevant for the prevention, detection, investigation or prosecution of terrorist offences has been highlighted in recent years. These exchanges should be carried out in accordance with national law and the applicable legal framework of the Union, such as:
– *Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences,*
– *Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)*[53]*,*
– *Directive (EU) 2016/681 of the European Parliament and of the Council on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*[54].

EU legislation makes sure that the information exchange described above complies with EU data protection rules, as defined by *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection and prosecution of criminal offences and the execution of criminal penalties, on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*[55], and is without prejudice to EU rules on cooperation between national competent authorities

[51] OJ EU L 210/1 of 6 VIII 2008.

[52] OJ EU L 180/1 of 29 VI 2013.

[53] OJ EU L 205/63 of 7 VIII 2007.

[54] OJ EU L 119/132 of 4 V 2016.

[55] OJ EU L 119/89 of 4 V 2016.

in criminal proceedings contained in acts such as, inter alia, *Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 on the European Investigation Order in criminal matters*[56].

Furthermore, Member States must adopt measures to protect, support and assist in response to the specific needs of victims of terrorism, in accordance with *Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime and replacing Council Framework Decision 2001/220/JHA*[57]. At the same time, assistance to victims in pursuing their claims for compensation is to be without prejudice to, and complementary to, the assistance that victims of terrorism receive from supportive bodies in accordance with *Council Directive 2004/80/EC of 29 April 2004 relating to compensation to crime victims*[58]. It should be added that the legal order of the European Union has regulated in a subject-matter manner, through Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015[59], common provisions on the prevention of the use of the Union's financial system for money laundering or terrorist financing.

Concluding the concise - due to the requirements of this study - considerations discussing the current state of European law of an anti-terrorist nature, it should be added that it remains in line with other normative actions of the international community created in particular within the framework of the United Nations and the Council of Europe, and is in a way inspired by them. Of these various measures, the first is undoubtedly the Council of Europe Convention on the Prevention of Terrorism[60], drawn up in Warsaw on 16 May 2005, which, pursuant to Article 2 thereof, aims to strengthen the efforts of the Parties to prevent terrorism and the negative impact of terrorism on the full enjoyment of human rights, in particular the right to life, both through measures taken at national level and through international cooperation, with due regard for existing multilateral or bilateral treaties or agreements

[56] OJ EU L 130/1 of 1 V 2014.

[57] OJ EU L 315/57 of 14 XI 2012.

[58] OJ EU L 261/2 of 6 VIII 2004.

[59] OJ EU L 141/73 of 5 VI 2015.

[60] Journal of Laws of 2008, No. 161, item 998.

between the Parties. As indicated in the explanatory memorandum to the request for ratification of this Convention, it is (...) *the first instrument of international law intended to regulate comprehensively inter-State cooperation - not in the field of combating and punishing terrorist offences already committed - but in the field of preventing terrorism. Its aim is to criminalise acts which precede and prepare the commission of a terrorist act*[61].

Perspectives and regulatory challenges of Polish law against the background of legislative activities of EU bodies

Speaking about the perspectives and regulatory challenges of the Polish law against the background of the legislative activities of the EU bodies, one should start with a kind of summary of the implementation process of the provisions of the *Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism*, which should be completed by 8 September 2018. It should be noted that pursuant to Article 29 of that Directive, by 8 March 2020, the Commission was to submit a report to the European Parliament and the Council assessing the extent to which the Member States had adopted the measures necessary to implement this Directive, and a report to the European Parliament and the Council by 8 September 2021 assessing the added value of this Directive on combating terrorism. The European Commission, in an evaluation report prepared for the European Parliament on the degree of implementation and application at the national level of the so-called Anti-Terrorism Directive (dated 24 November 2021)[62], pointed to the need to establish single points of contact for victims of terrorism, which, according to the report, are still lacking in Poland, which may, in the coming future, adversely affect the process of obtaining assistance or efficient recovery of claims

[61] *Explanatory memorandum to the request for ratification of the Council of Europe Convention on the Prevention of Terrorism*, https://archiwum.bip.kprm.gov.pl/ftp/kprm/dokumenty/070423u2uz.pdf [accessed: 3 XII 2021].

[62] *Report no. 13478/21 from the Commission to the European Parliament and the Council based on Article 29(2) of Directive (EU) 2017/541 of the European Parliament and of the Ciuncil of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA*.

related to a terrorist act under the influence of which Polish citizens have suffered. The report stresses, inter alia, that the planned actions of the Commission will focus on increasing the level of protection and adopting effective measures to improve the situation of victims of terrorism.

Importantly, the document indicates that further work of the Commission will be aimed at reviewing actions to counter violent extremism in EU Member States. As part of this effort, plans are emerging for a specific discussion among Member States on the application of the implemented provisions of the Directive to violent ultra-right terrorist acts.

In outlining the prospects for the direction of EU legislative action setting trends for changes in national law, attention should be drawn to the Communication on the EU Strategy for a Security Union published by the European Commission on 24 July 2020[63]. As A. Kozioł points out, this strategy (...) *aims to support Member States in the fight against changing threats and to build resilience in the long term by combating classic and hybrid threats in the physical and digital environment*[64].

Analysing the specific considerations of the Strategy, she observes that in its point 2, entitled 'The rapidly changing threat landscape', she states. "A rapidly changing European security threat landscape" it is pointed out that:

> (...) The COVID-19 crisis has also underlined how social divisions and uncertainties create a security vulnerability. This increases the potential for more sophisticated and hybrid attacks by state and non-state actors, with vulnerabilities exploited through a mix of cyber-attacks, damage to critical infrastructure, disinformation campaigns, and radicalisation of the political narrative. At the same time, more long-established threats continue to evolve. There was a downward trend in terrorist attacks in the EU in 2019. However, the threat to EU citizens of jihadist attacks from or inspired by Da'esh and al-Qaeda and their affiliates remains high. In parallel, the threat of violent right wing extremism is also growing. Attacks

[63] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020DC0605&from=EN [accessed: 15 II 2022].

[64] A. Kozioł, *Nowy plan zwalczania terroryzmu w UE* (Eng. New plan to combat terrorism in the EU), „Biuletyn Polskiego Instytutu Spraw Międzynarodowych", 19 II 2021 r., no. 33 (2231).

> inspired by racism must be a cause for serious concern: the deadly anti-Semitic terror attacks in Halle were a reminder of the need to step up the response in line with the 2018 Council Declaration. One in five people in the EU are very worried about a terrorist attack in the next 12 months. The vast majority of recent terrorist attacks were "low tech" attacks, lone actors targeting individuals in public spaces, while terrorist propaganda online took on a new significance with the live streaming of the Christchurch attacks. The threat posed by radicalised individuals remains high – potentially bolstered by returning foreign terrorist fighters and by extremists released from prison[65].

This section also points out that (...) *criminals and terrorists find it easier to access firearms, from the online market and through new technologies such as 3-D printing*[66].

In turn, point 3 of the strategy, 'A coordinated EU response serving the whole of society', emphasises the need for all actors in the public and private sectors to work together, as it is noted that in both sectors their main players are reluctant to share security information, either for fear of compromising national security or for competitive reasons.

However, the most effective action is through cooperation. In the first instance, this means increased cooperation between Member States, including law enforcement, judicial and other public authorities, as well as working with the Union's institutions and agencies to build the understanding and communication necessary for common solutions. Cooperation with the private sector is also crucial as industry owns much of the digital and non-digital infrastructure that is necessary to effectively fight crime and terrorism[67].

The strategy clearly identifies four strategic priorities for the security union: first, a security environment that stands the test of time; second, addressing evolving threats; third, protecting Europeans from terrorism and organised crime; fourth, a strong European security ecosystem.

Under the first priority, the focus is on the protection and resilience of critical infrastructure, cyber security and the protection of public

---

[65] *Communication from the Commission on the EU Security Union Strategy, Brussels, 24.07.2020 COM(2020) 605 final*, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020DC0605&from=EN [accessed: 3 XII 2021].

[66] Ibid.

[67] Ibid.

spaces. Action to improve cyber-security points out that it must go hand in hand with the fight against terrorism, extremism, radicalism and hybrid threats, and that the solution lies in better forms of cooperation between intelligence services, the EU INTCEN and other security organisations. Speaking about the protection of public spaces, it was stressed that:

> (...) Recent terrorist attacks have focused on public spaces, including places of worship and transport hubs, exploiting their open and accessible nature. The rise of terrorism triggered by political or ideologically motivated extremism has made this threat even more acute. This calls for both stronger physical protection of such places and adequate detection systems, without undermining citizens' freedoms. The Commission will enhance public-private cooperation for the protection of public spaces, with funding, the exchange of experience and good practices, specific guidance and recommendations. Awareness raising, performance requirements and testing of detection equipment and enhancing background checks to address insider threats will also be part of the approach[68].

It was also pointed out that the drone market is constantly evolving and generates additional risks, as these devices can be used by criminals and terrorists for illegal purposes. In particular, public spaces, critical infrastructure, law enforcement agencies, national borders and even individual individuals who may be attacked using them are at risk. The European Commission notes that the measures taken by the European Union Aviation Safety Agency regarding, among others, the registration of drone operators and the mandatory remote identification of drone operators are a first step. However, further actions are necessary and should include the exchange of information, development of guidelines and good practices for common use, including by law enforcement authorities, as well as wider testing of drone protection measures.

The second priority identified actions that should be taken in the face of evolving threats. These included cybercrime, combating illegal online content and hybrid threats. Speaking about the fight

[68] Ibid.

against illegal online content, the strategy points out that many serious threats to citizens, such as terrorism among others, are mainly spreading in the digital environment, and fighting them requires concrete actions and a framework ensuring the respect of fundamental rights.

An essential first step is swiftly concluding the negotiations on the proposed legislation on terrorist content online and ensuring its implementation. Strengthening voluntary cooperation between law enforcement and the private sector in the EU Internet Forum is also key to fight the misuse of the internet by terrorists, violent extremists and criminals[69].

For Union bodies, the EU's Suspicious Content Reporting Unit at Europol is of key importance and will continue to play a key role in monitoring the online activities of terrorist groups and the response of online platforms to such activities.

A key element of the strategy in the context of terrorism is Priority 3, and in particular its first part 'Terrorism and radicalisation'. "A key element of the Strategy in the context of terrorism is Priority Three, and in particular its first part, 'Terrorism and radicalisation', which emphasises that the threat of terrorism in the EU remains high and that the main responsibility for fighting terrorism and radicalisation remains with the Member States. *However, the ever-increasing cross-border/cross sectorial dimension of the threat calls for further steps in EU cooperation and coordination. Effective implementation of EU counter-terrorism legislation, including restrictive measures, is a priority. It remains an objective to extend the mandate of the European Public Prosecutor's Office to cross-border terrorist crimes*[70].

According to the document, Union action in this field will focus on:

- countering radicalisation combined with the promotion of social cohesion at local, national and European level;
- limiting the availability of chemical, biological, radiological and nuclear (CBRN) materials and explosive precursors which could be converted into weapons for use in attacks;
- effective prosecution of perpetrators of terrorist crimes, including foreign terrorist fighters. Important in this context are the ongoing efforts to fully implement border security legi-

[69] Ibid.

[70] Ibid.

slation and to make maximum use of all relevant EU databases to exchange information on known suspects;
– developing counter-terrorism partnerships and cooperation with countries in the EU neighbourhood and beyond, drawing on the expertise developed within the EU network of security and counter-terrorism experts.

Under the fourth priority of building a strong European security ecosystem, it is emphasised that this must be based on four elements, namely cooperation and information sharing, the importance of strong external borders, enhancing security research and innovation, and skills and awareness-raising.

There is no doubt that the plan submitted by the Commission offers many new solutions that are intended to increase the effectiveness of cooperation between EU bodies and Member States. However, these measures will require multi-level regulatory action by the European Union and their subsequent implementation in the Member States, in which achieving consensus may be problematic.

Undoubtedly, proper implementation of the provisions of the *Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on countering the dissemination of terrorist content on the Internet*[71], which will enter into force on 7 June 2022, will be among such challenges. The basic assumption of this normative act is to establish a harmonised legal framework for preventing the use of the Internet to disseminate content that promotes terrorism by introducing a mechanism for issuing and verifying orders to remove content of a terrorist nature or to prevent access to it.

Significantly, in Poland the Internal Security Agency is currently, pursuant to Article 32c of the ABW and the AW Act (added by the Act on anti-terrorist activities), able to apply the so-called availability blockade, i.e. in order to prevent, counteract and detect terrorist offences and to prosecute their perpetrators, the court, on a written application of the Head of the ABW submitted after obtaining a written consent of the Public Prosecutor General, by way of a decision may order the service provider providing electronic services to block access in the ICT system to specific IT data connected to a terrorist event

[71] OJ EU L 172/79 of 17 V 2021.

or specific ICT services used or intended to be used to cause a terrorist event.

However, when analysing the regulation in question, the powers of the competent authority in this respect should be much broader and include the possibility of using both operational and legal-administrative measures within the framework of the established mechanism for safeguarding the digital market against terrorist threats. Consequently, it will be necessary to make changes to national law, including:

- the designation of the competent authority to carry out the new tasks under the Regulation, including the issuing of removal orders (Article 3 of the Regulation), the review of removal orders (Article 4 of the Regulation), the extension of the period of retention of terrorist content that has been removed or to which access has been disabled as a result of a removal order (Article 6(2) of the Regulation), the issuing of decisions on hosting providers exposed to terrorist content and supervising their implementation of specific measures (Article 5 of the Regulation), the imposing of administrative fines (Article 18of the Regulation), the publishing of a report (Article 8 of the Regulation), the transmission of annual information to the European Commission pursuant to Article 21 of the Regulation;
- the designation by the competent authority of a contact point to carry out the tasks laid down in the Regulation;
- the establishment of a complaint mechanism for the issuance of removal orders and other decisions issued by the Competent Authority in relation to the performance of the tasks set out in the Regulation;
- the introduction of provisions for the imposition of administrative fines by the competent authority for infringements as defined in the Regulation;
- the establishment of a mechanism to monitor the application of the Regulation and the transmission of annual information in this regard to the European Commission.

To sum up the considerations of this part, it should be indicated that the main axis of legislative work of the European Union in the area of counter-terrorism in the coming period will focus

on the implementation of the discussed EU strategy in the field of security union and proper implementation in the Member States of individual regulations resulting from it.

Conclusion

Summarising the considerations undertaken in this article, it should be pointed out firstly that at the national level, the Act on anti-terrorist activities introduced in 2016 changed the model of anti-terrorist legislation from a diffuse material model to a concentrated formal model. Thus, this law, together with the new Law on Anti-Money Laundering and Financing of Terrorism enacted on 1 March 2018, became the pillar of national legislation that directly shapes the core of the counter-terrorism area.

Secondly, the European counter-terrorism legislation is highly differentiated, both by the nature of the source of law - which directly translates into the scope of the power of its impact, and by the dualistic methodology of the subject way of regulating terrorism, so that individual issues are either included in a separate scope subject normative act or are included together with other regulations of the security area. They are therefore closer to the material model.

Thirdly, moving on to the level of forecasts, on the basis of the analysis of actions summarising the process of implementation of the so-called Anti-Terrorist Directive and provisions of the adopted EU strategy in the field of security union, it should be indicated that the EU legislative actions will proceed in the direction of further approximation of the legislation of particular Member States, in particular with regard to the uniform definition of such concepts as 'terrorist offence', 'offence relating to a terrorist group' and 'offence linked to terrorist activity', so that these definitions cover more comprehensively acts relating in particular to the activity of foreign terrorist fighters and issues of financing terrorism. It is also important in this regard to cover activities via the Internet, including social media. Furthermore, the cross-border nature of terrorism calls for strong, coordinated action and cooperation both within and between Member States and with and between the relevant Union agencies and bodies involved in the fight against terrorism, including Eurojust

and Europol. In addition, the global nature of terrorism requires action to be taken at international level, which means that the Union and its Member States must and will work towards closer cooperation with relevant third countries. 3. also notes that the Commission's further work is to be directed towards reviewing countering violent extremism in EU Member States, which will undoubtedly remain part of the political and legal debate, particularly given the apparent attempt to leave left-wing extremism out of the public debate.

It is important to underline that the fight against terrorism can never be considered as a closed and concluded topic; on the contrary, changes in the nature of terrorist threats force continuous efforts to identify them and, consequently, to change the legal status, both at national and international level.

Bibliography

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

Kozioł A., *Nowy plan zwalczania terroryzmu w UE* (Eng. New plan to combat terrorism in the EU), „Biuletyn Polskiego Instytutu Spraw Międzynarodowych", 19 II 2021 r., no. 33 (2231).

Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem (Eng. Polish Act on anti-terrorist activities - responding to the threats of contemporary terrorism), W. Zubrzycki, K. Jałoszyński, A. Babiński (ed.), 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.

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

Żaryn S., *Polska antyterrorystycznym wzorem* (Eng. Poland as an anti-terrorist model), Portal wgospodarce.pl.

DOI: 10.4467/27204383TER.22.011.15427

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

MARIUSZ CICHOMSKI
ILONA IDZIKOWSKA-ŚLĘZAK

Strategic level of the Polish anti-terrorist system – 15 years of the Interministerial Team for Terrorist Threats

Abstract

The aim of the article is to summarise 15 years of the functioning of the Interdepartmental Team for Terrorist Threats, established by the Order No. 162 of the Prime Minister of 25 October 2006, as well as to present the evolution of the tasks carried out by this body. The Team, acting under the chairmanship of the minister in charge of internal affairs and consisting of heads of ministries, services and other entities performing tasks related to terrorist threats, sets out the basic directions of the state's activities in the field of prevention, preparation and response to terrorist threats. As an auxiliary body of the Council of Ministers, it, inter alia, monitors threats of a terrorist nature and presents opinions and conclusions for the Council of Ministers. As part of its work, proposals are also prepared to improve methods and forms of counteracting threats of a terrorist nature and requests to the relevant authorities to undertake legislative work. However, the team's activity is not limited to the sphere of legislation and also involves, inter alia, working out practical recommendations aimed at improving anti-terrorist security of facilities which may constitute a potential target of an attack or agreeing on procedures for cooperation of relevant services, as well as preparing preventive materials addressed to various groups of recipients. The team's activities were positively evaluated, among others, during the UN expert evaluation conducted in December 2019.

Keywords:

terrorism, strategic level, coordination of services, legislation, systemic solutions

In October 2006, i.e. 15 years ago, the Interministerial Team for Terrorist Threats[1] (MZds.ZT) was established, which, despite radical changes in legal and organisational terms that have taken place in the Polish anti-terrorist system since that time, still constitutes the strategic level of that system and *ensures cooperation of the government administration in preparing for prevention of terrorist events, taking control over them by means of planned undertakings and responding to them*[2].

This article aims to summarise 15 years of functioning of the MZds.ZT, as well as to present how the tasks performed by this body have evolved depending on current needs resulting from changing threats of a terrorist nature, as well as changes in the legal environment regulating the functioning of the Polish anti-terrorist system. The Team's initiatives described in the article, changes in the principles of its operation, their conditions and evaluations formulated by external entities may provide a basis for answering questions about what kind of tasks should be the focus of activity of this body and to what extent initiatives undertaken within its framework translate into the functioning of the entire anti-terrorist system.

The legal basis for the creation of the MZds.ZT was - and still is - the general authorisation contained in the *Act of 8 August 1996 on the Council of Ministers*[3], pursuant to which the Prime Minister (PRM), on his own initiative or at the request of a member of the Council of Ministers (RM), may, by way of an ordinance, create subsidiary bodies of the Council of Ministers or the Prime Minister, and in particular opinion-making or advisory boards and teams in matters belonging to the tasks and competences of the RM or PRM. The Prime Minister, creating such auxiliary bodies, specifies their name, composition,

---

1 *Ordinance No. 162 of the Prime Minister of 25 October 2006 on creation of the Inter-Ministerial Team for Terrorist Threats*. Current legal status: *Order No. 162 of the Prime Minister of 25 October 2006 on the creation of the Inter-Ministerial 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.

2 Ibid, § 2(1).

3 Pursuant to Article 12(1)(3) and (2) of that Act (i.e. Journal of Laws of 2021, item 178, as amended).

scope of activity and procedure. Therefore, the Interministerial Team for Terrorist Threats was not created on the basis of a specific legal norm embedded in the legislation on terrorist threats, but a general norm constituting the basis for the creation of various types of auxiliary bodies.

As mentioned above, the MZds.ZT is perceived as a strategic level of the Polish anti-terrorist system. Although this term does not have a direct normative basis, it is used both in analytical documents and formal governmental documents, as well as during international evaluation missions concerning the assessment of various aspects of Poland's preparedness to deal with terrorist threats, such as, for example, evaluations conducted by the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL, operating at the Council of Europe. On the other hand, an example of a formal document of governmental nature defining MZds.ZT as a strategic level of the Polish anti-terrorist system may be the *National Anti-Terrorist Programme for 2015-2019*, which was adopted on the basis of the *Act of 6 December 2006 on the principles of development policy*[4] as a resolution of the Council of Ministers[5]. Pursuant to the provisions of the Programme:

> The anti-terrorist system of the Republic of Poland adopted in Poland can be divided into three levels:
> - strategic - under which key actions of a systemic nature are taken by the Prime Minister and the Council of Ministers with respect to counter-terrorist protection of the country. Creating a national anti-terrorist policy is also the task of consultative and advisory bodies, i.e. the Interministerial Team for Terrorist Threats, the Special Services College and the Government Crisis Management Team (RZZK). A special role in the system is also played by the minister relevant for internal affairs,
> - operational - which performs tasks aimed at coordination of information exchange between particular services and institutions comprising the anti-terrorist system of the Republic of Poland, as well as current monitoring

[4] Pursuant to Article 19(2) of that Act (Journal of Laws of 2021, item 1057).

[5] *Uchwała nr 252 Rady Ministrów z dnia 9 grudnia 2014 r. w sprawie „Narodowego Programu Antyterrorystycznego na lata 2015–2019"* (Eng. Resolution No. 252 of the Council of Ministers of 9 December 2014 on the "National Anti-Terrorism Programme 2015-2019"), MP of 2014, item 1218.

and analysis of threats of a terrorist nature. Tasks on this level are coordinated by the Counter-Terrorism Centre of the Internal Security Agency and in relation to issues connected with crisis management by the Government Centre for Security (RCB),
- tactical - performed by individual services, bodies and institutions within the scope of competence of the anti-terrorist protection of the country[6].

As indicated in further provisions of the Programme, clarifying the role of the MZds.ZT as the strategic level of the anti-terrorist system:

> An important role in terms of determining the basic directions of the state's activities in the area of prevention, preparation and response to terrorist threats is played by the Interministerial Team for Terrorist Threats, which is an auxiliary body of the Council of Ministers. The tasks of the Team include, inter alia, monitoring threats of a terrorist nature, their analysis and assessment, as well as presenting opinions and conclusions to the Council of Ministers. An important task of the Team is also initiating, coordinating and monitoring activities undertaken by relevant government administration bodies in the field of preventing, preparing for and responding to terrorist threats. Within the framework of the works conducted, proposals are also prepared to improve the methods and forms of counteracting threats of a terrorist nature, together with the possibility of requesting the relevant authorities to undertake legislative works. The Chairman of the MZds.ZT may appoint, from among its members and persons invited to participate in its work, task forces in an advisory capacity in order to implement specific tasks[7].

As indicated in the introduction, the MZds.ZT was established in a radically different organisational and legal environment of the Polish anti-terrorist system. This organisational environment, understood for the purpose of this study as the institutional framework of the system, had, in comparison to the present state, significant limitations in terms of mechanisms for coordination and support of cooperation of services and other entities in relation to terrorist threats. Using the above quoted distinction of three levels in the anti-terrorist system, it should

[6] Ibid.

[7] Ibid.

be stressed that at that time there was no Counter-Terrorism Centre of the Internal Security Agency, ensuring coordination of cooperation and exchange of information on a 24-hour basis with the use of information resources of all participants in the anti-terrorist system, or the Government Centre for Security as a unit supporting exchange of information on threats from the perspective of crisis management. From the legal perspective, on the other hand, it should be noted that not only the scope of powers and the manner of defining the tasks of individual services was narrower and less detailed, but above all there was no law normalizing the key coordination mechanisms, which only years later, from the perspective of the moment the MZds.ZT was established, became the *Act of 10 June 2016 on anti-terrorist activities*[8].

In the context of systemic differences, the tasks ascribed to the MZds. ZT have also undergone changes over the years. Over time, those tasks connected with monitoring and forecasting threats have become less important, while those aimed at undertaking initiatives of a systemic nature have gained in importance. The very manner of defining these tasks has also changed, being adapted to the terminology used in the Act on counter-terrorist activities. These changes are presented in the table below.

Table 1. Evolution of tasks of the MZds.ZT

MZds.ZT in 2006	MZds.ZT in 2021	Comments
Purpose of the appointment		
The team ensures the interaction of government administration in the field of recognition, prevention and combating terrorism.	The team ensures cooperation of the government administration in preparation for preventing, taking control of and responding to terrorist events through planned undertakings.	Terminology has been aligned with the Act on anti-terrorist activities.
Tasks		
Monitoring terrorist threats, analysing and evaluating them and providing opinions and conclusions to the Council of Ministers.	Monitoring terrorist threats, analysing and evaluating them and providing opinions and conclusions to the Council of Ministers.	No changes have been made in this respect.

[8] Journal of Laws of 2021, item 2234.

Drafting counter-terrorism standards and procedures, in particular standards for assessing the presence of a threat and determining its level.	Drafting standards and procedures for responding to terrorist incidents.	Terminology has been aligned with the Act on anti-terrorist activities, hence the change of the word „combat" to „response" - the Act on anti-terrorist activities distinguishes four phases of activities - prevention, preparation, response and recovery. Reference to the development of standards and procedures for assessing the occurrence of a threat and determining its level has been dropped - this issue has been standardised in the Act on anti-terrorist activities.
Initiating, coordinating and monitoring the activities undertaken by the competent government administration bodies, in particular in the field of the use of information and the recognition, prevention and combating of terrorism.	Initiating, coordinating and monitoring the activities undertaken by the relevant governmental authorities in preparation for preventing, taking control over and responding to terrorist events through planned undertakings.	Terminology and scope have been aligned with the Act on anti-terrorist activities.
Proposing to the relevant ministers to take legislative action to improve the methods and forms of combating terrorism.	Developing proposals to improve the methods and forms of preventing, preparing to take control of and responding to terrorist incidents, and requesting the competent authorities to undertake legislative work in this regard.	The scope of the task has been clarified and the terminology and scope has been brought into line with the Act on anti-terrorist activities.
Organising cooperation with other countries in the fight against terrorism and coordinating the exchange of information and the organisation of joint operations.	Not tasks determined	The coordination of information exchange takes place on the operational level of the anti-terrorist system and, on the basis of the Act on anti-terrorist activities, constitutes the task of the Head of the Internal Security Agency - Article 4-8 of the Act. On the other hand, cooperation with other countries is carried out by individual services and other entities of the system both by way of direct contacts within the framework of bilateral cooperation with partner services, as well as through bodies and agencies of international organisations selected for these issues.

Initiating counter-terrorism training and conferences	Not tasks determined	The task has been abandoned - this issue is the domain of individual services and institutions, and not of an auxiliary body of the Council of Ministers. In order to implement the main training initiatives, the ABW's Terrorism Prevention Centre of Excellence (TP CoE) was established - its creation is directly in line with Article 3.1 of the Act on counter-terrorist activities, indicating the Head of the ABW as responsible for preventing anti-terrorist threats.

In the period of functioning of the MZds.ZT its composition was also adjusted, on the one hand - which is obvious - to the changing organisational structure of public administration (for example, transformation of the Customs Service into the National Revenue Administration, transformation of the Government Protection Bureau into the State Protection Service or establishment of the Government Centre for Security), and, on the other hand, which is more important, it was supposed to correspond to newly defined needs resulting from an increasingly broader approach to the issue of terrorist threats. Currently, the composition of the MZds.ZT consists of:

- Chairman - the minister in charge of internal affairs;
- Deputies - minister in charge of public finance, minister in charge of financial institutions, minister of national defence, minister in charge of foreign affairs, minister of justice, as well as minister - member of the Council of Ministers, coordinator of Special Services;
- Secretary - a person appointed by the Chairman of the Team from among the employees of the office serving the minister in charge of internal affairs;
- Members:
  - Secretary of State or Undersecretary of State appointed by the minister in charge of internal affairs, supervising the conduct of affairs covered by the section of government administration - internal affairs within the scope of security and public order protection,

- Secretary of State or Undersecretary of State appointed by the minister in charge of internal affairs, supervising the conduct of affairs falling within the section of government administration - internal affairs with respect to crisis management, fire protection and civil defence,
- Secretary of the Special Services College or a person substituting them,
- Head of the National Civil Defence or their deputy,
- Head of the Internal Security Agency or their deputy,
- Head of the Foreign Intelligence Agency or their deputy,
- Commander of the State Protection Service or their deputy,
- Police Commander-in-Chief or their deputy,
- Commander-in-Chief of the Border Guard or their deputy,
- Commander-in-Chief of the State Fire Service or their deputy,
- Chief of the General Staff of the Polish Armed Forces or their deputy,
- Armed Forces Operational Commander or their deputy,
- Head of the Military Intelligence Service or their deputy,
- Head of the Military Counterintelligence Service or their deputy,
- Chief Commander of the Military Police or their deputy,
- General Inspector of Financial Information or a person substituting them,
- Head of the National Fiscal Administration or their deputy,
- Director of the Government Centre for Security or a person substituting them.

A national prosecutor (or their representative) is invited to participate in the work of the Team as a member. A representative of the National Security Bureau also participates in the meetings.

Composition, in relation to that of 2006, has been expanded in particular to include the Minister of Justice, the Chief of the General Staff of the Polish Armed Forces, the Armed Forces Operational Commander, the Director of the Government Centre for Security, the Secretary of the Special Services College and the national prosecutor invited to participate in the sessions. Thus, the participation of the Ministry of Justice, which was not initially taken into account, was ensured and the participation of representatives of the prosecutor's

office was formalised, which is particularly important in the area of creating penal policy with regard to penalisation of crimes related to terrorist threats (actually, the activity of the MZds.ZT translated into changes in the Penal Code). The participation of the representatives of the Ministry of National Defence was also extended through the direct involvement of the representatives of the Armed Forces of the Republic of Poland.

From the perspective of 15 years of functioning and after summarising the activities of the MZds.ZT, it seems that the most significant role is played by those related to the initiation of legislative changes - some of which were fundamental for the Polish anti-terrorist system - and the implementation of common procedures and algorithms for the functioning of services and other entities, as well as the assessment of anti-terrorist security and the implementation of procedures aimed at raising their standards.

With regard to the issue of regulation, particular attention should be paid to the aforementioned Act on anti-terrorist activities, the *Act of 9 May 2018 on the processing of passenger flight data*[9] and the *Act of 17 September 2021 on amending the Act - Aviation Law and the Act on the Border Guard*[10], concerning detailed checks of aviation employees.

The Act on anti-terrorist activities entered into force on 2 July 2016, and its main objective - as stated in the justification - was to increase the effectiveness of the Polish anti-terrorist system and thus increase the security of all citizens of the Republic of Poland by strengthening the coordination of the activities of services and clarifying their tasks, providing response mechanisms adequate to the type of threats occurring and the possibility of more effective action in the event of a suspicion of a terrorist offence, including in the area of pre-trial proceedings, as well as adapting criminal provisions to new types of terrorist threats.

The importance of the Act on anti-terrorist activities for the Polish anti-terrorist system is demonstrated not only by the introduction of new legal solutions, but also by its integrating nature in relation to the provisions of other acts. It is worth noting that as many as 31 other laws have been amended by the Act, which is due to the fact that despite

[9] Consolidated text: Journal of Laws of 2019, item 1783.

[10] Journal of Laws of 2021, item 1898.

its comprehensive nature, in other legal acts there remain provisions on counteracting and combating terrorism, the inclusion of which in the Act would not be justified from a legislative and functional point of view[11].

The Act on anti-terrorist activities is also viewed positively in the international arena. In December 2019, a visit of the United Nations Counter-Terrorism Executive Directorate (UN CTED) took place in Poland to evaluate Poland's implementation of UN Security Council resolutions on counter-terrorism. During the visit attention was paid to the Act on anti-terrorist activities as a document comprehensively regulating the division of responsibility in particular areas of activity, as well as to the system of alert degrees established by this act in accordance with NATO requirements. The Act on anti-terrorist activities was also highly appreciated by the members of the European Centre of Excellence for Countering Hybrid Threats in Helsinki (Hybrid CoE), who decided to present the Polish regulations as a model legislative solution on the subject.

The way in which work on the so-called Anti-Terrorist Act, or the later Act on anti-terrorist activities, was carried out shows, however, that the effect itself depends not only on the involvement of the expert level of the Interministerial Team for Terrorist Threats, but also on decisions at the political level, on which the actual adoption of the solutions proposed by the Team depends. Work on a coherent regulation normalizing anti-terrorist issues was undertaken several times and lasted many years[12].

---

[11] 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 over events of a terrorist nature and reacting in the event of the occurrence of such events in the light of 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*, W. Zubrzycki, K. Jałoszyński, A. Babiński (ed.), Szczytno 2016 pp. 281–282.

[12] Cf. W. Zubrzycki, *Dzieje ustawy Antyterrorystycznej w Polsce,* w: *Polska ustawa antyterrorystyczna…* (Eng. History of the Anti-Terrorist Act in Poland); and also 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*, in: *Polska ustawa antyterrorystyczna….*

By decision of the Chairman of the MZds.ZT of 10 June 2008, under the chairmanship of a representative of the Ministry of the Interior and Administration, a Task Force for Systematising National Regulations and Legal Solutions Concerning Counteracting Terrorism was established. Its responsibilities included a review of legal regulations on counteracting and combating terrorism, which were in force in Poland, and the development of proposals of new legal and organisational solutions on preventing and combating terrorist threats. The report on the works of the Task Force presented, inter alia, the assumptions of the draft act on collecting and processing information for the purpose of recognising threats of a terrorist nature and recommended the establishment of an inter-ministerial team to develop the above-mentioned draft act. Subsequently, having regard, inter alia, to the aforementioned recommendation, by decision of the Chairman of the MZds.ZT of 12 January 2009 the Task Force for Elaborating Detailed Assumptions to the Act on Recognising, Counteracting and Combating Terrorism, acting under the chairmanship of a representative of the Internal Security Agency, was established. Despite the recommendations presented by the Task Force, it was not decided to initiate the legislative process in order to adopt the draft act in question, neither was a draft of assumptions to the draft act developed, while the work of the Task Force was terminated by a decision of the then management of the Ministry of the Interior and Administration.

Another initiative was undertaken in connection with the increase in the terrorist threat in Europe and actions taken on the forum of the Council of Europe and the United Nations aimed at criminalising the activity of the so-called foreign fighters who undertake travel abroad to commit, plan and prepare for terrorist attacks or to participate in them, as well as to give or receive terrorist training. The Chairman of the MZds. ZT on 26 March 2015 established a Task Force for the review of legal solutions relating to terrorist threats, acting under the chairmanship of a representative of the then Ministry of the Interior. However, the purpose of this body was not to draft a comprehensive law regulating the subject matter, but to present proposals for changes to the existing legal acts. The recommendations presented by the Task Force included - in addition to the criminalisation of the activities of so-called foreign fighters - proposals of legal changes aimed at improving the coordination of services and bodies forming the anti-terrorist system.

However, it was only in 2015, as part of another initiative, that it was possible to prepare, subsequently adopted, a draft law on anti-terrorist activities. The draft was prepared by the Ministry of the Interior and Administration and the Chancellery of the Prime Minister in cooperation with the Internal Security Agency and with the support of the Task Force for the development of the concept of a comprehensive regulation on the issues of recognition, counteraction and combating threats of a terrorist nature, appointed by the Chairman of the MZds.ZT on 4 December 2015.

Another important regulation adopted, inter alia, thanks to the cooperation within the framework of MZds.ZT is the aforementioned Act on collection and processing of air passengers' data. According to its provisions, air carriers are obliged to provide the Border Guard with data on the flights of passengers using their lines. Information on passengers is processed in order to prevent, detect and combat terrorism and other crimes, and to prosecute their perpetrators. The obligation to introduce the new legislation resulted from the *EU Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*[13].

The provisions of the Act of 17 September 2021 on amending the Act - Aviation Law and the Act on Border Guard, prepared in the framework of cooperation between the Border Guard and the Ministry of Infrastructure initiated by the Mds.ZT, entered into force on 31 December 2021". Also in this case, the need to issue new regulations resulted from changes in EU law, i.e. introduced in *Commission Implementing Regulation (EU) 2019/103 of 23 January 2019 amending Implementing Regulation (EU) 2015/1998 as regards clarification, harmonisation and simplification, as well as the strengthening of certain specific aviation security measures*[14]. Appointed by the Chairman of the MZds.ZT on 2 April 2019, the Task Force for the development of new solutions in the field of background checks of aviation employees has analysed the scope of the necessary legislative and organisational and technical measures aimed at adapting the Polish legal order to the above-

[13] OJ EU L 119 of 4 May 2016, p. 132.

[14] OJ EU L 21 of 24 January 2019, p. 13.

mentioned Regulation with regard to the performance of background checks of aviation employees in the context of their criminal history, developed new procedures for the performance of these checks and a scheme for the exchange of information in this regard, and finally prepared a draft of the provisions through which these procedures will be implemented.

In addition to its significant contribution to legislation relating to threats of a terrorist nature, the activity of the MZds.ZT in the area of developing recommendations relating to the improvement of the security of specific facilities, which - due to their strategic significance for the security of the state or their key importance from the perspective of providing specific services to society, such as efficient communication - may constitute a potential target of attacks, deserves particular attention. Thus, over the past 15 years, the MZds.ZT, within the framework of the work of successive task forces appointed for that purpose, has analysed and assessed both the level of terrorist threat and the preparedness in terms of the possibility to respond to events of a terrorist nature, as well as the mechanisms related to evacuation and transmission of information in the event of threats, in relation to:

- the grounds and buildings serving the President of the Republic of Poland;
- the grounds and building of the Chancellery of the Prime Minister;
- Parliament facilities (twice in 2010 and at the turn of 2016 and 2017);
- railway stations - Warszawa Centralna and Warszawa Śródmieście, as well as the Railway Cross-City Tunnel in Warsaw (whereby the developed recommendations were forwarded to relevant entities for use also with regard to other similar facilities in the country);
- the Warsaw metro;
- nuclear facilities in Świerk.

Each time, the work involving study visits of experts to the indicated facilities resulted in recommendations concerning changes of a technical as well as organisational and procedural nature. In the case of the areas and facilities administered by the Chancellery of the Prime Minister and the Chancellery of the President of the Republic of Poland, the work resulted also in the adoption of uniform plans for the protection

of these facilities, which were the basis for the development of detailed instructions and possible additional mechanisms for cooperation of the institution responsible for protecting the most important persons in the state, i.e. the State Protection Service, with the Chancellery of the Prime Minister, the Chancellery of the President of the Republic of Poland and other relevant entities, including the Police, the State Fire Service and special services.

The recommendations developed were passed on to relevant entities and ministries for implementation, and - as far as possible - the manner and scope of their implementation was monitored on the forum of the MZds.ZT. It should be stressed, however, that some of them were addressed to entities from outside the government administration, such as, for example, in the case of the entity managing the Warsaw underground, as a result of which the MZds.ZT could only provide an advisory opinion, while it had no competence to impose the application of specific solutions related to the implementation of these recommendations.

In this context, also the work of the Task Force for the development of anti-terrorist security standards and rules of cooperation concerning critical infrastructure and the principles of performing security checks of critical infrastructure facilities in accordance with the provisions of the Act on anti-terrorist activities, established on 26 May 2017, deserves attention. It should be emphasized that the implementation of the standards and recommendations developed by the Task Force remains largely dependent on the entities managing such facilities, and due to the potentially high costs in the context of the generally low level of terrorist threat in Poland, it is not always treated as a priority.

The contribution of the MZds.ZT to the improvement of procedures of cooperation of relevant services and institutions in the context of terrorist threats is also not without significance. Prior to the entry into force of the Act on anti-terrorist activities, the document constituting the basis for the organisation of cooperation was the agreement of the Head of the Internal Security Agency, the Police Commander-in-Chief, the Commander-in-Chief of the Border Guard, the Chief Commander of the Military Police and the Commander-in-Chief of the State Fire Service of 21 January 2014, concluded on the basis of the principles developed by the Task Force, established by the decision of the Chairman of the MZds.ZT of 13 August 2012, for the development

of a proposal for an algorithm of cooperation and management at the scene of a terrorist incident. The principles worked out at that time were then, by means of the Act on anti-terrorist activities, partly incorporated into the ground of universally binding provisions of law. Moreover, as a result of the arrangements made on the forum of the MZds.ZT, a new agreement of the heads of the above-mentioned formations on cooperation at the scene of a terrorist incident was concluded on 7 March 2018 - constituting this time only a supplement at the technical and organisational level to the statutory regulations.

The work of the MZds.ZT also resulted in the *Guidelines of the Prime Minister of 31 October 2021 on the coordination of exchange of information on terrorist threats* and a catalogue of incidents and events reported to the Counter-Terrorism Centre of the ABW, which was initially adopted by a resolution of the MZds.ZT. Both these documents were used in the development of the provisions of the Act on anti-terrorist activities - currently, the catalogue of terrorist incidents is defined in the Ordinance of the Minister of Internal Affairs and Administration of 22 July 2016[15] issued on the basis of the aforementioned Act, while the coordinating role of the Head of the ABW in relation to analytical and information activities of the remaining services of the Polish anti-terrorist system results directly from Article 5(1) of the Act.

The involvement of the MZds.ZT in the development of the methodology for the examination of terrorist and disaster crime scenes and the identification of victims' bodies is also not without significance. Prepared for the first time in 2011, the methodology was subsequently evaluated within the framework of the task team established by the decision of the Chairman of the MZds.ZT on 28 July 2017. Importantly, as a result of the work of the MZds.ZT, a solution currently regulated in the aforementioned agreement of 7 March 2018 on cooperation at the scene of a terrorist incident was also adopted, consisting in the creation of a central, part-time team to support investigation activities at the scene of an incident caused by the use of an explosive material or device, including one that may contain a chemical, biological or radioactive substance or agent. The possibility of rapid deployment of a joint team consisting of experts from the Police, the Internal Security Agency, the Border Guard, the Military

[15] Journal of Laws of 2017, item 1517.

Police and the State Fire Service, acting with the support of the Public Prosecutor's Office, is an extremely important tool when such events occur. It is also indispensable to ensure possibly frequent training sessions for representatives of this team - exercises conducted so far with its participation have shown the need to continue the cooperation in question and the added value of exchanging experiences between specialists in the field of visual inspection in particular formations.

The aforementioned so-called CBRN threats - chemical, biological, radiological and nuclear, more than once constituted the subject of the work of MZds.ZT due to the complicated arrangement of the scope of responsibility of individual entities in the event of responding to this particular form of threats, characterized by a potentially unlimited and sometimes difficult to foresee scale of impact. The results of actions undertaken in this respect include the *Algorithm of conduct and cooperation in the case of receiving an unidentified package which may pose a chemical, biological or radiological threat*, as well as preventive material in the form of generally available *Procedure for an institution receiving a suspicious package*.

Anti-terrorist prevention in the past years was one of the many aspects of MZds.ZT's activity. Within the framework of the Task Force - Permanent Expert Group operating within the MZds.ZT, a government website - antiterrorism.gov.pl - was prepared and updated on an ongoing basis, with not only materials prepared on the basis of the findings of the MZds.ZT, such as the above-mentioned *Procedure for an institution receiving a suspicious package*, instruction entitled *Proceedings in the case of a terrorist attack, Alarm instruction - principles of conduct in the case of obtaining information about planting or locating an explosive device in a public utility facility*, but also handbooks addressed to specific groups of recipients, such as the handbook entitled *Principles of conduct in the case of an attacker entering the premises of an educational facility*, prepared by the Warsaw Metropolitan Police Headquarters and the Warsaw City Hall or the publication prepared by the Internal Security Agency entitled *Security of Large-Scale Commercial Facilities - Anti-Terrorist Security. Universal handbook*, but also basic information on the functioning of the Polish anti-terrorist system, as well as up-to-date information on obligatory alarm degrees or CRP alarm degrees, introduced pursuant to the provisions of the Act on anti-terrorist activities. Following the entry into force of the provisions of the A*ct*

of 19 July 2019 on ensuring accessibility to persons with special needs[16], the website previously functioning on the ABW server has been transferred as the tab *Anti-Terrorist System of the Republic of Poland*[17] to the website of the Public Information Bulletin of the Ministry of Internal Affairs and Administration, while the above-mentioned preventive materials are still available in the tab.

An important achievement of the MZds.ZT in the context of the threat related to false reports on explosive devices was development of rules for circulation of information in such situations with a coordinating role of the Central Investigation Bureau of the Police, which made it possible to identify the phenomenon of the so-called cascade reports, i.e. reports addressed to many institutions or concerning many objects at the same time. As a consequence, these actions made it possible to limit the number of evacuations which are a significant hindrance not only to the functioning of public administration entities or the judiciary but also to the private sector, involving considerable forces and resources on the part of services and resulting in financial losses or even posing a threat to life and health, as in the case of the evacuation of hospitals.

Among the many significant initiatives carried out over the last 15 years on the forum of the MZds.ZT, it is impossible to omit the issue of first preparing a draft and then coordinating the implementation of the *National Anti-Terrorist Programme for 2015-2019*.

This document, which was discussed within the framework of the Task Force - Permanent Expert Group supporting the MZds. ZT at the expert level, presented the then current level of terrorist threat, indicated - even before the adoption of the Act on anti-terrorist activities - the mechanisms for conducting its current assessment, as well as the elements conditioning the effectiveness of the functioning of the anti-terrorist system of the Republic of Poland. The programme provided for undertaking activities aimed at ensuring optimum cooperation of entities carrying out tasks with regard to counteracting and combating threats of a terrorist nature. One of the fundamental objectives of the document was also raising public awareness of threats of a terrorist nature, principles of behaviour in the event of an occurrence and forms and means of state involvement in counteracting

[16] Consolidated text: Journal of Laws of 2020, item 1062.

[17] https://www.gov.pl/web/mswia/system-antyterrorystyczny-rp [accessed: 13 XII 2021].

and combating terrorism. The specific objectives of the programme assumed streamlining the implementation by the entities of the Polish anti-terrorist system of tasks in the individual phases of crisis management and anti-terrorist activities, i.e.: prevention, preparation, response and recovery[18].

According to the mechanism of its implementation specified in the programme, the coordinator of the programme, on behalf of the Council of Ministers, was the minister in charge of internal affairs, who carried out his tasks by means of the Interministerial Team for Terrorist Threats[19]. The programme also emphasised, as it had been mentioned earlier, the role of the Interministerial Team for Terrorist Threats (MZds.ZT) in terms of initiating, coordinating and monitoring activities undertaken by relevant bodies of government administration, as well as developing proposals to improve methods and forms of combating terrorism and applying to relevant bodies to undertake legislative work in this respect, resulting from the *Order No. 162 of the Prime Minister of 25 October 2006 on the establishment of the Interministerial Team for Terrorist Threats*.

The main tool for implementing the programme and its current monitoring was the so-called *Action Plan*, being its integral part, which defined the undertakings of legislative and organisational nature (priorities) of key importance for achieving greater effectiveness of the Polish anti-terrorist system. At the same time, the *Action Plan* indicated leading entities and entities cooperating in the implementation of individual priorities. In accordance with the implementation mechanism defined in the programme itself, the heads of individual services, bodies and institutions, listed as leading entities in the implementation of individual priorities resulting from the *Action Plan*, were obliged to develop, in cooperation with the heads of cooperating entities, schedules for the implementation of each priority, including the deadlines for their planned implementation.

---

[18] Cf. *Raport o stanie bezpieczeństwa w Polsce w 2016 r.*(Eng. Report on the state of security in Poland 2016), p. 279, https://archiwumbip.mswia.gov.pl [accessed: 13 XII 2021].

[19] Cf. M. Cichomski, K. Więcek, *Narodowy Program Antyterrorystyczny na lata 2015–2019 jako operacyjno-wdrożeniowy dokument służący realizacji polityki rozwoju* (Eng. National Anti-Terrorism Programme 2015-2019 as an operational and implementation document for development Policy), „Przegląd Bezpieczeństwa Wewnętrznego" 2014, no. 11, pp. 321–322.

These schedules were then forwarded to the minister in charge of internal affairs and discussed and adopted within the MZds.ZT. The team not only monitored the implementation of individual schedules on a current basis, but also carried out an annual evaluation of the progress in implementing the programme in the form of a report discussed at a meeting of the MZds.ZT and then submitted to the Council of Ministers for information[20]. Moreover, it was at the forum of the MZds.ZT that decisions were made as to the allocation of funds from the special purpose reserve allocated for the implementation of the programme.

Among the most important results of the programme's implementation, it should be noted, in particular, the aforementioned implementation of a new model of cooperation between services in the area of assessing the reliability of information on the planting of an explosive device, the commencement of work aimed at implementing in Poland a mechanism for collecting and processing airline passenger data in accordance with the provisions of the Directive on the management of airline passenger data (PNR) for the purposes of preventing, detecting, investigating and prosecuting terrorist offences, which is finalised by the aforementioned Act on the processing of passenger name record data, implemented in 2016 a series of trainings on anti-terrorist prevention for management and teaching staff of schools, under which more than 98,000 headmasters and employees of educational institutions were trained, trainings for representatives of the industry of large-area commercial facilities on how to behave in a terrorist threat situation, trainings for directors general of government administration offices on how to behave in the case of receiving a suspicious package and how to behave in the case of obtaining information about planting an explosive device in a facility of a public institution.

At present, the works of the MZds.ZT are carried out primarily on the basis of annual schedules adopted continuously since the team was established. Some of the tasks included in them are cyclical, others result from current needs and the evolution of terrorist threats.

The former include, in recent years, the assessment and forecast of terrorist threats to the Republic of Poland and its citizens made

[20] Cf. *Uchwała nr 252 Rady Ministrów z dnia 9 grudnia 2014 r. w sprawie „Narodowego Programu Antyterrorystycznego na lata 2015–2019"* (Eng. Resolution No. 252 of the Council of Ministers of 9 December 2014 on the "National Anti-Terrorism Programme 2015-2019"), MP of 2014, item 1218.

by the ABW, the discussion of the security situation of Polish tourists in selected countries in connection with the tourist season, as well as the preparation by the Government Centre for Security of a compilation of conclusions from exercises on responding to terrorist events or the reports of the General Inspector of Financial Information on the implementation of the *Act of 1 March 2018 on preventing money laundering and terrorist financing*[21].

The last two years of the functioning of the MZds.ZT have brought a new challenge - this time of an organisational nature. The situation related to the COVID-19 pandemic has not been without impact on the functioning of the team, whose work remains largely a matter protected by law as classified. In view of the change to the virtual formula of meetings of most bodies of a similar nature to the MZds. ZT, in the case of this team, for security reasons, a decision was taken to carry out part of its work through the exchange of correspondence and to make binding decisions by circulation. The need for these changes was reflected in changes to the rules of procedure of the Team, which, despite these difficulties, has maintained continuity of its activities and implements the adopted work schedules also during the pandemic period.

During the aforementioned visit of the UN Counter-Terrorism Executive Directorate in December 2019, our country was positively assessed in terms of the adopted anti-terrorism solutions of a systemic nature, as well as with regard to the activities of individual services undertaken to combat this type of crime. UN experts highly evaluated our systemic approach to the threat, stating that although Poland faces a relatively low threat from terrorism, it nevertheless takes this threat seriously, introducing a number of legal, institutional and operational counter-terrorism measures.

It should be emphasized that such a high rating would not have been possible without the inter-institutional cooperation forum, such as the MZds.ZT, which has been operating continuously for 15 years.

To sum up, it should be emphasised that the Interministerial Team for Terrorist Threats, despite significant changes in the legal environment which have taken place since its establishment, still plays the role of a strategic body, a key one in the context of coordination

[21] Consolidated text: Journal of Laws of 2021, item 1132, as amended.

of undertakings aimed at creating legal and procedural grounds for preventing terrorist events, preparing to take control over them and responding to the occurrence of such events. This is evidenced above all by its uninterrupted activity since 2006 in the area of initiatives of a legislative and procedural nature. Particularly important from the perspective of ensuring a possibility of effective coordination of undertakings in the scope in question and enabling cooperation of a number of services and entities of the Polish anti-terrorist system is also the continuity of functioning of this body - allowing to avoid ad hoc actions undertaken without due analysis of the evolution of terrorist threats and effectiveness of regulations and procedures implemented so far.

Bibliography

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., Więcek K., *Narodowy Program Antyterrorystyczny na lata 2015–2019 jako operacyjno-wdrożeniowy dokument służący realizacji polityki rozwoju* (Eng. National Anti-Terrorism Programme 2015-2019 as an operational and implementation document for development Policy), „Przegląd Bezpieczeństwa Wewnętrznego" 2014, no. 11.

Zubrzycki W., *Dzieje ustawy antyterrorystycznej w Polsce* (Eng. The history of the anti-terrorist law in Poland), in: *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, W. Zubrzycki, K. Jałoszyński, A. Babiński (ed.), Szczytno 2016.

Internet sources

Raport o stanie bezpieczeństwa w Polsce w 2016 r. (Eng. Report on the state of security in Poland 2016), https://archiwumbip.mswia.gov.pl [accessed: 13 XII 2021].

https://www.gov.pl/web/mswia/system-antyterrorystyczny-rp [accessed: 13 XII 2021].

Legal acts

Commission Implementing Regulation (EU) 2019/103 of 23 January 2019 amending Implementing Regulation (EU) 2015/1998 as regards clarification, harmonisation and simplification, and strengthening of certain specific aviation security measures, OJ EU L 21 of 24 January 2019, p. 13.

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime), OJ EU L 119 of 4 May 2016, p. 132.

Act of 17 September 2021 on amending the Act - Aviation Law and the Act on the Border Guard, Journal of Laws of 2021, item 1898.

Act of 19 July 2019 on ensuring accessibility for persons with special needs, i.e.: Journal of Laws of 2020, item 1062.

Act of 9 May 2018 on the processing of Passenger Name Record data, Journal of Laws of 2019, item 1783.

Act of 1 March 2018 on the prevention of money laundering and financing of terrorism, i.e.: Journal of Laws of 2021, item 1132, as amended.

Act of 10 June 2016 on anti-terrorist activities, Journal of Laws of 2021, item 2234.

Act of 6 December 2006 on the principles of development policy, Journal of Laws of 2021, item 1057.

Act of 8 August 1996 on the Council of Ministers, i.e.: Journal of Laws of 2021, item 178, as amended.

Regulation of the Minister of Internal Affairs and Administration of 22 July 2016 on the catalogue of terrorist incidents, Journal of Laws 2017, item 1517.

Order No. 162 of the Prime Minister of 25 October 2006 on the creation 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.

Resolution No. 252 of the Council of Ministers of 9 December 2014 on the "National Anti-Terrorist Programme for 2015-2019", MP of 2014, item 1218.

DOI: 10.4467/27204383TER.22.012.15428

ORCID: 0000-0002-7082-8511

JĘDRZEJ ŁUKASIEWICZ

Unmanned aerial vehicles as a source of threats to the state's electricity supply infrastructure and the proposed methods of protecting this infrastructure

Abstract

Unmanned aerial vehicles pose a threat to objects important to national security. Their versatility, resulting from the characteristics of individual types of aircraft, means that the scale of their use in attacks is virtually unlimited. The electricity supply system is extremely important for state security. Due to the vastness of transmission networks and a significant number of node points of these networks, the question should be asked to what extent this system is resistant to terrorist attacks, especially those carried out with the use of unmanned aerial vehicles. In this paper, the author analyses an attack consisting in causing a short circuit of the electrical system with the use of a copper wire suspended under an unmanned aerial vehicle. The implementation of the recommended protection methods described in the paper should lead to an increased level of safety of transmission networks.

Keywords:

unmanned aerial vehicles, power grid, protection of facilities critical to national security, anti-drone prevention

Unmanned aerial vehicles (UAVs) are a source of threats to facilities important to national security. Unmanned aerial vehicles (e.g. aircraft, multirotor or helicopter) are devices that perform their missions without the presence of a pilot on board. They can attack targets, including humans, using artificial intelligence algorithms[1]. Press releases reveal further examples of the use of UAVs in warfare, but also in terrorist attacks[2], including on the electricity supply system. The aim of the analysis presented in this paper is to determine the vulnerability of the power grid to attacks carried out by unmanned aerial vehicles and to identify methods of preventing attacks carried out by such devices on power facilities in Poland. Conducting such an analysis seems justified as media reports entitle to formulate the hypothesis that the success of one such attack may cause a trend towards drone attacks on power grid facilities in Europe, including Poland.

Structure of the power grid in Poland

Electricity in Poland is produced by thermal, hydro, wind, photovoltaic, biogas and biomass power plants; some electricity is imported from abroad[3]. Electricity from the producer to the end user is transmitted through the power grid, consisting of lines and substations. Every transmission of energy generates losses. To keep these losses as low as possible, transmission networks with voltages between 220 kV and 400 kV, known as the highest voltages, are used for long-distance transmission of electricity. For transmission of electricity over distances of up to several tens of kilometres, lines with a voltage of 110 kV are used. This is a high voltage. In local distribution lines, the voltage is between 10 kV and 30 kV and this is called medium voltage. The medium voltage is transformed to a low voltage of 220/230 V or 380/400 V. The low voltage

[1] https://www.newscientist.com/article/2278852-drones-may-have-attacked-humans-fully-autonomously-for-the-first-time/ [accessed: 30 XI 2021].

[2] https://edition.cnn.com/2019/03/14/americas/venezuela-drone-maduro-intl/index.html [accessed: 30 XI 2021]; https://www.bbc.com/news/world-middle-east-59195399 [accessed: 30 XI 2021]; https://www.reuters.com/world/middle-east/iran-backed-militia-behind-attack-iraqi-pm-sources-2021-11-08/ [accessed: 30 XI 2021].

[3] *Energetyka, dystrybucja, przesył* (Eng. Energy, distribution, transmission), PTPiREE, http://ptpiree.pl/raporty/2021/raport_ptpiree_2021.pdf [accessed: 30 XI 2021].

is used by the end customer[4]. The plan of the power grid in Poland, including planned investments, is presented in Figure 1.

Fig. 1. Diagram of the power grid in Poland.

Source: https://www.pse.pl/obszary-dzialalnosci/krajowy-system-elektroenergetyczny/plan-sieci-elektroenergetycznej-najwyzszych-napiec/planowana [accessed: 30 XI 2021].

The power system in Poland consists of system substations for extra-high voltage, distribution substations for high voltage and transformer substations. According to information provided by Polskie Sieci Energetyczne SA, 281 extra-high voltage lines with a total length of 15 316 km and 109 extra-high voltage substations are currently operated in Poland. The high, medium and low voltage lines are managed by: Enea Operator, Energa-Operator, Polska Grupa Energetyczna Dystrybucja, Innogy Stoen Operator and Tauron Dystrybucja. The total

[4] https://www.pse.pl/obszary-dzialalnosci/krajowy-system-elektroenergetyczny/informacje-o-systemie [accessed: 30 XI 2021].

length of connections managed by the aforementioned operators is 169,076 km. The operation of the aforementioned lines required the construction of 111 extra-high voltage, 1,537 high voltage and 262,989 medium voltage substations[5]. The highest voltage lines and the high voltage lines are made of cables that are not insulated. Medium voltage lines are usually not insulated. Insulation is used on medium voltage lines when they run through a forest. Low voltage lines are insulated[6]. Overhead lines are equipped with remote-controlled disconnectors and short-circuit alarms, which allow a fault to be located quickly.

Damage to an electrical installation by means of an unmanned aerial vehicle

Threats to electricity networks have long been recognised[7], with reports of attacks on network components appearing in the media[8].

On 4 November 2021, the information contained in the Joint Intelligence Bulletin (JIB) report was published. In it, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI) and the National Counterterrorism Center (NCTC) referred to an incident that occurred in the United States of America, in Pennsylvania, which involved an attempted attack on elements of the electrical grid using a drone with an electrical wire suspended from its enclosure. The attack most likely involved an unmanned aerial vehicle manufactured by DJI Mavic 2[9]. This is a model commonly available in shops.

In connection with the disclosure of information about the possibility of attacking the power grid with an unmanned aerial

[5] *Energetyka, dystrybucja, przesył...*, pp. 33–49, 2021 [accessed: 30 XI 2021].

[6] Ibid., pp. 51–67, 2021 [accessed: 30 XI 2021].

[7] P.W. Parfomak, *Physical Security of the U.S. Power Grid. High-Voltage Transformer Substations*, Congressional Research Service, 17 VI 2014; R. Baldick, B. Chowdhury, I. Dobson, *Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures*, in: *IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century*, 2008.

[8] https://www.wsj.com/articles/SB10001424052702304851104579359141941621778 [accessed: 30 XI 2021].

[9] https://www.thedrive.com/the-war-zone/43015/likely-drone-attack-on-u-s-power-grid-revealed-in-new-intelligence-report [accessed: 30 XI 2021].

vehicle, a question should be asked to what extent the power grid in Poland is susceptible to such an attack.

For the analysis of the possibility of damaging the grid with an unmanned aircraft, devices whose flight parameters are similar to models commonly available on the market were selected. It should be assumed that some models are designed to perform only specific types of missions, e.g. in the case of models carrying a camera, such a mission is to film an object, while other types of aircraft are universal platforms, adapted by the manufacturer to lift any payload, whose only limitation is its size and weight. Such a payload could be, for example, an air quality device, a lidar system, but also an explosive. Aircraft designed to perform a specific mission are compact, enclosed structures, and it is somewhat difficult to suspend additional payloads underneath them. Vessels that are universal platforms are open structures with decks specially prepared for the suspension of cargo. Analysing the parameters of platforms generally available on the market, it may be assumed to some extent that in most cases an aircraft can lift an additional load of approx. 30% of the weight of the platform without equipment. Platforms that can lift the following cargo weights have been selected for analysis: 0.25 kg, 0.50 kg, 2.5 kg and 4.0 kg. As the weight of the payload increases, the size of the aircraft also increases, so there is a difficulty in transporting and concealing it.

Damage to the electrical system and thus stopping its operation can be done in various ways: it can be mechanical damage by detonation of an explosive charge, damage by causing a short-circuit of live wires to earth, known as grounding, and damage by causing a short-circuit of live wires, with the short-circuit occurring between different phase wires. The November 2021 press release describes an attempted attack involving an induced short circuit in the electrical system, so two scenarios were chosen for analysis:

1. An unmanned aerial vehicle with a long, uninsulated electrical wire suspended from it flies up to the uninsulated phase wire and short circuits it to the ground;
2. An unmanned aerial vehicle with a long uninsulated electric wire suspended flies up to a pole with uninsulated electric wires and short circuits the wires.

Determination of the length of an uninsulated copper conductor which will be used to create a short circuit in an electrical installation

A short circuit will occur between one of the phase conductors and ground or between phase conductors. The length of an electrical conductor that will serve to create a short circuit in an electrical installation can be determined from the formula:

$$l = \frac{m}{\sigma \times S}[\mathrm{m}]$$

where:
l - length of the conductor expressed in m,
m - mass of the wire expressed in kg which the unmanned aerial vehicle will lift up,
σ - density of the material expressed in kg/m3; the density of copper is 8920 kg/m^3,
S - cross-sectional area of the material expressed in m^2.

The cross-sectional areas of electrical conductors are standardised quantities. Calculated lengths of conductors constituting an additional charge with masses: 0.25 kg, 0.5 kg, 2.5 kg, 4.0 kg, are listed in Table 1.

Table 1. Summary of the lengths of the electric cables suspended under the unmanned aerial vehicle, with given cross-sections and assumed masses.

Conductor cross-sectional area S [mm^2]	**Length of cable as additional aircraft payload [m] depending on the mass of the cable suspended from the unmanned aircraft**			
	0,25 [kg]	**0,50 [kg]**	**2,50 [kg]**	**4,00 [kg]**
0,50	55,7	111,5	446,3	892,6
0,75	37,1	74,3	297,5	594,8
1,00	28,5	56,9	227,7	455,4
1,50	18,2	36,4	145,7	291,5
2,50	11,0	22,0	88,2	176,3
4,00	7,1	14,2	56,9	113,8
6,00	4,5	9,1	36,4	72,9
10,0	2,7	5,5	22,0	44,02
16,0	1,7	3,5	14,1	28,2
25,0	1,1	2,2	8,9	17,9
35,0	0,8	1,6	6,4	12,9
50,0	0,5	1,1	4,5	8,9

As can be read from Table 1, for cross-sectional areas up to 4 mm^2 the length of the cable that can be suspended from the UAV is sufficient to cause a short circuit of the phase conductors on the pole. For smaller conductor cross-sections, its length will be sufficient to make a short circuit - a grounding - between the phase conductor and the earth. When a cable suspended from an unmanned aerial vehicle is suspended from the phase conductor of an electrical installation, a short circuit will occur and a short-circuit current will flow through the short-circuiting wire. Such a wire may melt, and the approximate time of melting will depend on its cross-sectional area and the short-circuit current[10]. The approximate values of the currents that will cause the conductor to melt in the declared time are listed in Table 2. This approximation results from the different cross-sectional area S of the conductors used in the United States.

Table 2. List of approximate currents which will cause the conductor to melt after the declared time for the given cross-sections.

Cross-sectional area of the conductor S [mm^2]	**Approximate value of the electric current flowing in the declared time until conductor melting [A] depending on the time of the electric current flow**		
	10 s	**1 s**	**32 ms**
0,50	58,5	158	882
0,75	83,0	250	1400
1,00	99,0	316	1800
1,50	140,0	502	2800
2,50	198,0	798	4500
4,00	280,0	1 300	7100
6,00	396,0	2 000	11 000
10,0	561,0	3 200	18 000
16,0	795,0	5 100	28 000
25,0	1 100	8 100	45 000
35.0	1 300	10 200	57 000
50.0	1 900	16 000	91 000

[10] W.H. Preece, *On the Heating Effects of Electric Currents. No. II*, „Proceedings of the Royal Society of London" 1887–1888, vol. 43; W.H. Preece, *On the Heating Effects of Electric Currents. No. II*, „Proceedings of the Royal Society of London" 1887–1888, vol. 44; E.R. Stauffacher, *Short-time Current Carrying Capacity of Copper Wire*, „General Electric Review" 1928, vol. 31, no. 6.

The fault tripping times are described in the technical documentation[11] and are 120 ms for 400 kV and 220 kV networks and 150 ms for 110 kV networks, respectively. The currents flowing through the lines vary greatly and depend among other things on the type of line. The maximum values of the measured currents can reach up to 1152 A[12]. This means that practically each of the conductors indicated in the table should melt before the line protections are switched off. In the case of an attack on high-voltage distribution substations and transformer stations, which are complex installations not protected from above, the consequences of an attack may be more serious. However, due to the complexity of the construction of the above installations shown in Figure 2, it is difficult to estimate the extent to which elements of the installation will be damaged.

Fig. 2. 400/110 kV high-voltage switching station.

Source: https://elbud.katowice.pl/pl,30,3,projekty-rozbudowa-stacji-400_110-kv-dobrzen.html [accessed: 30 XI 2021].

[11] PSE Operator SA, *Standardowe Specyfikacje Funkcjonalne. Elektroenergetyczna automatyka zabezpieczeniowa, pomiary i układy obwodów wtórnych* (Eng. Standard Functional Specifications. Electricity protection control, metering and secondary circuits), Warszawa 2010 (update 2012).

[12] M. Jaworski, M. Szuba, *Analiza obciążeń napowietrznych linii najwyższych napięć w aspekcie wytwarzania pola magnetycznego* (Eng. Load analysis of overhead high-voltage lines in terms of magnetic field generation), „Przegląd Elektrotechniczny" 2015, no. 5.

The consequences of damage to transmission lines or servicing stations may be similar to those observed during the failure at the Rogowiec substation (through which the power plant in Bełchatów is connected to the national grid system). As indicated in the report[13], the cause of the failure was human error, which led to a short circuit in the electrical system. As a result of the failure, most of the units of the Bełchatów Power Plant were switched off.

It is worth mentioning that there is no ban on flying over transmission lines. The law[14] only stipulates that operations carried out with the use of unmanned aerial vehicles of open and special category over power lines and other devices located in open terrain, the destruction or damage of which may pose a threat to human life or health and the environment or cause serious material losses, shall be carried out with special caution.

Methods of detection of unmanned aerial vehicles

The most commonly used UAV detection methods include:

- radar methods,
- methods detecting communication between the flying unmanned platform and the ground station,
- methods detecting the acoustic signal emitted by the rotating parts of the flying unmanned platform,
- methods based on image analysis, both visible and infrared.

None of these methods used alone can be relied upon to detect a flying object. Therefore, UAV detection systems are made up of different detection devices, operating on different principles. Currently, many companies are developing anti-drone systems, so it is to be expected that their sales will also increase due to the growing number of UAVs.

[13] https://businessinsider.com.pl/wiadomosci/awaria-elektrowni-belchatow-pse-podaje-przyczyny/qpp086b [accessed: 30 XI 2021]; https://www.teraz-srodowisko.pl/aktualnosci/elektrownia-belchatow-awaria-stacja-rozdzielcza-PSE-10340.html [accessed: 30 XI 2021]; https://www.cire.pl/artykuly/serwis-informacyjny-cire-24/184908-poniedzialkowa-awaria-odlaczyla-od-sieci-niemal-cala-elektrownie-belchatow [accessed: 30 XI 2021]

[14] *Guideline No. 7 of the President of the Civil Aviation Authority of 9 June 2021 on the modalities of operations using unmanned aircraft systems in view of the entry into force of the provisions of Commission Implementing Regulation (EU) No 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aircraft.*

As the functionality of UAVs increases, the functionality of anti-drone systems is also changing.

Detecting a vessel using radar is a method familiar from manned aviation. However, the radars used to detect drones are different from those used to detect manned aircraft. The latter detect objects with a larger beam reflecting area and a higher progressive speed than unmanned aircraft[15]. The advantage of this method is that it can detect an attack when it is carried out at high altitudes. Radar will effectively detect an aircraft if there are no obstacles between the radar antenna and the flying aircraft. It will also detect the passing of an unmanned aircraft if it is far from the radar antenna. Unfortunately, the disadvantage of this method of detection is that an unmanned aircraft using a lidar distance measurement system, including distance from the ground, may be travelling just above the surface. In such a situation, the radar system will not detect the flying UAV. The same lidar system will allow the drone to detect and avoid terrain obstacles. The market is currently quite saturated with anti-drone radar systems[16]. However, it seems that attempts to detect a drone flying in a densely built-up area will be mostly ineffective.

An unmanned aircraft can also be detected by monitoring the communication-control between the flying unmanned platform and the ground station. Among the most common methods of controlling an unmanned aircraft is control using a transmitting apparatus, the so-called transmitter, which is located on the ground, in the hand of the pilot. Such apparatus is equipped with two sticks allowing to control the platform in each direction and a set of switches and knobs allowing to operate additional on-board devices. For example, the knobs can be used to control a gimbal with an on-board camera, and a set of switches can be used to control other devices, such as a raised landing gear or a key that releases a suspended load, allowing the load to be dropped at a desired location. Communication between the transmitter and the UAV's computer can take place at two frequencies: platform control at 2.4 GHz and camera image transmission at 5.8 Ghz. In typical solutions, this control method allows control of the UAV over a distance of up to about 3 or 4 kilometres.

[15] https://www.defence24.pl/dlaczego-konflikt-w-gorskim-karabachu-powinien-zmienic-wojsko-polskie [accessed: 30 XI 2021].

[16] https://www.hertzsystems.com/en/antidrone-systems/ [accessed: 30 XI 2021].

The second method of controlling the platform is to send commands from the ground to the computer controlling the UAV via a ground computer and a tablet using what is known as a telemetry channel. Telemetry is a two-way communication channel responsible for transmitting aircraft parameters from the platform to the ground, including such parameters as position, altitude, horizontal progress velocity, rate of climb or descent, battery charge status, as well as forward or backward tilt and left or right roll. Telemetry also allows a command from the pilot to be sent to the aircraft. Such a command can be defined on the ground by drawing in the telemetry software a given geographical position of the platform, its height at a given position, the progressive speed the platform should achieve on its way to the next position, and the so-called POIs (*Point of Interest*), i.e. points towards which the unmanned aircraft should point the camera lens during flight. Communication between the aircraft and the pilot takes place through this channel on different frequencies, e.g. 433 MHz or 868 MHz. The communication distance using telemetry is longer than the communication distance using 2.4 GHz or 5.8 GHz frequencies and can be even above 20 kilometres. An unmanned flying platform can also be controlled by using GSM networks. A schematic of such a control system is shown in Figure 3.

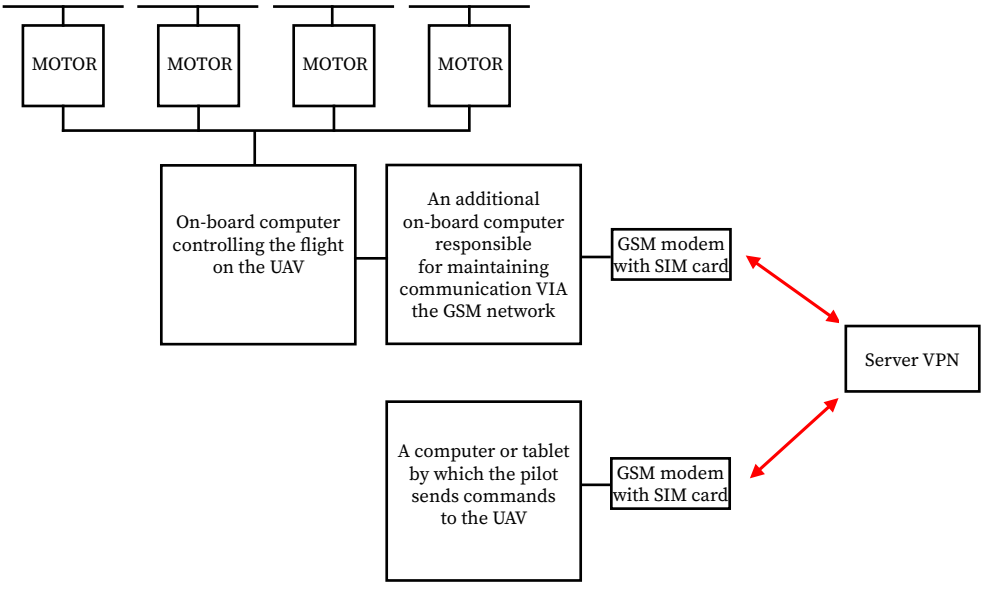


Fig. 3. Scheme of communication between the unmanned aerial vehicle and the pilot via the GSM network.

Source: Author's own elaboration.

GSM communication makes it possible to control an unmanned aircraft without distance limitations. The pilot of the aircraft can control it from any place on earth. The only condition to realise such a connection is the access to the GSM network of both the pilot and the aircraft. The communication is realised through a VPN server, so it is an encrypted communication.

Current detection systems for flying UAVs control the frequency spectrum of electromagnetic radiation in the region of the detector location. Since standard UAVs use electromagnetic radiation of known frequencies to communicate with the pilot, the detector can detect the appearance of a source of emission of such radiation. It is possible to use artificial intelligence and machine learning technologies to indicate to the detector which sources are drones and which are not[17]. It is worth noting that these systems can detect UAVs that maintain communication with a ground station during flight. They usually detect typical aircraft, commonly available on the shelves. However, they become ineffective when the aircraft has been programmed before take-off and flies without communicating with the base station, or maintains communication with the base station at unusual frequencies. Additionally, the electronic elements of which the drone is composed can be separated from the environment by a so-called Faraday cage, which prevents the penetration of electromagnetic radiation into the aircraft and from its interior to the outside. It cannot then be detected because the Faraday cage isolates it from the electromagnetic radiation detectors. Monitors controlling the operation of selected aircraft models can be used to detect typical aircraft. Such monitors include the AeroScope device, which can detect communication and aircraft status in real time. However, such a device only detects drones made by DJI[18]).

Another method of unmanned aircraft detection is based on the detection of noise originating from their rotating components. In UAVs, the sources of noise are propellers and, to a lesser extent, engines. Every flying UAV emits sound, with the frequency and intensity of the sound wave depending on the shape of the propeller

[17] https://www.droneshield.com/ [accessed: 30 XI 2021]; https://www.dedrone.com/ [accessed: 30 XI 2021]; https://www.echodyne.com/security/counter-drone-radar/ [accessed: 30 XI 2021].

[18] https://www.dji.com/pl/aeroscope [accessed: 30 XI 2021].

and the angular speed at which the propeller rotates. There are methods to reduce the noise emitted by unmanned aircraft[19]. These include the use of propulsion units with lower rotational speeds, the use of propellers with different numbers of blades, the use of propellers with different aerodynamic profiles. An unmanned aircraft may therefore go undetected if it emits low noise levels and flies where other noise sources are present, such as public transport vehicles, manned aircraft during take-off and landing, other man-made noises. It should also not be forgotten that an aircraft like an aeroplane can approach a protected object by gliding flight, so it will not be a source of propeller noise.

The last significant method of identifying unmanned aircraft is space analysis using cameras operating in both visible and infrared spectrums. Image analysis is carried out using a computer system which, based on the image recorded by the camera, recognises whether the flying object is a drone or, for example, a bird. Visual detection systems are based on machine learning and artificial intelligence technology. Teaching a computer to recognise an object is a tedious, time-consuming process that requires high computing power and a large database of source images depicting the object to be detected. Such systems detect typical aircraft. Once an aircraft has an unusual shape, it will be impossible to detect. Unmanned aerial vehicles can be built so that the shapes are very unusual. For example, Greenpeace members famously built a Superman-shaped drone and crashed it into a concrete reactor shield at the Bugey nuclear power plant in France[20]. The moment of the attack is shown in Figure 4. The drone itself hitting the wall of the reactor shield did not endanger the safety of the reactor.

[19] F.B. Metzger, *An Assesment of Propeller Aircraft Noise Reduction Technology*, NASA Contractor Report 198237, 1995; W. Yuliang et al., *Noise Reduction of UAV Using Biomimetic Propellers with Varied Morphologies Leading-edge Serration*, „Journal of Bionic Engineering" 2020, vol. 17, pp. 767–779.

[20] https://www.reuters.com/article/uk-france-nuclear-greenpeace-idUKKBN1JT17G [accessed: 30 XI 2021].

Fig. 4. The moment of attack on a nuclear reactor using a Superman-shaped drone.

Source: https://www.reuters.com/article/uk-france-nuclear-greenpeace-idUKKBN1J-T17G [accessed: 30 XI 2021].

Such walls are built to withstand the impact of a manned aircraft which, flying at high speed and possessing a large mass, would hit the target with high kinetic energy. However, this case has shown how irresistible protected facilities are to drone action, especially those built at a time when drones were not yet so widely available. Cameras operating in the visible band of electromagnetic radiation are unable to detect flying aircraft in low visibility conditions. Analysing space with cameras operating in the infrared range of electromagnetic waves makes it possible to detect heat sources other than those naturally found in space. An infrared camera can detect and distinguish an unmanned aircraft because it uses components that emit heat during operation. Such components can include both electric and internal combustion engines, as well as lithium-polymer batteries, which spontaneously heat up during operation. An infrared camera can detect a flying aircraft at night. However, also this way of detecting drones is not always effective. Knowledge of manned aviation indicates that it is possible to build the aircraft in such a way that the heat energy is dissipated to a large extent, so that the aircraft cannot be detected.

Selected methods to neutralise unmanned aircraft

The process of detecting an unmanned aircraft itself is only the first stage of defence against its attack. The following methods are used to neutralise hostile UAVs:

- hitting and entangling the moving parts of the UAV with a net,
- interference with the positioning of the satellite system used by the aircraft,
- interference with aircraft-ground station communications,
- use of high-power laser light,
- damage to electronic systems by high-power electromagnetic pulse.

Hitting and entangling an unmanned aircraft is a difficult process. The attacking aircraft may be a multirotor craft, an aircraft or a helicopter. It can also combine features of all the above-mentioned types and then a hybrid of them is formed. Such hybrids include aircraft with vertical take-off capability, the so-called V-tol (from Vertical Take Off and Landing). Each of these devices has different physical characteristics, against which the method of neutralisation with a net will be ineffective. Such characteristics certainly include the progressive speed of the ship in flight. An aircraft moves at a high speed, while a multirotor moves at a relatively low speed. The throwing device may be in the hand of a member of the site security staff or it may be suspended from another aircraft piloted by a member of the site security staff. Mesh systems used to neutralise aircraft are effective when the attacking aircraft is moving at low speed or remains in a so-called hover. The main problem when using this method is the short distance of the net throwing device from the target. After a successful hit, an unmanned aircraft entangled in the net falls to the ground with the help of a parachute system. Thanks to its low speed of descent, it will not crash to the ground, damage infrastructure elements or cause loss of health or life if it falls on a person. An undamaged aircraft with a computer on board can provide evidence for a court if the perpetrator of an attack is discovered.

Another method of neutralising a flying aircraft is to jam or impersonate the satellite positioning system signal. The interference or impersonation of a satellite signal is reported in the press[21].

[21] https://www.techtarget.com/searchsecurity/definition/GPS-jamming [accessed: 30 XI 2021]; https://www.militaryaerospace.com/rf-analog/article/14207023/gps-

The interference is when a signal is emitted from the interfering device at the frequencies on which the positioning system operates. The jamming signal is more powerful than the satellite signal. In such a situation, the satellite receiver used for navigation on board the unmanned aircraft considers the signal of the jamming device as correct and is not able to determine its position properly using that signal. Impersonation is when the impersonating device emits a signal containing a false position. In this way, the aircraft, instead of reaching its target, will fly to the place indicated by the neutralising device and the attack will be ineffective. The answer to this defence can be navigation, which allows to determine the position of the aircraft without access to the positioning system signal. Such navigation also allows an unmanned aircraft to fly through buildings or mines[22]. Non-satellite based navigation systems identify the position of the aircraft by means of lidar readings, ultrasonic distance measuring devices, visible or infrared camera systems[23]. Systems for navigation in the absence of access to satellite signals will develop rapidly due to the possibility of damage to satellites in the event of war[24]. A method of navigation without the use of satellite positioning system is also the deployment of ground stations emitting a position signal and navigation based on triangulation[25].

The devices interfering with the communication signal between the aircraft and the ground station emit high-power electromagnetic radiation at different frequencies, which include the frequencies used by the unmanned aircraft. Interference with communication takes place through the emission of an electromagnetic wave with a completely flat spectrum and noise intensity uniform throughout the jammed

signals-jamming [accessed: 30 XI 2021]; https://www.c4isrnet.com/newsletters/military-space-report/2020/04/15/natos-new-tool-shows-the-impact-of-gps-jammers/ [accessed: 30 XI 2021].

[22] https://polskiprzemysl.com.pl/przemysl-energetyczny/gornictwo-urzadzenia-maszyny/drony-w-kopalniach/ [accessed: 30 XI 2021].

[23] F. He et al., *Automated Aerial Triangulation for UAV-Based Mapping*, „Remote Sensing", December 2018, no. 10 (12), 1952.

[24] https://spidersweb.pl/2021/11/rosja-satelita-smieci-kosmiczne.html [accessed: 30 XI 2021].

[25] R. Kapoor et al., *UAV Navigation Using Signals of Opportunity in Urban Environments. An Overview of Existing Methods,* 1st International Conference on Energy and Power, ICEP 2016, 14–16 December 2016, Melbourne, Australia.

band. This is known as white noise[26]. This uniformity means that for each frequency of electromagnetic noise the power of emitted wave is the same. Such noise drowns out communication between aircraft and pilot, making control impossible. Interference systems can be circumvented quite simply, i.e. by using unusual frequencies not used in commonly available aircraft for vessel-pilot communication or by hiding the aircraft's electronic equipment in a so-called Faraday cage. Another method to prevent the aircraft from being neutralised is to program the mission before the flight and perform the flight in an autonomous manner, i.e. without the pilot's involvement, based on commands given before take-off.

The use of a high-power laser beam is an effective method under the right conditions. The laser light illuminates the flying aircraft and causes it to light up. This method is currently being developed in many countries[27]. The advantage of this method of destroying a drone is that it can be brought down from a relatively long distance. The disadvantages of the system are: the requirement to power the laser from a high-power source, sensitivity to weather conditions, including fog or rain. The system can destroy UAVs one at a time. When an attack is carried out with multiple drones or even with a swarm, this system has limited effectiveness.

Damaging electronic systems with a high-powered electromagnetic pulse is a technique known from military applications. An unmanned aerial vehicle is a technical object that uses systems of advanced electronics. Electronic devices used in drones include a control computer, an auxiliary computer that can be used to perform calculations such as image analysis, electronic controllers of the rotation of aircraft engines, receivers used to receive commands from the pilot, telemetry devices used to exchange information between the craft and a ground station, e.g. the status of the aircraft, satellite navigation devices, etc. Aircraft may be protected against electromagnetic pulse by using multilayer trays to shield electronic equipment from the impulse.

---

[26] B. Carter, R. Mancini, *Op Amps for Everyone,* Burlington 2009, pp. 174–175.

[27] https://www.rafael.co.il/worlds/air-missile-defense/c-uas-counter-unmanned-aircraft-systems/ [accessed: 30 XI 2021]; https://www.thedefensepost.com/2021/07/09/france-anti-drone-laser/ [accessed: 30 XI 2021]; https://www.aerospacetestinginternational.com/news/defense/us-air-force-progresses-testing-of-anti-drone-laser-weapons.html [accessed: 30 XI 2021].

All the methods mentioned above are of limited effectiveness, so it is necessary to look for other ways of protecting the object. Prevention, preventing the start of an attack, is important for the security or defence of the state. Such methods include:

- securing the protected object with a DRA-P zone,
- using devices which cut off the possibility of flying in the protected area,
- training of police officers in aviation law, procedures in force in unmanned aviation and regulations allowing for punishment of pilots flying illegally,
- training of facility security staff in piloting multirotor vessels and aircrafts,
- masking the elements of infrastructure of the protected facility,
- covering elements of the infrastructure from impact or from the effects of explosive cargo carried by aircraft,
- actions for the benefit of the local community.

Securing a protected facility with a DRA-P zone

According to the current guidelines of the President of the Civil Aviation Office (ULC)[28], the Polish Air Navigation Services Agency (PAŻP) may designate the following drone geographical zones:

a) DRA-T - a zone in which the flight of an unmanned aircraft is possible after the aircraft meets the technical requirements indicated by the PAŻP. In this zone, it is allowed to meet additional conditions for flight, including for example the requirement to obtain a permit to fly;
b) DRA-U - a zone where flight of an unmanned aircraft may only take place with the support of services required for this zone and under conditions of flight performance indicated by PAŻP;
c) DRA-I - information area, where the approval for flight is not required but where information is required to ensure flight safety;

[28] See: *Wytyczne nr 7 Prezesa Urzędu Lotnictwa Cywilnego z dnia 9 czerwca 2021 r...*

d) DRA-P - prohibited area, in which operations with unmanned aircraft systems may not be conducted;
e) DRA-R - restricted area for unmanned aircraft systems, in which operations with unmanned aircraft systems may be performed with the permission and under conditions specified by PAŻP or an authorised entity, at the request of which the geographical area was designated.

The DRA-R zone may consist of additional sub-zones designated by:

1. DRA-RH - in which the probability of obtaining permission to fly with an unmanned aircraft is high (*high*);
2. DRA-RM - in which the probability of obtaining permission to fly with the unmanned aircraft is medium (*middle*),
3. DRA-RL - in which the probability of being cleared to fly with the unmanned aircraft is low (*low*).

Due to the needs of actions or activities of particular operational or reconnaissance importance for ensuring national security or public order, conducted in order to carry out statutory activities, the geographical zones may be designated on the motion of the Operational Commander of the Armed Forces, Commander-in-Chief of the Military Police, Chief of the Air Traffic Services of the Polish Armed Forces, Head of the Internal Security Agency, Head of the Foreign Intelligence Agency, Police Commander-in-Chief, Commander-in-Chief of the Border Guard, Head of the National Revenue Administration or Commander of the State Protection Service. Due to the need to protect critical infrastructure facilities, prevent the effects of natural disasters or their removal, save human health or life, the geographical zones may be designated at the request of the Police Commander-in-Chief, the Commander-in-Chief of the State Fire Service or the Director of the Government Centre for Security.

Uniform rules on the operation of unmanned aircraft currently apply throughout the European Union[29]. According to these rules, flights by unmanned platforms are performed in three different categories. Each category corresponds to a certain level of risk

[29] *Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aerial vehicles; Commission Implementing Regulation (EU) 2020/746 of 4 June 2020 amending Implementing Regulation (EU) 2019/947 as regards the postponement of the dates of application of certain measures in relation to pandemic COVID-19 (OJ EU L 176 of 5 VI 2020, p. 13).*

associated with the mission. There are three levels of risk: low, for the OPEN category; medium, for the SPECIFIC category; and high, for the CERTIFIED category. The certified category includes flights carrying persons or dangerous goods. The SPECIFIC category are flights which require, in principle, consent to conduct the operation. Such consent, as implied, is given to pilots holding the appropriate rating to fly under the so-called standard scenarios. Standard scenarios are a set of rules of flight whose observance guarantees that the mission is performed with an acceptable risk. Currently in Poland, there are eight standard scenarios concerning flights within visual range (VLOS) and beyond visual range (BVLOS) for aircraft such as aeroplanes, multirotors and helicopters with take-off mass up to 4 kg and for aircraft such as aeroplanes, multirotors and helicopters with take-off mass not exceeding 25 kg. The open category is low-risk flights and therefore no flight approval is required. Pursuant to *Guideline No 7*, flights in the open category and in the special category in the DRA-P drone geographical zone shall take place with the consent of the zone manager and under the conditions specified for that zone. *Guideline No 7* does not include rules for flights in the certified category. The analysis of aviation documentation contained in the messages of the DroneRadar application (DroneRadar is an application for the Android and iOS systems, free and widely available in the shops of mobile network operators) indicates that in the DRA-P zones designated over protected objects, flights with unmanned aerial vehicles are allowed, but only up to a height of 30 m above the ground with an aircraft weighing not more than 0.9 kg and at a distance of not less than 500 m from the border of the protected object. These provisions indicate that DRA-P zones can be used to protect facilities, provided they are properly designed.

Let us consider two cases of DRA-P zones designated as in Figure 5.

1. The boundaries of the DRA-P zone are located at a distance "L" of less than 500 m from the boundaries of the protected object. Outside the zones, according to the general rules of flight, an unmanned aircraft can fly up to an altitude "H" of no more than 120 m above the ground. Using the Pythagorean theorem, it is possible to calculate the angle at which a camera from an unmanned platform can observe a protected object when flying at the maximum permissible

height. The minimum angle at which it can observe the object is 15 degrees, with the shorter the distance from the protected object boundary to the DRA-P zone boundary, the greater the angle of observation will be. For example, if the borders of the DRA-P zone are determined at a distance "L" of about 120 m, the angle of observation of the object from the platform will be equal to 45 degrees.

2. The boundaries of the DRA-P zone are at a distance "L" greater than 500 m from the boundaries of the protected object. According to the rules, the unmanned platform can perform a flight in the space between the 500th meter counted from the boundaries of the object and the border of the DRA-P zone. The flight can take place up to a height of 30 m above the ground. Using the Pythagorean theorem, it is possible to calculate the angle at which the camera from the unmanned platform can observe the protected object when the flight takes place at the maximum permissible height. The maximum angle at which it can observe the object is 15 degrees, with the greater the horizontal distance of the flying platform from the border of the protected object, the smaller the angle of observation will be. If there are any natural terrain obstacles, e.g. trees, between the protected object and the eye of the camera, it will be practically impossible to observe the object.

The decision to designate a DRA-P zone over a facility should be made after a thorough analysis of the actual threats and an assessment of the facility's vulnerability to attack using an unmanned aircraft. Only if the threat and vulnerability assessments indicate that the risks associated with a potential attack on the facility are unacceptable should the zone be designated. The designation of such a zone is a clear indicator that something important from the point of view of defence or national security is happening at a given facility.

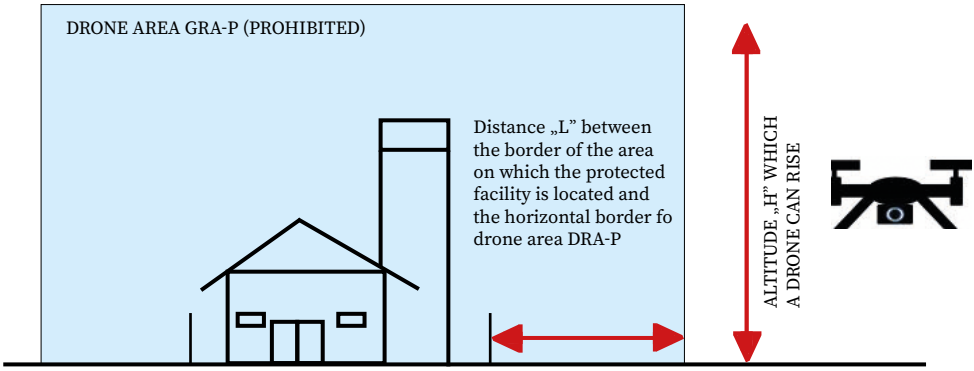


Fig. 5. Diagram of the DRA-P drone geographical zone.

Source: Author's own elaboration.

The use of devices to prevent flight into a protected space

Devices preventing the flight of unmanned aircraft include the Aeroscope[30]. However, it affects only DJI aircraft. It is not able to protect the protected object against aircraft manufactured by other companies or built by independent designers. Aeroscope can identify the aircraft's serial number, its location as read from the satellite signal receiver, its speed and direction of flight and the altitude at which it is flying. These parameters are read out in real time. Polish law does not require registration of the aircraft, which makes identification of the aircraft and assigning it to a particular pilot extremely difficult. The only possibility to identify the pilot is to declare the serial number of the aircraft, which each pilot must submit if he/she wants to fly in the aeronautical CTR zone, and to register the drone, i.e. to provide this number in the Pansa_UTM system[31]. Without this registration, it is not possible to obtain conditions for flight in CTR zones. However, if the aircraft was manufactured by a manufacturer other than DJI or by an independent builder, Aeroscope will not identify it. Aeroscope can also restrict a flight by designating a zone in which the flight will not take place. Such a function is called GeoFencing. The Aeroscope

[30] https://www.dji.com/pl/aeroscope [accessed: 30 XI 2021].

[31] https://utm.pansa.pl [accessed: 30 XI 2021].

operator can indicate the horizontal and vertical boundaries of the zone in which the flight cannot take place. DJI aircraft will therefore not be able to fly in this zone. The disadvantage of the device is that it cannot detect every DJI model and non-DJI models. An additional problem is posed by the storage of data collected by Aeroscope on the servers of the Chinese company DJI. This data can be used to obtain information about the location of protected facilities[32].

Training of police officers in aviation law, procedures in force in unmanned aviation and provisions allowing for punishment of pilots flying illegally

Such training should be a standard activity in Police units in whose area of operation there are objects important for the security or defence of the state. The training should cover European regulations:

- *Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation* (OJ EU L 212 of 22 VIII 2018, p. 1);
- *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aerial systems and operators of unmanned aerial systems from third countries* (OJ EU L 152 of 11 VI 2019., p. 1);
- *Commission Delegated Regulation (EU) 2020/1058 of 27 April 2020 amending Delegated Regulation (EU) 2019/945 as regards the introduction of two new classes of unmanned aircraft systems* (OJ EU L 232 of 20 VII 2020., p. 1);
- *Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aerial vehicles* (OJ EU L 152 of 11 VI 2019, p. 45);
- *Commission Implementing Regulation (EU) 2020/639 of 12 May 2020 amending Implementing Regulation (EU) 2019/947 as regards standard scenarios for operations within visual range or beyond visual range* (OJ EU L 150 of 13 V 2020, p. 1).

The training should also cover the provisions of national law, including the *Aviation Law* Act and the guidelines of the President of the Civil Aviation Authority (ULC):

[32] https://www.911security.com/blog/dji-aeroscope-review-features-specs-and-how-its-used-in-layered-drone-detection [accessed: 30 XI 2021].

– *Guideline No. 7 of the President of the Civil Aviation Authority of 9 June 2021 on the modalities of operations using unmanned aircraft systems in relation to the entry into force of the provisions of Commission Implementing Regulation (EU) No 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aerial vehicles* (Official Journal of the Civil Aviation Authority of 2021, item 35);
– *Guideline No. 24 of the President of the Civil Aviation Office of 30 December 2020 on the designation of geographical zones for unmanned aircraft systems* (Official Journal of the Civil Aviation Authority of 2020, item 78).

For facilities located in MCTR military zones, Police officers should also refer to the document:

– *Guidelines of the Commander-in-Chief of the Air Traffic Service of the Armed Forces of the Republic of Poland No. 6 of 17 September 2018 on detailing the principles of performing flights of flying models and unmanned aerial vehicles with an MTOW of 25 kg or less in air traffic zones of military airports (MATZ) and controlled zones of military airports (MCTR),* (https://ssrlszrp.wp.mil.pl/u/Wytyczne_w_sprawie_wykonywania_lotow_przez_RPAS.pdf).

In addition, Police officers should familiarise themselves with the use of the DroneRadar application used to image the structure of airspace, including the identification of horizontal boundaries of drone geographical zones. This application also allows to read the rules of performing flights by unmanned aerial vehicles in the zones. Knowledge of the law and familiarity with flight rules will allow police officers to identify pilots who perform flights in violation of flight rules.

The provisions allowing for the punishment of pilots flying against the rules are contained in various pieces of legislation. Selected provisions that talk about criminal liability are:

1. Within the scope of the *Act of 3 July 2002 Aviation Law* (i.e. Journal of Laws of 2020, item 1970, as amended):
   a) Article 211.1 Who:
      5) contrary to Article 97 of the Act, performs a flight or other aeronautical activities without a valid license or certificate of competence or contrary to their contents and conditions,
      6) contrary to Article 105, paragraph 2 of the Act, performs flights or other aerial activities despite the loss of the

required mental and physical fitness,

9a) contrary to Art. 123 par. 2, discharges from an aircraft in flight,

shall be subject to a fine, the penalty of limitation of liberty or deprivation of liberty for up to one year.

b) Art. 212.1. Whoever:

1. while performing a flight by means of an aircraft:

c) violates the air traffic regulations in force in the area where the flight takes place,

d) crosses the state border without the required permit or in breach of the conditions of the permit,

e) violates, issued pursuant to Art. 119 par. 2 of the Act, the prohibitions or restrictions on flights in Polish airspace introduced due to military necessity or public security

shall be subject to the penalty of deprivation of liberty for up to 5 years.

2. Within the scope of the Act of 6 June 1997 - Penal Code (Journal of Laws of 2021, item 2345, as amended):

a) Article 267.1. Whoever, without authorisation, gains access to information not intended for him by opening a closed letter, by connecting to a telecommunications network or by breaking or bypassing electronic, magnetic, IT or other specific protection thereof,

shall be subject to a fine, the penalty of limitation of liberty or deprivation of liberty for up to 2 years.

b) Art. 267.3. The same punishment shall be imposed on anyone who, in order to obtain information to which he is not entitled, sets up or uses a listening or visual device or any other device or software.

During the training, other regulations which have an impact on flight operations and are contained in legal acts should also be taught: Code of Petty Crimes, Atomic Law, Law on protection of persons and property, on protection of nature, on copyright and related rights, on protection of personal data. A police officer familiar with the above-mentioned regulations should know how to impede or prevent the flight of an unmanned aerial vehicle in the area of a protected facility.

Training of facility security staff in piloting multirotor and aerial vehicles

Facility security personnel should be competent to fly aircraft to enable them to effectively protect the protected facility. Aircrafts are capable of long-range flight over long distances. Aircraft equipped with cameras operating in the visible and infrared bands of electromagnetic waves allow observation of the foreground of the protected object both during the day and at night. Equipping these aircraft with a computer with installed software that uses AI algorithms to detect unusual activity should enable security personnel to prepare for an attack on the protected object. A multirotor aircraft allows for short distance flight, but can hover in one place. Such hovering allows for prolonged observation of a location where suspicious activity has been observed.

Masking the infrastructure of a protected facility

One of the ways of attacking facilities important to national security and defence is with cameras operating in the visible and infrared bands. The camera can be used to obtain information on the technology used at the facility, the technical equipment used in the physical protection system, the customs and procedures followed by the physical protection staff or other employees of the facility. Masking of infrastructure elements should prevent or hinder the acquisition of sensitive information from an unmanned platform.

Shielding of infrastructure elements from impact or from the effects of an explosive charge carried by the aircraft

An unmanned aircraft can be a useful platform for carrying explosive cargo or cargo containing chemicals. Explosive cargo can easily damage infrastructure components, causing the facility to slow down or stop operations. Contamination of the facility area or its foreground can have the same effect. The consequence of such an attack will be financial losses for the facility operator, financial losses for recipients of goods or services provided on the premises. Loss of health or life of employees of the attacked facility and losses related to environmental pollution are also possible. Shielding important parts of the facility's infrastructure

from the effects of an explosive device or from a direct hit by an unmanned aerial vehicle can protect the facility from the effects of an attack.

Measures for the benefit of the local community

Facilities that are important for the security or defence of the state are sometimes located in populated areas. Proper cooperation between the facility operator and the local population can help protect the facility. Local residents can easily recognise strangers behaving in an unusual way. Actions allowing to increase the degree of cooperation between the operator and the local population include: funding scholarships for talented young people, support for local health centres and hospitals, joint events such as "cleaning up the world", inviting local people to visit the protected facility in places where there are no devices sensitive from the point of view of protection of technological information or physical protection of the facility.

Conclusions

1. Paralysis of the functioning of the state, including disruption or interruption of critical infrastructure systems may occur not only by attacking well-protected facilities where electricity is generated, but also by attacking unprotected infrastructure used to deliver energy to the consumer,
2. The electricity grid in Poland is, with the exception of insulated lines, not resistant to short-circuit attacks using a cable suspended from an unmanned aerial vehicle.
3. Unmanned aerial vehicles, even the smallest ones, will easily lift a small payload of copper wire, which can be used to cause a short circuit.
4. The length of overhead lines and the multiplicity of substations serving them practically exclude any chance of preventing an attack by short circuiting the installation.
5. Successful attacks can result in large financial losses for both the power generator and grid operator and for power consumers.
6. Designs for new overhead lines must take into account the emergence of new sources of threat, which are drones. Thus, overhead

lines should, where possible, be built with insulated conductors in such a way that they cannot be short-circuited by a drone. An impulse to change the way lines are designed may be provided by the project of increasing the cabling of medium-voltage networks by 2040. Such cabling should be carried out as long as the level of network cabling in Poland does not equal the average EU level.

7. Properly designated DRA-P zone allows to increase the level of security of the protected facility. Due to the ease of attack, the designation of DRA-P zones around node points, critically important for the transmission of electricity in the country, should be considered.
8. The location of the DRA-P zones is public and information about it is available to everyone, so the selection of objects, for which the designation of DRA-P zones could be critically important, must be carried out with extreme caution.
9. In the absence of technical capabilities and given the financial constraints of network operators, it is worth considering preventive measures to secure facilities where electricity is generated and those used for the transmission of electricity by means other than detection devices and UAV neutralisation systems.

Bibliography

Baldick R., Chowdhury B., Dobson I., *Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures*, w: *IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century*, 2008.

Carter B., Mancini R. , *Op Amps for Everyone*, Burlington 2009.

Jaworski M., Szuba M., *Analiza obciążeń napowietrznych linii najwyższych napięć w aspekcie wytwarzania pola magnetycznego* (Eng. Load analysis of overhead high-voltage lines in terms of magnetic field generation), „Przegląd Elektrotechniczny" 2015, no. 5, pp. 149–154.

Kapoor R. et al., *UAV Navigation Using Signals of Opportunity in Urban Environments. An Overview of Existing Methods*, 1st International Conference on Energy and Power, ICEP2016, 14–16 XII 2016, Melbourne, Australia.

Metzger F.B., *An Assesment of Propeller Aircraft Noise Reduction Technology*, ASA Contractor Report 198237, 1995.

Parfomak P.W., *Physical Security of the U.S. Power Grid. High-Voltage Transformer Substations*, Congressional Research Service, 17 VI 2014.

Preece W.H., *On the Heating Effects of Electric Currents. No. II*, „Proceedings of the Royal Society of London" 1887–1888, vol. 43, no pagination.

Preece W.H., *On the Heating Effects of Electric Currents. No. II*, „Proceedings of the Royal Society of London" 1887 1888, vol. 44, no pagination.

Standardowe Specyfikacje Funkcjonalne. Elektroenergetyczna automatyka zabezpieczeniowa, pomiary i układy obwodów wtórnych (Eng. Standard Functional Specifications. Electricity protection control, metering and secondary circuits), Warszawa 2010 (update 2012).

Stauffacher E.R., *Short-time Current Carrying Capacity of Copper Wire*, „General Electric Review" 1928 r., vol. 31, no. 6, pp. 326–327.

Yuliang W. et al., *Noise Reduction of UAV Using Biomimetic Propellers with Varied Morphologies Leading-edge Serratio*n, „Journal of Bionic Engineering" 2020, vol. 17, pp. 767–779.

Internet sources

Energetyka, dystrybucja, przesył (Eng. Energy, distribution, transmission), PTPiREE, http://ptpiree.pl/raporty/2021/raport_ptpiree_2021.pdf [accessed: 30 XI 2021].

Legal acts

Commission Implementing Regulation (EU) 2020/639 of 12 May 2020 amending Implementing Regulation (EU) 2019/947 as regards standard scenarios for operations within visual range or beyond visual range (OJ EU L 150, 13 V 2020, p. 1).

Commission Delegated Regulation (EU) 2020/1058 of 27 April 2020 amending Delegated Regulation (EU) 2019/945 as regards the introduction of two new classes of unmanned aircraft systems (OJ EU L 232, 20 VII 2020, p. 1).

Commission Implementing Regulation (EU) 2020/746 of 4 June 2020 amending Implementing Regulation (EU) 2019/947 as regards the postponement of the dates of application of certain measures in relation to the COVID-19 pandemic (OJ EU L 176, 5 June 2020, p. 13).

Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aerial vehicles (OJ EU L 152 of 11 VI 2019, p. 45).

Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aerial systems and third-country operators of unmanned aerial systems (OJ EU L 152 of 11 VI 2019, p. 1).

Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Agency for Aviation Safety and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 of the European Parliament and of the Council 2014/30/EU and 2014/53/EU and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ EU L 212 of 22 VIII 2018, p. 1).

Act of 3 July 2002 Aviation Law (i.e. Journal of Laws of 2020, item 1970, as amended).

Act of 6 June 1997 - Penal Code (i.e.: Journal of Laws of 2021, item 2345, as amended).

Guideline No. 7 of the President of the Civil Aviation Authority of 9 June 2021 on how to conduct operations using unmanned aircraft systems in connection with the entry into force of the provisions of Commission Implementing Regulation (EU) No 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aircraft (Official Journal of the Civil Aviation Authority of 2021, item 35).

Guideline No. 24 of the President of the Civil Aviation Office of 30 December 2020 on the designation of geographical zones for unmanned aircraft systems (Official Journal of the Civil Aviation Office of 2020, item 78).

Guidelines of the Commander-in-Chief of the Air Traffic Service of the Armed Forces of the Republic of Poland No. 6 of 17 September 2018 on detailing the rules for flights of flying models and unmanned aerial vehicles with MTOW not exceeding 25 kg in air traffic zones of military airports (MATZ) and controlled zones of military airports (MCTR), https://ssrlszrp.wp.mil.pl/u/Wytyczne_w_sprawie_wykonywania_lotow_przez_RPAS.pdf.

DOI: 10.4467/27204383TER.22.013.15429

ORCID: 0000-0002-3793-5913

ALEKSANDER OLECH

Unique solutions of the French Republic in the fight against terrorism and radicalisation

Abstract

Experience and solutions of the French Republic, where anti-terrorist structures are constantly developed, should be a signpost for other countries. Creation of unique deradicalization programs and conducting a policy of responding to cases of extremism are actions that can be implemented in Poland. In addition, the use of social media to combat terrorist content and to provide information about threats shows the innovative use of the Internet. It is also worth noting the involvement of French municipal guards and medical services in the process of responding to terrorism, as well as highlighting the role of NGOs working to support victims. Decades of France's struggle with different types of terrorism have meant that methods that would be effective in countering radicalisation and threats have been improved and reviewed over the years. In the author's opinion, it would be advisable to take advantage of the French experience and implement at least some of the solutions in Poland.

Keywords:

anti-terrorism,
France,
Poland,
radicalization,
deradicalization

Terrorist threats, including growing radicalisation, are on the rise in Europe, posing a threat to all countries on the continent. In addition to international action, such as involvement in the global fight against terrorism, there is a need to respond to internal threats. The reasons for this can be traced to changes in religious, political and social beliefs. In some countries, groups are forming which undertake anti-state terrorist activity in order to achieve their goals. In addition, they seek to build a message by involving others, including young people, reinforcing in them the need to support extreme ideological views.

Citizens who become aggressive and uncompromising in their views and modes of action may undertake to organise attacks or develop extremist cells. This is why so much attention needs to be paid to domestic or home-grown terrorism[1]. Often, but not always, people who have been brought up in the culture of European countries, but who are orthodox Muslims or who only identify with Islam when preparing an attack, as in France[2], become terrorists. They are strongly radicalised (adopting opinions, views and ideas that lead to extremism) and as a result may attempt to carry out attacks on the territory of the State of which they have had citizenship by birth, obtained it or in which they have been granted the right to reside. This type of terrorism is also described as a sociological curiosity, since religion dominates the republican values promoted in the country of residence.

In the French Republic, it is stated that radicalisation is the type of any ideology or religion that induces an individual to choose violence in the name of beliefs, while not recognising compromise and choosing to terrorise society. Radicalisation is a process of gradual commitment to and rejection of the rules of society. It occurs during socialisation and relationship building and affects the psyche. It is a phenomenon strongly linked to the reinforcement of identity conflicts and weaknesses

[1] K. Rekawek et al., *Who are* the *European jihadis? Project Midterm Report*, Bratislava 2018.

[2] In France, the authorities have long pursued assimilation as a model of social integration, believing that minimising cultural and religious differences will maintain France as both secular and multicultural. In reality, many people in the country feel alienated and excluded from French society. This problem has been evident for more than two decades. See: K. Thachuk, M. Bowman, C. Richardson, *Homegrown Terrorism. The Threat Within*, Washington 2008, pp. 5, 15-16.

by ideology or religion (problems at work or school, family or personal)[3]. Although radicalisation is not exclusive to jihadist terrorists, it is mainly such people who pose a threat in France today.

Terrorism is a phenomenon that constantly occurs in the international environment. France is constantly facing terrorist threats and is the most frequently attacked country in the European Union in the 21st century. Since the 1950s it has experienced virtually all types of terrorism: from right-wing, to left-wing, to separatist and now jihadist terrorism. So far, Poland has not been a target of terrorist attacks and is not a country where terrorists are constantly and actively operating, although they do transit the country. Moreover, there are indications which make us reflect on the potential threat in Central and Eastern Europe and the growing radicalisation among the citizens of this part of the continent.

The use of solutions applied in France creates an opportunity not only to improve anti-terrorist systems and methods of operation of counter-terrorist units in Poland and other states, but also to educate and make the society aware of emerging threats and challenges. Constant cooperation and supervision of all entities that may be susceptible to terrorist threats are necessary for the proper development of security structures in the state. The use of France's experience also seems extremely important in the context of building anti-terrorist potential in all EU and NATO member states. The most effective way to fight terrorism is to prevent it, so member states should use proven methods that have been developed for decades in France[4], thanks to which they can now be described as unique[5].

The aim of the article is to systematize knowledge and to direct the activities of entities obliged to fight against terrorism in Poland and other countries, using the anti-terrorism prevention used in the French Republic. In the author's opinion, some of the elements of French

[3] Secrétariat général du Comité interministériel de prévention de la délinquance et de la radicalisation, *Une politique publique volontariste et évolutive*, https://www.cipdr.gouv.fr/prevenir-la-radicalisation, [accessed: 4 XI 2021].

[4] Already in 2005, French counter-terrorism activities carried out since the 1980s were recognised as the most effective in Europe. See: L. Block, *Evaluating* the *Effectiveness* of *French Counter-Terrorism*, "Terrorism Monitor Volume" 2005, vol. 3, no. 17.

[5] A. Olech, *Walka z terroryzmem. Polskie rozwiązania a francuskie doświadczenia* (Eng. Fight against terrorism. Polish solutions versus French experience), Warszawa 2021.

solutions, above all concerning deradicalization, should also be applied on a European scale. Moreover, on the basis of the conducted research, it will be possible to develop a concept of organisation of the system for combating terrorist threats not only in France and Poland, but also in other member states of the European Union and NATO.

Undertaking research focused on the system of combating terrorist threats requires proper organisation, planning and verification. Elementary in these activities is the methodology of research. The conducted search was based on research questions, hypotheses and the objective, which were formulated on the basis of an in-depth analysis of the research problem. The aim of the research was to improve scientific cognition and confront hypothesis with facts[6]. The research questions took the following form:

1. How to use the expertise of the French Republic in the fight against terrorism in order not to make the same mistakes in the counter-terrorism process?
2. Which of the methods and actions of France in the implementation of counter-terrorism tasks should be used in Poland and other democratic countries in Europe?
3. How can the anti-terrorism prevention in the French Republic, including the implementation of projects to combat radicalisation in prisons, on the Internet and within civil society, minimise the risk of a terrorist attack in the country?
4. Are the solutions applied in France valuable for the development of Polish anti-terrorist and deradicalisation structures?
5. In what direction should organizational, functional and normative changes for maintaining national security of the Republic of Poland go in the face of contemporary threats?

Scientific hypotheses have been set on the basis of research conducted so far and are related to the state of knowledge on terrorism[7]. In order to organize the considerations, to achieve the goal presented above and to clarify the research problem, the following research hypotheses have been adopted:

[6] Kuc B., Ściborek Z., *Podstawy metodologiczne nauk o bezpieczeństwie* (Eng. Methodological foundations of security sciences), Warszawa 2013.

[7] Johnson J.B., Reynolds H.T., Mycoff J.D., *Metody badawcze w naukach politycznych* (Eng. Research methods in political science), translation A. Kloskowska-Dudzińska, Warszawa 2010.

1. Analysis of at least some of the solutions applied in France and an attempt to implement them in Poland will enable to adjust the Polish anti-terrorist system to contemporary international threats
2. Using the methods applied in France may significantly increase the ability and effectiveness of anti-terrorist and counter-terrorist activities in Poland, especially in the context of introduction of deradicalisation programs in prisons and the use of social media.
3. Conducting activities for combating terrorist threats still at the level of their spread, especially among young people, as well as strengthening national anti-terrorist policy among the society will significantly raise the level of awareness of the threats.
4. The unique solutions introduced in France have significantly affected the number of people radicalised, with fewer terrorist attacks recorded between 2017 and 2021, which means that similar methods could be effective in Poland.
5. If, in accordance with the terrorist experience and solutions of the French Republic, the current and future conditions of international security, appropriate legal, organisational and functional changes in the anti-terrorist activity of the Republic of Poland are made, it will be possible to efficiently carry out defence activities and raise the level of national security.

The solutions presented in this article are less popular than activities carried out by special services and counterterrorist units. However, their importance is equally important in building the state's security potential. In the French Republic, threat response capabilities are being developed most rapidly and are constantly adapted to new challenges, both internal and external. In addition to the enactment of the Law on Strengthening Internal Security and the Fight against Terrorism[8] and the transformations carried out in the counter-terrorism services, a number of side measures are also relevant. These are undertaken to reduce the impact of terrorism on the functioning

[8] Loi n° 2017-1510 du 30 octobre 2017 *renforçant la securite interieure et la lutte contre le terrorisme*, JORF n°0255 du 31 octobre 2017 texte n° 1.

of the state. They are the responsibility of the municipal police (municipal guards), the prison administration, the health service or NGOs, among others. It must be emphasised that all activities bearing the hallmarks of counter-terrorism are fundamental to maintaining the security of citizens and consist of both actions aimed at eliminating the attacker and deradicalisation programmes for people fascinated by jihadist ideology.

The intentions under the provisions of the law set out the main tasks to be accomplished by the end of 2022. These are:

- intensification of activities aimed at preventing radicalisation,
- greater cooperation between security services in the fight against terrorism,
- countering radicalisation in prisons,
- providing educational support to radicalised youth as well as minors returning from the Middle East,
- improving the functioning of the justice system in the context of suppressing acts of terrorism and punishing terrorists,
- simplifying and improving procedural issues for victims of acts of terrorism.

Counter-terrorism system in the French Republic

The anti-terrorism system, which in the French Republic is referred to as the counter-terrorism system (système français de lutte contre le terrorisme), includes campaigns against not only terrorism (le plan d'action contre le terrorisme, PACT) but also radicalisation (le plan national de prévention de la radicalisation, PNPR). The General Secretariat of Defence and National Security (Secrétariat général de la Défense et de la Sécurité nationale, SGDSN) in 2018 was mandated by the Prime Minister to develop, in collaboration with the national coordinator of intelligence and counter-terrorism (Coordination nationale du renseignement et de la lutte contre le terrorisme, CNRLT), the priorities in the counter-terrorism system. No specific bodies or institutions have been singled out for specific actions, but all services and ministries that are involved in any way in maintaining security

have been brought to the forefront of the SGDSN's work[9]. International cooperation is also highlighted as a cornerstone in the campaign against acts of aggression[10]. As a whole, the anti-terrorist system is supposed to achieve the following objectives:

- to know: to better identify and understand the terrorist threat and its development;
- to obstruct: to prevent acts of violence by keeping watch on dangerous persons, stopping the financing of terrorism and resolving conflicts which give rise to terrorist threats;
- to protect: adapt the tasks of protection of persons and property in the light of the threats identified (this requires in particular the development of technological capacities and greater involvement of public and private operators);
- to deter: punish perpetrators of terrorist crimes and bring jihadists to justice;
- to increase cooperation between European countries and promote France's initiatives to combat terrorism more effectively within the European Union[11].

In analysing countries' anti-terrorism systems, in addition to identifying centres, coordinators or inter-ministerial bodies, it is always necessary to recognise the level at which decisions are taken and courses of action set. The President and the Prime Minister are formally involved in the French anti-terrorist security structure. However, the actual steps are taken at the level of ministers responsible for security or the functioning of individual areas of the economy. An extremely important role in this system is played precisely by the Minister of the Interior, who oversees the work of the Directorate-General for Internal Security (Direction générale de la sécurité intérieure, DGSI). The service was created in April 2014 following the transformation of the Central Directorate of Internal Intelligence (Direction centrale du renseignement intérieur, DCRI) created on 1 July 2008[12]. It is a counterintelligence service whose main task is to detect

[9] *Plan d'action contre le terrorisme,* Paris 2018, pp. 15–16.

[10] *Rapport: Conférence sur la lutte contre le terrorisme et la prévention de la radicalisation violente,* Paris 2016, pp. 35–36.

[11] *Plan d'action…*

[12] Décret n° 2014-474 du 12 mai de l'article 6 nonies de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement 2014 *pris pour l'application des assemblées parlementaires et portant désignation des services spécialisés de renseignement.* Article 1.

threats within the state and neutralise threats from foreign entities[13]. Its specific mission is to participate in the surveillance of radicalised individuals and groups who may resort to violence and threaten the security of the state. In addition, the primary role of the special service is to cooperate with the Anti-Terrorism Subdirectorate (Sous-direction anti-terroriste (SDAT))[14] and the Anti-terrorism Section (Section anti-terroriste (SAT))[15] in combating terrorist threats. The specificity of the DGSI[16] is its dual judicial[17] and intelligence competence[18].

It can be assumed that the counterpart of the Polish anti-terrorist system (which would have to be re-enacted, i.e. for the period 2022-2026) is the Vigipirate plan[19]. Its genesis dates back to 1978, when France and Europe faced the first waves of terrorist attacks carried out

[13] In Poland, the Internal Security Agency has similar tasks.

[14] SDAT is based in the same building as the DGSI special service. It is also part of the new counter-terrorism plan presented in January 2020, under which the counter-terrorism service works directly with the intelligence service.

[15] It is the equivalent of SDAT in the Paris police prefecture.

[16] The DGSI is systematically informed of all cases related to terrorism in France. It also coordinates investigations into acts committed abroad against French interests (embassies, French victims abroad, etc.). It cooperates on a permanent basis with the National Anti-Terrorism Prosecutor's Office (PNAT).

[17] DGSI is the only secret service in the French Republic to work directly with judicial institutions (*institution judiciaire*), including the Judicial Police (Police Judiciaire). The aim is to protect intelligence that has been collected by the service and cannot appear in court proceedings because of the secrecy clause. The essence is to protect sources, to keep secret the cooperation of third parties with the service, as well as the way in which information is acquired. Those involved in cooperation with the DGSI are assured that they will not be recognised in court. It is customary for the Judicial Police to be responsible for cooperation with the service and with the courts, acting as an intermediary. In this specificity, the DGSI has dual competences: in the intelligence and judicial spheres. In the intelligence sphere, it has to undertake activities for the benefit of the national interest in all areas of security, and in the judicial sphere - for the purposes of counterintelligence, maintaining the secrecy of national defence and cooperating with the Judicial Police (including the SDAT and SAT branches) in combating terrorist threats. DGSI also interacts with specialist police and gendarmerie services in combating cybercrime.

[18] *Les services judiciaires anti-terroristes*, https://www.dgsi.interieur.gouv.fr/la-dgsi-en-clair/decouvrir-la-dgsi/nos-missions/police-judiciaire-specialisee/services-judiciaires [accessed: 24 XI 2021].

[19] "Vigipirate" is an acronym for: *vigilance et protection des installations contre les risques d'attentats terroristes à l'explosif* (Eng. vigilance and protection of installations against the risk of terrorist attacks).

by extremist organisations and separatists. The government's Vigipirate plan was officially implemented in 1995. In its current form, it has been in operation since December 2016. It addresses the three stages of threat analysis, namely vigilance, prevention and protection[20]. Vigipirate, which is overseen by the Prime Minister, is the main tool of the French anti-terrorism system as it brings together all national actors (state, local, public authorities, private economic operators and citizens). They report to the Prime Minister and all ministers. The Ministry of the Interior plays a dominant role in the implementation of the programme[21].

The programme envisages two phases of action: the ordinary phase and the emergency phase. The basic premise of the plan is to prevent terrorist attacks, as well as to inform the public about the degree of threat and ways to protect themselves against a possible attack. It also indicates specific protective instructions to the police and security services. The latest version of the plan is based on three pillars of operation[22]. These are:

1. The development of a culture of individual and collective security, involving the entire civil society.
2. The creation of three levels of threat and their representation on a logo visible in public spaces:
   a) The vigilance level (le niveau de "vigilance") - corresponds to maintaining security and implementing precautionary measures through surveillance of certain means of transport and public places. This level may apply in a specific region.
   b) Enhanced level, tightening of security measures[23] - there is a risk of attack (le niveau "sécurité renforcée - risque

[20] Importantly, it can be extended to include other government plans to combat terrorist threats, e.g. the Pirate NRBC plan (nuclear, radiological, biological or chemical attack), the Piranet plan (IT, cyber attack), and the Piratair-Intrusair, Pirate Mer, Metropirate plans (terrorist attack in airspace, on water or in the metro).

[21] *Comprendre le plan Vigipirate*, https://www.gouvernement.fr/risques/comprendre-le-plan-vigipirate [accessed: 4 XI 2021].

[22] A. Olech, *Counterterrorism Strategies* in *Poland* and *France*, https://warsawinstitute.org/counterterrorism-strategies-poland-france [accessed: 15 XI 2021].

[23] In France, a second level is introduced during: major international events (such as sporting events, e.g. Euro 2016, United Nations Climate Change Conference [COP]), etc., major national events such as the start of the school year and holiday celebrations, after an attack on French territory or abroad, in order to urgently adapt the national protection system.

attentat") - when it is declared, the possible response of the State must be adapted to the high or even very high terrorist threat. In addition to the protection of particularly sensitive points (airports, railway stations, places of worship, etc.), additional places requiring enhanced control may be identified. This level may apply throughout the national territory and specifically involves patrolling the streets, as well as taking counter-terrorist measures such as searching homes and arresting suspects. There is no time limit.

c) Alert level - imminent threat of attack (le troisième niveau, intitulé "urgence attentat") - may be established immediately after an attack or when a terrorist group is identified and the need to locate the threat arises. This level is established for a specific period of time: during the attack. It allows the mobilisation of all services, the closure of public places, and the dissemination of information via websites, television and radio that can protect citizens in this specific crisis situation[24].

3. Implementing new measures to strengthen government action in the fight against terrorism[25]. This means implementing new measures, which may be implemented over a period of months, six months or even several years, in order to verify their effectiveness (e.g. the introduction of a higher threat level on national territory, the organisation of protection zones, and the evaluation of the application of a new law - i.e. the anti-terrorism law - in order to determine whether it should continue to be applied[26])[27].

[24] Between 2003 and 2013, four levels were in place: yellow (jaune), orange (orange), red (rouge) and scarlet (ecarlate), and from 2014-2016, two: the vigilance level (le niveau de vigilance) and the attack alert level (le niveau d'alerte attentat).

[25] L. Wicky, *Le plan Vigipirate et ses trois niveaux d'alerte*, https://www.lemonde.fr/les-decodeurs/article/2016/12/20/en-france-le-plan-vigipirate-et-ses-trois-niveaux-d-alerte_5052094_4355770.html [accessed: 4 XI 2021].

[26] Ministère de l'Intérieur, Premier bilan de l'application de la loi renforçant la sécurité intérieure et la lutte contre le terrorisme, Communique de Presse 12 II 2019.

[27] J. Sulzer, *Loi Renforçant La Securite Interieure Et La Lutte Contre Le Terrorisme, Analyse juridique critique – Mise en œuvre – Suivi du contentieux constitutionnel, 30 octobre 2017 – 29 octobre 2018*, H. Decoeur (ed.), Paris 2018.

Under the Vigipirate plan, intelligence services assess the terrorist threat and their analyses allow the General Secretariat of Defence and National Security to adopt a certain level of danger. The Vigipirate plan applies on French territory, at sea and even abroad. Some of the plan's measures can be activated outside the borders if a threat to French citizens or French interests is proven and if they are compatible with the sovereignty of the countries concerned. These measures include, for example, strengthening security around French diplomatic representations[28].

Importantly, since 12 January 2015, the protective tasks of the Vigipirate plan have been entrusted to soldiers as part of the "Opération Sentinelle" mission, which aims to secure particularly sensitive points in the country. Operations are being carried out with all security services. Initially, 10,412 soldiers and 4,700 police and gendarmes were mobilised to protect 830 locations in France most vulnerable to attacks, including: places of worship, schools, diplomatic and consular representations, press offices (they are monitored 24 hours a day). It is not insignificant that since the "Opération Sentinelle" was launched, there have been regular attacks (also of a terrorist nature) on soldiers who are in vulnerable places[29]. According to the then Minister of the Armed Forces, Jean-Yves Le Drian, the cost of maintaining the operation is one million euros a day[30]. Currently, between 7 thousand and 10 thousand soldiers are deployed in the vicinity of the most important points in the country (including the protection of critical infrastructure[31]). It is worth noting that similar systems of operations have been introduced by, among others:

---

[28] *Plan Vigipirate. Foire aux Questions*, Paris 2016, p. 3.

[29] *Comprendre...*

[30] *Attentats: „L'opération Sentinelle coûte 1 million d'euros par jour"*, http://www.leparisien.fr/faits-divers/le-drian-l-operation-sentinelle-coute-1-million-d-euros-par-jour-08-02-2015-4515903.php [accessed: 4 XI 2021].

[31] Critical infrastructures in France are facilities, centres or installations that provide services and goods essential to the life of citizens. In 2006, in order to protect critical infrastructure in France, 12 sectors of activity of the highest importance (*secteurs d'activités d'importance vitale*, SAIV) were defined, divided into four pillars: human, state, economic and technological. Key operators (*opérateurs d'importance vitale*, OIV), considered fundamental to the functioning of the economy and society, and points of critical importance (*points d'importance vitale*, PIV) have been identified. Critical infrastructure protection in France is defined as: a set of activities, essential and not replaceable, contributing

– Belgium - after the attacks of January 2015, the operation "Vigilant Guardian" was launched there on the model of the French "Opération Sentinelle"[32],
– Italy - 4800 soldiers were deployed on the streets in February 2015 to protect important public places, including the Vatican, from possible terrorist attacks[33],
– Israel - the country has deployed officers in vulnerable areas, i.e. city centres, critical infrastructure and temples, since 2015[34],
– United Kingdom - after the Manchester bombing in May 2017, it was decided to launch Operation Temperer, which placed 5100 soldiers on city streets[35].

The army's commitment to protecting the population and territory of the country is meant to be a wake-up call to terrorists. In the face of a sustained terrorist threat, it is justified. Soldiers carry out observation and monitoring tasks[36].

The French Republic carries out many anti-terrorist missions outside the country (in addition to maintaining permanent military bases[37]), mainly in North Africa in cooperation with the G5 Sahel group[38].

---

to the exercise of state authority, the functioning of the economy, the preservation of the defence potential and the security of the nation, in order to maintain the production and distribution of essential goods or services for the functioning of the state.

[32] *Deux ans après: l'image de la Défense améliorée par la présence des militaires en rue*, https://www.rtbf.be/info/dossier/explosions-a-brussels-airport/detail_deux-ans-apres-l-image-de-la-defense-amelioree-par-la-presence-des-militaires-en-rue?id=9505164 [accessed: 13 XI 2021].

[33] *Rome déploie 4 800 soldats autour de sites sensibles*, https://www.ouest-france.fr/europe/italie/antiterrorisme-rome-deploie-4-800-soldats-autour-de-sites-sensibles-3195080 [accessed: 13 XI 2021].

[34] M. Bachner, *Hundreds* of *thousands more Israelis okayed to carry guns under new rules*, https://www.timesofisrael.com/hundreds-of-thousands-more-israelis-okayed-to-carry-guns-under-new-rules [accessed: 13 XI 2021].

[35] L. Lagneau, *Terrorisme: Engagée dans l'opération „Temperer", la British Army devra faire face à de nouveaux défis*, http://www.opex360.com/2017/05/24/terrorisme-engagee-dans-loperation-temperer-la-british-army-devra-faire-face-un-defi-nouveau [accessed: 13 XI 2021].

[36] *Plan Vigipirate. Foire...*, p. 3.

[37] A. Olech, *International Military Involvement* of the *French Republic*, Warsaw 2021.

[38] Chad, Niger, Burkina Faso, Mali and Mauritania have established a formal framework of cooperation to improve security and develop counter-terrorism efforts in the region due to the proliferation of terrorist organisations.

Counter-terrorism measures are already being taken outside French territory, as the government in Paris is aware of the threat posed by migrating terrorists. The idea is to strengthen the security capabilities of the countries in the region and also to prevent terrorists from entering Europe. French soldiers are using the latest weaponry, using the same methods as in the current armed conflict[39]. It is debatable, however, whether opting for a so-called global war on terror - far beyond a country's borders - is really effective in stopping terrorists, and whether it is not sometimes a case of maintaining a conflict by force and then quickly withdrawing all troops, as in the case of France in the Barkhane mission or the Americans in Afghanistan.

Public policies in the fight against radicalisation

An important body to be distinguished in the French system is the Interministerial Committee for the Prevention of Crime and Radicalisation (Comité interministériel de prévention de la délinquance et de la radicalisation), which, together with the Secretary General (constituting the SG-CIPDR - Secrétariat général du Comité interministériel de prévention de la délinquance et de la radicalisation), deals with prevention and the fight against radicalisation and sets guidelines for government policy within the scope of the Committee's name. It supports the work of ministries and the use of budgets to stop radicalisation, separatism[40] and sectarianism[41]. It also assists in the preparation of information campaigns and conducts field activities.

The SG-CIPDR plays a key role in supporting civil society by promoting good practices and providing training to state services, local authorities, associations and citizens. Visible results of this are the organisation of training courses and workshops on, inter alia,

[39] J.-D. Merchet, *Mali: une „cinquantaine de terroristes neutralisés" par l'armée française*, „L'Opinion" 3 XI 2020.

[40] Code de la sécurité intérieure, Version en vigueur au 23 novembre 2021. Section 1: Comité interministériel de prévention de la délinquance et de la radicalisation (art. D132-1 à D132-4).

[41] Décret n° 2020-867 du 15 juillet 2020 modifiant le décret n° 2002-1392 du 28 novembre 2002 instituant une mission interministérielle de vigilance et de lutte contre les dérives sectaires, NOR : INTX2004492D, JORF n°0173 du 16 juillet 2020.

the prevention of radicalisation[42], the provision of online materials for those interested in this issue[43], the development of strategies for the state in informing and educating the public about the radicalisation process and the use of social media to reinforce government policies to combat crime and terrorism.

The public response to crime prevention and radicalisation aims to involve as many partners as possible to ensure an interdisciplinary approach to emerging challenges. In this way, the SG-CIPDR coordinates a network of actors working in cooperation with civil society to promote solidarity in countering organised crime and radicalisation. In addition, the institution operates within a European cooperation network and participates in the exchange of good practices. It represents France in the working group on radicalisation at the European Commission and at the EU Internet Forum at the European Commission.

Identifying people who have been radicalised or are in the process of doing so is essential to provide them with the support they need and to prevent terrorist attacks. However, the identification of the radicalised must be detailed enough to focus on the right people and not to include those who pose no threat. It is therefore necessary to rely on a structured and professionalised system of action at departmental level. The CIPDR is responsible for building a preventive response of a social - public nature, offering detailed information on possible radicalisation in the public space, presenting a kind of radicalisation indicators developed by experts.

As the phenomenon of radicalisation is starting to become more prevalent among young people, the government is reaching

[42] An open training session on the prevention of radicalisation was organised on 4-5 November 2021, with topics such as: the public response to preventing and combating radicalisation, key concepts of Islam, the geopolitics of the jihadist movement, the process of radicalisation: knowledge, controversies and research methods, support for deradicalisation, combating and preventing radicalisation in prisons, countering radicalisation in sport, psychiatry and radicalisation. The aim of the public events is to create a network of actors at national level, so that all potentially radicalised people can be detected in order to observe them and then provide the necessary care.

[43] Videos made available on YouTube entitled: *E-learning „Znaj, wykrywaj i zgłaszaj zjawiska radykalizacji"* (Eng. Know, detect and report radicalisation phenomena), https://www.youtube.com/playlist?list=PL2VXuAZDO9kb6gI8u4GT0v-J8nrXitELO [accessed: 22 XI 2021].

out to them, using the same channels as terrorist group recruits, i.e. through the Internet and social networks. One example of this was the launch of the #ToujoursLeChoix campaign[44]. Increasingly, young people are becoming radicalised, regardless of their background, social role and place of residence. This is being exploited by online campaigns showing that radicalisation can happen to anyone and that we need to support each other to prevent it from happening. Another approach to building confidence among citizens is the launch of e-learning courses on emerging terrorist threats and how to respond to them[45]. In addition, the DGSI describes in detail on its website how to recognise signs of radicalisation (e.g. change in dress, eating habits, gradual fading of relationships, new online interests in religions and cults)[46]. In young people, they can be the result of failing to achieve success and experiencing injustice and discrimination[47].

The involvement of a governmental actor in dialogue with society, who offers training and aims to prevent radicalisation, is an innovative solution. The use of the Internet (91% of French people have access to the Internet and 75.1% of French people have access to the Internet) is innovative. The use of the Internet (91% of French people have access to the Internet and 75.9% have an account on a social networking site[48]), the preparation of government plans and strategies on de-radicalisation[49], as well as the organisation of lectures and events, are important elements in the process of strengthening anti-terrorism measures in the country. This rather new approach to the challenges is important for building links with society and lays the foundations

[44] Eng. there is always a choice.

[45] *Faire Face Ensemble,* https://vigipirate.gouv.fr [accessed: 22 XI 2021].

[46] *Reconnaître les signes de la radicalisation violente,* https://www.dgsi.interieur.gouv.fr/la-dgsi-a-vos-cotes/lutte-contre-terrorisme/sinformer/reconnaitre-signes-de-la-radicalisation [accessed: 22 XI 2021].

[47] Since 2017, there is a specific platform for teachers to help understand the phenomenon of radicalisation: CANOPÉ - https://www.reseau-canope.fr/prevenir-la-radicalisation/ressorts-et-etapes.html [accessed: 22 XI 2021].

[48] A. Patard, *Chiffres clés d'Internet et des réseaux sociaux en France en 2021,* https://www.blogdumoderateur.com/chiffres-internet-reseaux-sociaux-france-2021 [accessed: 22 XI 2021].

[49] Comité interministériel de prévention de la délinquance et de la radicalisation, «Prévenir Pour Protéger» Plan national de prévention de la radicalisation, Communiqué du Premier ministre, vendredi 23 février 2018.

for jointly creating an environment in which terrorist threats will not have the opportunity to grow in strength. Other countries should consider launching similar initiatives that allow citizens to understand the causes of not only radicalisation, separatism and sectarianism, but also nationalism, for example. At the same time, public policy on this topic must be conducted with respect for values and with a focus on social dialogue involving theorists and practitioners.

Responding to radicalisation at departmental and national level

Since 2014, there have been two instruments at departmental level to counter radicalisation. The first - with a security profile - is the special evaluation group on Islamist radicalisation (groupe d'évaluation départemental de la radicalisation islamiste, GED)[50], created by the prefect[51] in each department to maintain the exchange of information between departmental and national authorities. The groups are above all considered to be the first operational body. They are responsible for ensuring that any person who is reported as radicalised is properly assessed and monitored. The GED cooperates with the units of the Ministry of the Interior (DGSI, police[52], Gendarmerie and judicial police) and, as necessary, with other institutions (prison intelligence, customs, border police[53], etc.). The second entity - with a social profile - is the unit for the prevention of radicalisation and family support (Cellule de prévention de la radicalisation et d'accompagnement des familles, CPRAF)[54]. Its main task is to provide social, educational, medical and psychological and even psychiatric support if it concerns radicalisation. CPRAF representatives, at departmental level, provide clarification

[50] Its powers are limited to the control of communes and departments and the management of state services operating in the department. More: M. Ofiarska, *Francja*, "Annales Universitatis Paedagogicae Cracoviensis. Studia Politologica" 2010, no. 4, pp. 88-111.

[51] It is composed of representatives of the department, the Ministry of the Interior, the police and the gendarmerie.

[52] Manily with the Service central du renseignement territorial.

[53] Central Directorate of Border Police (Direction Centrale de la Police Aux Frontières).

[54] It is composed of, among others, representatives of: the police, the Ministry of Education, the judiciary (Directorate for the Judicial Protection of Young People - Direction de la protection judiciaire de la jeunesse), social services, youth welfare associations, but it may also include representatives of the GED.

to citizens in their understanding of religion, complement the legal protection of young people and the social assistance activities for children or the probation service. The unit's activities are also family-oriented, to work with the relatives of the radicalised person. The observations carried out by CPRAF are based on the indications provided by the GED[55].

In addition, a National Centre for Assistance and Prevention of Radicalisation (Centre national d'assistance et de prévention de la radicalisation, CNAPR) has been set up at departmental level and can be contacted by people[56] who believe that someone is being radicalised. In the first two years, since its opening in 2014, the hotline of the institution was called more than 5 thousand times[57]. The information obtained by the centre is transmitted to the DGSI, more precisely to the Coordination Unit for the Fight Against Terrorism (Unité de coordination de la lutte antiterroriste, UCLAT). Once CNAPR confirms that a person is being radicalised, the information is forwarded to the department of residence so that psychological and educational support can be applied or monitoring by intelligence units can be implemented. All departmental security services obtain information on the suspect and send it to UCLAT.

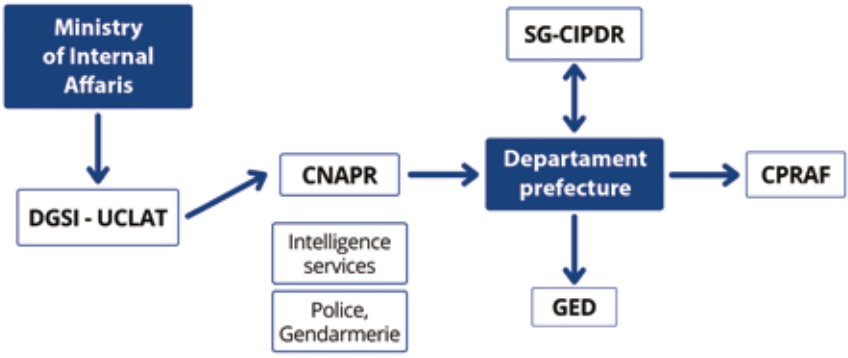


Fig. 1. Actors involved in activities implemented at national and departmental level to counter radicalisation.

Source: Own elaboration based on https://www.cipdr.gouv.fr/le-cipdr/.

[55] *Le dispositif territorial de prévention de la radicalisation violente*, https://www.cipdr.gouv.fr/wp-content/uploads/2019/06/Dispositif-territorial-de-pr%C3%A9vention-de-la-radicalisation-violente-1.pdf [accessed: 22 XI 2021].

[56] By phone or online form.

[57] *Country Reports on Terrorism 2016*, Washington 2017, p. 120.

In French legislation, the possibility of investigating radicalisation against public officials should be singled out. Article 11 of the anti-terrorism law changes the way in which action is taken to ensure internal security. The fight against radicalisation, which does not exist in the state of emergency, is a novelty in the law. An official (officer) carrying out his or her mission or profession related to security and defence can be transferred or even removed if an administrative investigation reveals tendencies towards radicalisation. The procedure also applies to military and prison officers. The new law allows action to be taken on mere suspicion and not, as was previously the case, in an already open investigation. It also involves the withdrawal of certain authorisations from the suspect. Any contradictions are resolved by a specially appointed commission (whose composition and functioning is determined by a decree of the Council of State)[58].

Moreover, in French law, the legislator has defined a new sanction - penalties for parents who incite their children to commit acts of terrorism or travel abroad for this purpose. Defining a new offence and imposing sanctions in the form of: 15 years imprisonment, a fine of 225,000 euros for parents and the possibility of losing parental rights[59] - is a precedent on a European scale[60].

The National Anti-Terrorist Prosecutor's Office

A novelty of sorts is the establishment of a procedural body that has a dominant influence on the functioning of the counter-terrorism system in France. The National Antiterrorist Prosecutor's Office (Parquet national antiterroriste, PNAT) was created on 1 July 2019. (the project emerged at the end of 2017) and its competences, although national,

[58] LOI n° 2017-1510... Art. 11.

[59] Where an act is committed by a person exercising parental authority over a minor, the court of first instance shall decide on the total or partial withdrawal of parental authority pursuant to Articles 378 and 379-1 of the Civil Code. It may also rule on the withdrawal of parental authority with respect to other minor children of that person.

[60] R. De Massol De Rebetz, M. van der Woude, *Marianne's liberty* in *jeopardy? A French analysis on recent counterterrorism legal developments*, „ Critical Studies on Terrorism' 2020, vol. 13, no. 1, pp. 1-23.

also relate to international cooperation in the fight against terrorism[61]. The PNAT has jurisdiction over such matters as crimes against humanity, war crimes, specific crimes, terrorism, distribution of weapons of mass destruction and their means of delivery, torture and kidnapping. The Public Prosecutor's Office has specific competence for the most serious crimes[62], taking over such cases from local prosecutors' offices[63]. In addition, information is provided to the institution on actions taken by other authorised entities (in accordance with the provisions of the Law on Combating Terrorism)[64]. The PNAT is staffed by judges specialised in the investigation of terrorism and extremism.

The creation of the PNAT is part of Emmanuel Macron's strategy to centralise the fight against terrorism by ensuring that the services are properly coordinated by an anti-terrorist prosecutor, to enable them to act more quickly and effectively in the event of a threat[65]. The functioning of the public prosecutor's office is a legal response to terrorist threats. Under French law, the National Anti-Terrorist Prosecutor's Office is now an autonomous, specialised structure dedicated to the fight against terrorism. Its creation was intended to consolidate the actions of the judiciary, particularly in view of the series of trials of the terrorists who carried out the attacks in 2015 and 2016 and are currently on trial. In 2019 alone, there were 87 trials related to acts of terrorism conducted by the National Anti-Terrorist Prosecutor's Office[66]. It is important to stress that not all acts of terrorism

[61] Décret n° 2019-628 du 24 juin 2019 portant entrée en vigueur des dispositions relatives au parquet antiterroriste, JORF n°0145 du 25 juin 2019 texte n° 4, NOR: JUSD1917754D.

[62] *Zoom sur le nouveau Parquet national antiterroriste,* http://www.justice.gouv.fr/justice-penale-11330/zoom-sur-le-nouveau-parquet-national-antiterroriste-32661.html [accessed: 10 XI 2021].

[63] In practice, local prosecutors, when notified that a potentially terrorist act has been committed in their area, contact the National Anti-Terrorism Prosecution Service so that the latter can assess whether it intends to use its powers in this regard in cooperation with the local authority.

[64] Code de procédure pénale: art. 628-1, art. 706-17, art. 706-169. Code de la sécurité intérieure: art. L228-2. Code de l'organisation judiciaire: art. L217-1, art. L217-5.

[65] J. Jacquin, *Vers la création d'un parquet national antiterroriste,* „Le Monde" 18 XII 2017.

[66] *Le parquet national antiterroriste, une force de frappe judiciaire,* https://france3-regions.francetvinfo.fr/paris-ile-de-france/le-parquet-national-antiterroriste-une-force-de-frappe-judiciaire-1881258.html [accessed: 22 XI 2021].

can be processed by the PNAT if there is no factual indication that it was a terrorist event[67].

Individualised de-radicalisation programme

In the process of combating radicalisation, an individualised programme of acceptance and social readmission (le programme d'accueil individualisé et de réaffiliation sociale, PAIRS) should be distinguished. Initially, a programme of research and intervention against extremism (Programme Recherches et Intervention sur les violences extrémistes, RIVE) was run, in operation since 2016, but in 2018, after a positive evaluation of its activities, its activities were extended and renamed[68]. Organised in prisons, PAIRS offers, under the supervision of the judiciary, a support system for inmates accused or convicted of acts of terrorism and identified as radicalised. This means that the project is carried out not only in prisons, but also in the homes of inmates or at points chosen by the court. The main objective is to create conditions in which the inmate rejects violence and the desire to integrate with terrorists by participating in individualised behavioural monitoring, with the involvement of a social support group (social workers, psychologists, psychiatrists, educators, as well as researchers and religious scholars) and, in exceptional cases, family and relatives. Each participant undergoes a personalised course that addresses issues such as social, professional and cultural integration, with the main objective being for the inmate to achieve intellectual autonomy rather than a total rejection of religion. The whole is based on three pillars: social, psychological and ideological. Each person participating in the deradicalisation process is evaluated every three months, and the programme can last up to a year.

[67] A man with a knife attacked four police officers, but the regional prosecutor's office concluded early in the investigation (computer check and psychiatric examination) that there were no grounds to involve PNAT. The man was charged with attempted murder. See: K. Blondelle, *Attaque de policiers à Cannes: pas de saisie du parquet national antiterroriste*, francebleu.fr/infos/faits-divers-justice/cannes-pas-de-saisie-du-parquet-national-antiterroriste-apres-l-agression-de-policiers-au-couteau-1636728441 [accessed: 23 XI 2021].

[68] M. Hecker, *Djihadistes un jour, Djihadistes toujours? Un programme de déradicalisationvu de l'intérieur*, Paris 2021, pp. 9–15.

Currently, PAIRS covers not only those who have been accused and radicalised, but also those who may undergo this process in the future. The average time spent working with clients is six hours a week, and the therapy provided can last between three and 20 hours a week. There are currently four de-radicalisation centres in the country, managed by the prison administration (Administration pénitentiaire en France[69]), which are located in Paris, Lyon, Marseille and Lille. A maximum of 50 people can be accommodated in the capital, and a total of 125 radicalised people can be accommodated by the programme nationwide. In 2019, 70 inmates took part in PAIRS, 90 in 2020 and over 110 in 2021[70].

What stands out in the deradicalisation efforts is the involvement of health services. People who suffer from mental disorders will be recorded in reports and their data will be passed on to the security services without the patients' knowledge. Cooperation will be local and information will be verified at departmental level. Data of people with mental disorders are stored in the HOPSYWEB register[71].

PAIRS was also in operation during the full closure when the COVID-19 crisis occurred, with staff connecting with those on the programme via video calls and remaining in contact by telephone. Those in care admitted that the support of professionals was very important to them when they were alone during the nationwide quarantine[72].

Currently, the biggest challenge in the functioning of the programme is to determine whether the radicalised are practising Takijja[73].

---

[69] Subordinate to the Ministry of Justice, responsible for the enforcement of court decisions in criminal matters and promoting the social reintegration of detainees.

[70] According to the Institut français des relations internationales, no person in the programme committed a terrorist act after completing it (as of February 2021). However, it must be stressed that the most radicalised people, even those who have committed or attempted murder, did not take part.

[71] Décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement, NOR: SSAP1811219D, JORF n°0117 du 24 mai 2018.

[72] M. Hecker, *Djihadistes*..., p. 54.

[73] The permission in Islam to hide one's true beliefs in the event of religious persecution (or personal danger). Taqiyyah means hiding one's religion or belief because of fear, but deep down the person must adhere to the religion he or she is hiding. In other words, it is a form of self-defence which includes defending one's life, property, respect and beliefs. According to Shariah, if one is threatened from two sides, and one of the dangers is greater, a danger of lesser consequence (e.g. lying about abandoning one's faith compared to long imprisonment) may be accepted to protect oneself.

At the same time, during several months of observation, the PAIRS support group and specialists from the special services observe the inmate, which, according to experts, should allow them to catch signs of extremism[74].

In view of the development of PAIRS, amendments to the Penal Code have been recommended to authorise the judge in charge of sentencing to extend monitoring to the prisoner after release. The main idea is to verify the radicalisation of former prisoners[75].

In prisons there are also so-called prison intelligence units (renseignement pénitentiaire), which are part of the National Service of Prison Intelligence (Service national du renseignement pénitentiaire[76]), one of whose tasks is to obtain information on persons convicted, inter alia, of offences of a terrorist nature, and to take action for the security of prisons. There are currently around 100 officers operating in the field, but this number is expected to increase by another 50 by the end of 2022.

It should be noted that French prisons were running out of places to hold people convicted of terrorism. Therefore, since 2018, the number of cells in penitentiaries for terrorists, including particularly dangerous ones, has been steadily expanded. Special single cells will be set up in 80 prisons by the end of 2022, with a target of 1,500[77].

Taqiyyah can be defined as protecting life, property and honour from the enemy. See: Shia Pen, Chapter One: Definition of Taqiyyah, www.shiapen.com/comprehensive/taqiyyah/definition-of-taqiyyah.html [accessed: 2 XI 2021].

74 *Programme de suivi des individus radicalisés: „On n'a absolument pas à rougir de ce qu'on fait en France par rapport à ce qui est fait à l'étranger",* www.ifri.org/fr/espace-media/lifri-medias/programme-de-suivi-individus-radicalises-na-absolument-rougir-de-quon [accessed: 2 XI 2021].

75 Rapport d'information fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur le contrôle et le suivi de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme. Rapport d'information n° 348 (2019-2020) de M. Marc-Philippe Daubresse, fait au nom de la commission des lois, déposé le 26 février 2020, s. 49.

76 Arrêté du 29 mai 2019 portant création et organisation d'un service à compétence nationale dénommé « Service national du renseignement pénitentiaire » NOR: JUST1911857A, JORF n°0125 du 30 mai 2019.

77 LOI n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, NOR: JUST1806695L, JORF n°0071 du 24 mars 2019.

Previously, there were programmes for the assessment and observation of prisoners convicted of terrorism and radicalised, which were implemented in selected prisons in separate and adapted parts. The first, conducted in selected pavilions, concerns the assessment of radicalisation (quartier d'évaluation de la radicalisation, QER), the second covers terrorist recidivists and those most radicalised (détenus radicalisés les plus prosélytes, QPR). Importantly, initially, women convicted of terrorism were not included in any radicalisation assessment programme[78], but now, thanks to PAIRS, there has been an increase in such measures in France.

Critics of the operation of programmes for prisoners stress their non-individualised form. Persons convicted of terrorist offences do not have the right to attend the funeral of a family member or other important moments (e.g. a serious illness in the family, a religious celebration)[79], despite their inclusion in the Code of Criminal Procedure[80]. This is due to the criminal policy of the PNAT, which maintains that the current terrorist threat requires maintaining a high level of anti-terrorism activity in the state[81].

In mid-2021, the prison administration was responsible for almost 82,000 people in France: 66,591 inmates, including 19,168 defendants who were housed in 187 prisons (occupancy rate as high as 110%) and 14,701 convicts under electronic supervision. At the end of 2021, French prisons held 454 convicted terrorists and 648 radicalised[82]. In 2020, there were 558 terrorists (522 jihadists and 36 Basque separatists) and a total of more than 1,400 inmates suspected of radicalisation were under surveillance in prisons[83].

---

[78] C. Hache, *„Plus prosélytes et violentes": les détenues radicalisées, un défi pour les prisons*, „L'Express" 5 II 2020.

[79] The equivalent of Article 141a - permission to leave prison of the Act of 6 June 1997. - Executive Penal Code (Journal of Laws of 2021, item 53).

[80] Code de procédure pénale. Version en vigueur au 16 novembre 2021. Art. 723-6.

[81] C. Cottineau, *Justice antiterroriste post-sentencielle: la tentation de la résignation*, https://www.dalloz-actualite.fr/node/justice-antiterroriste-post-sentencielle-tentation-de-resignation#.YaPYadDMI2w [accessed: 18 XI 2021].

[82] *La France dénombre „648 détenus radicalisés" dans ses prisons, affirme Éric Dupond-Moretti*, https://www.lci.fr/justice-faits-divers/terrorisme-islamisme-la-france-denombre-648-detenus-radicalises-dans-ses-prisons-affirme-eric-dupond-moretti-2195734.html [accessed: 18 XI 2021].

[83] R. Basra, P.R. Neumann, *Prisons* and *Terrorism: Extremist Offender Management*

In France, the issue of monitoring Islamist terrorists coming out of prison is also very important. By 2023. 230 of them will have left prisons: in 2020 it was 83 convicts, in 2021. - 70, in 2022 it is expected to be 50 and in 2023. - Importantly, only 29% of prisoners will be subject to individual administrative control and supervision measures[84] (mesures individuelles de contrôle administratif et de surveillance, MICAS) for a maximum of 12 months[85]. It will therefore be a priority to verify during the course of a sentence that those convicted of terrorism do not re-offend.

The deradicalisation and prisoner control programmes appear to be effective, and France has been developing its anti-terrorist structures very dynamically and wisely since 2017. However, it should be noted that the measures were taken far too late and the programmes should have been in place since 2013-2014. At the same time, the implementation of new solutions must be a signal to other countries in Europe that all kinds of manifested extremes must be countered earlier. Especially when the number of people who need to be controlled is not yet large and they have not engaged in terrorist activities.

Once again in 2020, it was stressed that the penalties for those convicted of terrorist offences who become radicalised again should be increased, by means of a higher sentence, as well as an order to undergo permanent control. In addition, it recommended several measures to be implemented on a permanent basis, in particular: the transmission of information on the surveillance of individuals to the national prosecutor's office and the territorial prosecutor's offices, giving prefects the possibility to close - even several times for the same reason - places of worship, as well as facilities that belong to legal or natural persons, the permanent control and monitoring

in *10 European Countries*, London 2020, p. 7.

84 J. Leclerc, *L'inquiétante défaillance du suivi des terroristes sortant de prison*, https://www.lefigaro.fr/actualite-france/l-inquietante-defaillance-du-suivi-des-terroristes-sortant-de-prison-20201109 [accessed: 28 XI 2021].

85 The Constitutional Council ruled on the constitutionality of the various administrative control and supervision measures (MICAS) created by the law of 30 October 2017 on strengthening internal security and combating terrorism. This is the equivalent of house arrest. See: Loi n° 2017-1510...; O. Cahn, J. Leblois-Happe, Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme: perseverare diabolicum, "Actualité juridique. Pénal" 2017, p. 468; Loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence; Décision n° 2017-624 QPC, 16 mars 2017.

of persons convicted of terrorism in order to verify their possible radicalisation, and facilitating the services' access to suspects' computer data. In the end, the intensification of counter-terrorism and anti-radicalisation measures implemented in the State to date was assessed positively[86].

Use of municipal guards or equivalent services in other countries

Due to the terrorist threats present on the territory of the French Republic, more and more municipalities are choosing to train officers. This is a new strategy that started to be implemented at the end of 2019[87]. This is due to the fact that municipal police[88] are usually on the front line when there is danger. The mayor of the municipality of Cannes said that even if responding to terrorism is not part of the municipal police officers' mandate, everyone in the municipality will undergo training by the end of 2020. In November 2019 200 Cannes police officers have been trained to respond in the event of a terrorist attack. Counter-terrorists from RAID (Recherche, Assistance, Intervention et Dissuasion) and BRI (Brigade de recherche et d'intervention) conducted a course based on a potential attack scenario at the Palais des Festivals et des Congrès in Cannes[89]. This is a very important example of actions that involve basically every actor in responding to terrorist threats. It is important to note that actions taken just before or just after an attack are critical to the security situation in the area.

When the attack in Nice in July 2016 occurred, it was, among others, the city guards who were responsible for road safety. Their knowledge of terrorist threats and the rapid transmission of information about

[86] *Rapport d'information fait…*

[87] M. Auray, *La place de la police municipale dans la lutte contre le terrorisme*, Lille 2019, pp. 1–2.

[88] Which, for the purpose of this article, is called the municipal police, and its competences are similar to those of the formations operating in Poland, Stadtpolizei in Germany, Policia Local in Spain, městská policie in the Czech Republic, Handhaving in the Netherlands or Муніципальна поліція in Ukraine.

[89] P. Renoir, F. Azur, *Cannes forme ses policiers municipaux à intervenir en cas d'attaque terroriste*, https://www.francebleu.fr/infos/faits-divers-justice/cannes-forme-ses-policiers-a-intervenir-en-cas-d-attaque-terroriste-1574963396 [accessed: 10 XI 2021].

the danger to other services meant that there were far fewer casualties[90]. In addition, they cooperated well during and after the attack with the police and the soldiers acting in Operation Sentinelle. Their appropriate movements were the result of the preparations for the EURO 2016 matches in Nice, as they had undergone five anti-terrorism training courses[91].

Municipal guards were given powers to organise and maintain protection zones in municipalities. The separation of areas (in order to maintain security during sporting, cultural and festive events as well as assemblies and demonstrations) reduces the risk of a terrorist attack by controlling access and the movement of people[92]. This is an example of using a force that is not strictly counter-terrorist in order to strengthen the state's anti-terrorist capacity. As many as 98% of municipalities in France have municipal guards.

The involvement of municipal guards is intended to strengthen the effectiveness of the social response to crises, as they know the situation in each municipality best. The officers could support the police and gendarmerie, as well as being a liaison officer to inform about the need to use counter-terrorist units or special forces, as they are already used during increased threats in the state under the Vigipirate plan[93]. Importantly, police municipale officers may be authorised to carry arms (until 2016 they did not have them) at the request of the mayor of the municipality[94]. The main purpose of their involvement is to take integrated action in the fight against terrorism, so that all measures used on the national territory are coordinated. This also includes responding

[90] It is also worth mentioning that, at the time, the officers of this formation did not have weapons at their disposal, as is the case with the police, and thus they did not manage to stop the truck in the first phase of the attack and could only pass on information about the threat to other entities.

[91] Déclaration de M. Manuel Valls, Premier ministre, en réponse à diverses questions portant sur la lutte contre le terrorisme depuis 2012, l'attentat de Nice, la prorogation de l'état d'urgence et les opérations extérieures menées par la France contre Daech, à l'Assemblée nationale le 20 juillet 2016.

[92] Code de la sécurité intérieure, Version en vigueur au 18 novembre 2021. Art. L226-1.

[93] *Lutte contre la radicalisation et le séparatisme islamiste: la ville agit pour votre sécurité!*, https://www.vernon27.fr/actualites/lutte-contre-la-radicalisation-et-le-separatisme-islamiste-la-ville-agit-pour-votre-securite [accessed: 19 XI 2021].

[94] Code de la sécurité intérieure, Version en vigueur au 19 novembre 2021. Paragraphe 1: Armes susceptibles d'être autorisées (art. R511-12 à R511-13).

to other threats in the municipality, such as organised crime. In France, it is recommended that the competencies of the municipal police are further strengthened and that they work more closely with the police[95].

NGO activities in **favour** of **victims** of **terrorism**

In addition to actions taken against terrorism or responding to an attack, it is equally important to involve people and resources in civic assistance to those affected by attacks. In the French Republic, NGOs are complementary to state institutions. Specially designated entities are tasked with supporting the country's counter-terrorism system and providing support to those in need. Selected institutions supporting victims of attacks or the impact of terrorism include:

- Association française des Victimes du Terrorisme (AfVT, French Association of Victims of Terrorism) - is funded by the European Commission and aims to establish a dialogue between victims of terrorist attacks and the general public (especially young people) in order to prevent radicalisation and promote a sense of citizenship and camaraderie in the face of terrorism. The organisation aims to provide assistance to victims of terrorism and their families. This assistance can be moral, administrative, financial, legal, medical or other. Three types of mission are carried out: psychological, legal or preventive. AfVT supervises and monitors the activities of the International Federation of Associations of Victims of Terrorism (FIAVT). It also provides online diversionary content for search engines such as Google to display to people searching for extremist topics[96].
- Association IMAD pour la jeunesse et la paix (IMAD Association for Youth and Peace) - was set up to establish inter-religious dialogue, to prevent extremist excesses, and to support secular and republican tradition[97].

[95] L'ancrage territorial de la sécurité intérieure – Rapport final, n° 323 (2020-2021), Date de remise: 29 janvier 2021.

[96] Association française des Victimes du Terrorisme, https://www.afvt.org/ [accessed: 8 XI 2021].

[97] Association IMAD pour la jeunesse et la paix, https://association-imad.fr/en/association-for-youth-and-peace/ [accessed: 8 XI 2021].

– Fédération nationale des victimes d'attentats et d'accidents collectifs (FENVAC, National Federation of Victims of Attacks and Collective Accidents) - was founded in 1994. It brings together more than 70 associations in France and abroad (Barcelona, Bardau, Ouagadougou, Marrakech, etc.). Through its experience, it shares guidance based on members' testimonies and encourages victims to come together. This support can also be individual and cover legal, administrative, psychological, social, etc. problems encountered by victims[98].
– Association 13 novembre: fraternité et vérité (13onze15, Association of 13 November: Brotherhood and Truth) - supports victims of attacks in courts and institutions. It also contributes to the commemoration of the victims of the attacks[99].
– Association Montjoye - offers social, legal and psychological support to victims. The Foundation strongly supported the creation of an information zone for the victims of the Nice bombing of 14 July 2016, in which 87 people were killed and 202 injured, in order to provide assistance as soon as possible[100].

State bodies have also been involved in financial support. Under the Law on Planning and Reform of Justice 2018-2022[101], victims of terrorism, i.e. French citizens and including public officials and soldiers, will be compensated. Funds may be awarded to victims of acts of terrorism committed both at home and abroad, as well as to the dependents of the victims, regardless of their nationality. Importantly, if a dangerous situation has occurred through the fault of the victim, compensation may be refused or reduced[102]. The money will be paid from a specially created guarantee fund (Fonds de Garantie des Victimes des actes de Terrorisme et d'autres Infractions, FGTI[103]).

[98] Fédération nationale des victimes d'attentats et d'accidents collectifs, https://www.fenvac.com/ [accessed: 8 XI 2021].

[99] Association 13 novembre: fraternité et vérité, http://13onze15.org/ [accessed: 8 XI 2021].

[100] Association Montjoye, https://montjoye.org/ [accessed: 8 XI 2021].

[101] LOI n° 2019-222…

[102] Code des assurances, Version en vigueur au 17 novembre 2021. Art. L126-1.

[103] *Les statuts du Fonds de Garantie des Victimes des actes de Terrorisme et d'autres Infractions (FGTI)*, https://www.fondsdegarantie.fr/fgti/statuts/ [accessed: 18 XI 2021].

Currently, the funds allocated by the government to help victims of terrorism amount to 30 million euros.

Financial and psychological assistance is the most important thing to support citizens in the event of a terrorist attack. Therefore, countries that are particularly vulnerable to this type of attack should improve their social support system. In Germany, there is still a problem in providing good living conditions for victims of terrorism, and legislative changes are needed here. Many people are struggling to get sufficient support from the government and insurance money because they do not have the funds for life and rehabilitation[104]. The French Republic has therefore taken the right step to help those affected.

Using social media to inform citizens

An example of a measure aimed at convincing the public to alert the authorities of a potential danger is the initiative of the Ministry of the Interior of the French Republic, which calls on people to inform the services that a person in their environment may have been radicalised, intends to carry out an attack or there is a terrorist threat. A special hotline has been set up for this purpose, so that the report can be directed to a specific entity.

Another solution to come to the fore is the use of social media as a form of information to the security services. Such measures are being introduced not only in France, but also in other countries such as Austria. During the terrorist attack in Vienna on 2 November 2020, while the police were in pursuit of the terrorist, bystanders reported on his movements. The Austrian Interior Ministry decided to have people who saw the terrorist share the information via a special form on the website to help the services locate the threat. The Austrian interior ministry asked people not to post the information on social media, which could lead to misinformation, but to pass the data directly to the police, who then distributed the verified information to citizens.

Another important element in strengthening the system for combating terrorist threats using social media is constant communication

[104] H. Rubinich, *Überlebende von Terroranschlägen. Der schwierige Weg aus dem Trauma*, https://www.deutschlandfunkkultur.de/ueberlebende-von-terroranschlaegen-der-schwierige-weg-aus-100.html [accessed: 20 XI 2021].

between the services and the public. The use of digital tools to transmit information important to citizens should be the basis for building a sense of security and stopping the growing disinformation, for example from false websites or terrorist groups[105]. It is therefore necessary to reach out to platforms that make it possible to notify risks and to pinpoint the location of attacks and zones that are dangerous. The use of the Internet for communication is widespread and the creation of an official profile exclusively for risk reporting would be of great help not only to citizens but also to tourists or migrants who are at a given moment in the region at risk[106]. This requires an official profile on these portals (one for the whole country, so that messages are not duplicated or modified on the websites of the police, the crisis management centre or the Ministry of Defence[107]), which will always present the most important and official data on risks to citizens. It would be a profile that would report on the danger and give specific guidelines, for example not to use the chosen metro line or not to go to the city centre. Moreover, such a website could be part of the state's security policy and made available through tourist portals and on embassies' websites, so that visitors to the country know that in case of, for example, a terrorist attack, they can check the official message on the Internet. It should be noted, however, that it must be operational 24 hours a day and constantly updated.

Training of medical personnel

Another very important part of the system for fighting terrorist threats is the appropriate response to an attack. In addition to the activity of the security services, the most important thing in the event of an attack

[105] S. Gliwa, A. Olech, *Republika Francuska w obliczu działalności Państwa Islamskiego. Doświadczenia płynące z ataków terrorystycznych i propagandy w mediach społecznościowych w latach 2015–2019* (Eng. The French Republic in the face of Islamic State activities. Experiences from terrorist attacks and social media propaganda in 2015-2019),„Wiedza Obronna" 2020, vol. 271, no. 2, pp. 109-130.

[106] During the terrorist attacks in 2020, the interior ministries of Austria and France constantly informed (also in Polish) on their social media profiles about the existing threat.

[107] Ministère de l'Intérieur – Alerte, https://twitter.com/Beauvau_Alerte [accessed: 19 XI 2021].

is the proper and rapid organization of medical services. In the French Republic, there are special emergency teams prepared to provide assistance during a terrorist attack, as well as to help a large number of victims. In response to an attack, special medical and firefighting teams and reserve groups (in case of further attacks) are immediately activated, as well as a crisis regulation team, which is responsible for organising patient admissions and sending mobile units (doctors and nurses). This approach does not result in too large an influx of injured people into a single hospital. In addition, doctors, nurses, police and firefighters regularly undergo joint simulations and training in order to properly undertake life-saving measures in a coordinated rescue operation.

During the Paris attacks in November 2015, the medical services handled the situation despite the brutality of the perpetrators and the horrific number of injured because they were well prepared. Already since January of the same year (after the attacks on the headquarters of "Charlie Hebdo") there was a danger that another attack could take place in France. Moreover, in 2013, protocols for action were introduced for medical emergency teams (*Service d'aide médicale urgente*, SAMU), police and fire brigades on first aid and the transport of victims in the event of a terrorist attack[108]. Proper training of the medical team has the effect of reducing the risk of death of victims, as well as sending patients to the units that will provide them with the necessary assistance (depending on the specialisation of the hospital and the availability of medics and equipment). Of all the patients who arrived at the hospital after the 13 November 2015 attack in Paris (a total of 302 people), four died, representing less than 1% of the injured[109]. The execution of a very efficient rescue operation was the result of previous exercises for medical services in the event of a terrorist threat.

Referring to the above actions, it should be stressed that currently in many countries in Europe, including Poland, there is no compulsory

[108] On the day of the attack in France, 13 November 2015, SAMU, the police and the fire service took part in an exercise simulating the organisation of emergency teams in the event of a shooting in Paris. The scenario focused on attacks involving multiple locations. In the evening, when the same medics were confronted with this situation in reality, some of them thought it was another simulation exercise.

[109] M. Hirsch et al., *The medical response to multisite terrorist attacks* in *Paris*, „The Lancet" 2015, no. 386 (10012), pp. 1–4.

training for paramedics and doctors, which would prepare them for this type of situation. Moreover, this has not been included in the planned in-service training courses. There are also no legal regulations or financial resources to carry out such exercises. At the same time, there are grassroots initiatives that offer medics to undergo a course to be able to react appropriately in a critical moment[110]. This is very important, because the behaviour of health professionals may be crucial if there is an attack. It is therefore necessary to regulate this issue legally and to take action at ministerial level to ensure that the majority of paramedics receive such training, or at least those who work in large cities where the terrorist threat is higher. Preparatory courses for paramedics and hospitals have also been introduced in, among others, Spain[111], the UK[112] and Turkey[113], countries that have already experienced terrorist attacks. This does not mean that paramedics have to operate before the threat is contained, but qualified medical staff should have the knowledge and schemes to respond and minimise losses.

[110] *Czy polscy ratownicy są przygotowani na udzielenie pomocy po ataku terrorystycznym?* (Eng. Are Polish rescuers prepared to help after a terrorist attack?), https://www.infosecurity24.pl/czy-polscy-ratownicy-sa-przygotowani-na-udzielenie-pomocy-po-ataku-terrorystycznym?fbclid=IwAR2S8FsK2p2wHhVPrU99lvUJrf9LcLnZf6fmpOhORB1RhV14NT4s3u2eJeU [accessed: 18 XI 2021].

[111] *Así funcionan los protocolos sanitarios en caso de atentados en España*, https://www.consalud.es/pacientes/asi-funcionan-los-protocolos-sanitarios-en-caso-de-atentados-en-espana_22428_102.html?fbclid=IwAR0fqXimun7oK2vbK7UCiFddJqSYfGbLRc0BKRHQ2ec_ZRuTF8Uw4LQZ41w [dostęp: 21 XI 2021]; *Simulacro antiterrorista*, https://www.diariodesevilla.es/vivirensevilla/Simulacro-antiterrorista_0_1131787221.html [accessed: 21 XI 2021].

[112] E. Skryabina, N. Betts, G. Reedy, P. Riley, R. Amlot, *UK healthcare staff experiences* and *perceptions* of *a mass casualty terrorist incident response: a mixed-methods study*, „Emergency Medicine Journal" 2021, vol. 38, no. 10.

[113] G. Tarihi, *Hastanemiz çalışanlarına Adıyaman Emniyet Müdürlüğü Terörle Mücadele Daire Başkanlığı Büro Amirliği tarafından "Terörle Mücadele" eğitimi verildi*, https://besnidh.saglik.gov.tr/TR,36418/hastanemiz-calisanlarina-adiyaman-emniyet-mudurlugu-terorle-mucadele-daire-baskanligi--buro-amirligi-tarafindan-terorle-mucadele-egitimi-verildi.html [accessed: 21 XI 2021].

Conclusion

In the author's opinion, the process of counteracting threats of a terrorist nature requires cooperation of various entities and groups at many stages. Nowadays it is not enough just to maintain a counterterrorist unit. Combating this type of aggression requires the involvement of entire societies and all the resources possessed by the state. Each of the elements supervised by the public administration has an important role to play in the process of verification and response to threats. Counter-terrorism should nowadays include a response to: the process of progressive radicalisation, the terrorist activities undertaken, and the activity of those convicted of terrorism (or other terrorist offences) who have already served their sentences. In addition, other challenges must be taken into account, such as the radicalisation of young people, the lack of access to rehabilitation programmes for inmates, insufficient support for victims of aggression and terrorism, the untapped potential of the Internet and social media, the ineffectiveness of the different uniformed formations in responding to terrorism, and the unpreparedness of medical teams in the event of an attack. All these measures can be taken in a short space of time, as many European Union countries, including Poland in particular, have the right tools and the capacity to implement them. The determinant factor should be that in France terrorism is a regular occurrence, and in Poland the threat is still low, so it may be considered a good time to prepare for an emergency now. French expertise demonstrates both mistakes and shortcomings that should not be repeated, and unique and proven solutions that should be used.

In the process of deradicalisation[114] of convicts and those who may be about to embark on terrorist activities, assistance from many groups of people is important. The 'de-radicalisation team'[115] includes: teachers

[114] Radicalisation need not necessarily take the form of a terrorist attack. Moreover, this process concerns all ideologies that take violent and aggressive actions with the intention of forcing changes in the state, leading to destabilisation, confusion and unrest. Any religion, any ideology, any political party or movement can be radicalised. This applies equally to jihadism, right-wing terrorism, left-wing terrorism, separatism, nationalism and even actions within specific communities.

[115] The author states that a nomenclature is needed for the entire team involved in supporting a person who may be influenced by a harmful ideology, and therefore proposes a name of its own.

(who can inhibit the radicalisation of young people), psychologists, guards (or supervisors) at the place of detention, co-workers, family, friends and clergy (or someone perceived as an expert or guide in the religion or ideology the person professes). These groups, if they cooperate, are in a position to help an individual who is succumbing to harmful influences. The basis of cooperation is conversation and exchange of views between team members. It does not have to have an official framework, but the necessary contact between those surrounding the radicaliser is sufficient. Just as the whole state is important in the system for fighting terrorist threats, here the team is crucial, as it can react early enough so that an attack does not take place. Furthermore, outsiders can point out worrying symptoms, which will be analysed by those surrounding the radical. This is why it is important to pay attention to increasing aggression (based on ideology) whether on the Internet or in the workplace (study). Any person can become a threat whistleblower. This does not mean that the suspect will immediately be held criminally responsible, but their behaviour can be monitored by the security services. In the French Republic, this is how the process works, which makes it much easier to take action if strong radicalisation actually occurs. This is now such a very specific danger that it requires constant vigilance and observation by all citizens.

In the fight against terrorism and in preventing violent radicalisation, governments as well as regional and international organisations face major challenges. However, through transnational cooperation they are able to respond not only to conventional but also to asymmetric threats such as extremism and organised crime. Moreover, with the dividing line between internal and external security increasingly blurred, it is necessary to re-examine the adaptation of security systems to the geopolitical situation in order to make them more effective. Using even some of the solutions applied in France will be very effective on Polish soil. The threat of an attack or radicalisation is just as possible. All that changes is the perpetrator and his motivation.

The lack of a uniform perception of the phenomenon of terrorism in France and Poland does not mean that effective methods and countermeasures cannot be identified that are appropriate for both countries. The actors responsible for counter-terrorism cannot only be called upon when a threat is detected or an attack occurs.

The overriding aim should be prevention and the creation of conditions to stop the radicalisation of particular groups and individuals. At the same time, in the event of an attack and during the reorganisation afterwards, the government should have a set of measures to mitigate the negative impact of the aggression on society. Many of the solutions presented in this paper are intended to draw attention to less popular methods of conducting the state's anti-terrorist policy, but equally important in the process of building security capacity. Additionally, the solutions described in France can be implemented and extended in Poland quite naturally, within the framework of the development of the existing tools[116]. Currently, the environment in which radicalisation and terrorist attacks take place is changing. Due to technological progress, what is happening is that terrorism is not only an attack with explosives, but also the destructive use of the Internet and social media. Consequently, recognising the methods and means that terrorists may use is extremely important in verifying the threat in order to be able to effectively eliminate it in the first phase of its development.

Strengthening the current structures for combating terrorism in Poland will be very important in the coming years due to the growing phenomenon of radicalisation[117]. Furthermore, defining already now strategies and methods to respond to challenges that are not yet as common as in France, will allow a proper assessment of the potential and skills of the different actors[118]. The evaluation carried out will also highlight inadequacies that need to be remedied and will allow the direction of change and improvement of Polish and European counterterrorism to be set.

When analysing future solutions for Poland, it is worth at the outset resuming work on the next edition of the National Anti-Terrorist Programme in order to include in it the area of radicalisation

[116] These include the launch of e-learning courses by the ABW Terrorism Prevention Centre (see: https://learning.tpcoe.gov.pl/ [accessed: 27 November 2021]) and the creation of a special prison cell with the right to surveillance (see: infosecurity24.pl/specjalna-komorka-wieziennictwa-z-prawem-do-inwigilacji [accessed: 27 XI 2021]).

[117] Collegium Civitas, *Społeczny wymiar radykalizacji – czynniki wpływające na proces radykalizacji młodych ludzi. Wnioski z badań w projekcie „DARE"*(Eng. The social dimension of radicalisation - factors influencing the radicalisation process of young people. Conclusions from the research in the „DARE" project), Warszawa 2021.

[118] A. Olech, *Walka z terroryzmem*... (Eng. Fight against terrorism...)

in a manner adequate to the results of the above-mentioned research. Thanks to that, this issue would be comprehensively developed within the existing AT system in the Republic of Poland. This would allow for the creation of a subsystem supporting the identification of terrorist threats, consisting of social initiatives, scientific and research projects and institutional solutions, which would combine the potential of information collected by local administration bodies, the Police, the Internal Security Agency or the Prison Service.

Bibliography

Auray M., *La place de la police municipale dans la lutte contre le terrorisme*, Lille 2019.

Basra R., Neumann P.R., *Prisons* and *Terrorism. Extremist Offender Management* in *10 European Countries*, London 2020.

Block L., *Evaluating* the *Effectiveness* of *French Counter-Terrorism*, „Terrorism Monitor" 2005, vol. 3, no. 17, without pagination.

Cahn O., Leblois-Happe J., *Loi n° 2017–1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme: perseverare diabolicum*, „Actualité juridique. Pénal" 2017, no. 11, pp. 468–471.

Collegium Civitas, *Społeczny wymiar radykalizacji – czynniki wpływające na proces radykalizacji młodych ludzi. Wnioski z badań w projekcie „DARE"* (Eng. The social dimension of radicalisation - factors influencing the radicalisation process of young people. Conclusions from the research in the „DARE" project), Warszawa 2021.

Country Reports on Terrorism 2016, Washington 2017.

De Massol De Rebetz R., Woude M. van der, *Marianne's liberty* in *jeopardy? A French analysis on recent counterterrorism legal developments*, „Critical Studies on Terrorism" 2020, vol. 13, no. 1, pp. 1–23.

Gliwa S., Olech A., *Republika Francuska w obliczu działalności Państwa Islamskiego. Doświadczenia płynące z ataków terrorystycznych i propagandy w mediach społecznościowych w latach 2015–2019* (Eng. The French Republic in the face of Islamic State activities. Experiences from terrorist attacks and social media propaganda in 2015-2019), „Wiedza Obronna" 2020, vol. 271, no. 2, pp. 109–130.

Hache C., *„Plus prosélytes et violentes": les détenues radicalisées, un défi pour les prisons*, „L'Express", 5 II 2020.

Hecker M., *Djihadistes un jour, Djihadistes toujours? Un programme de déradicalisationvu de l'intérieur*, Paris 2021.

Hirsch M. i in., *The medical response to multisite terrorist attacks* in *Paris*, „The Lancet" 2015, no. 386, pp. 1–4.

Jacquin J., *Vers la création d'un parquet national antiterroriste*, „Le Monde" 18 XII 2017.

Johnson J.B., Reynolds H.T., Mycoff J.D., *Metody badawcze w naukach politycznych* (Eng. Research methods in political science), tłum. A. Kloskowska-Dudzińska, Warszawa 2010.

Kuc B., Ściborek Z., *Podstawy metodologiczne nauk o bezpieczeństwie* (Eng. Methodological foundations of security sciences), Warszawa 2013.

Merchet J.-D., *Mali: une «cinquantaine de terroristes neutralisés» par l'armée française*, „L'Opinion", 3 XI 2020.

Ofiarska M., *Francja*, „Annales Universitatis Paedagogicae Cracoviensis. Studia Politologica" 2010, no. 4, pp. 88–111.

Olech A., *International Military Involvement* of the *French Republic*, Warsaw 2021,

Olech A., *Walka z terroryzmem. Polskie rozwiązania a francuskie doświadczenia* (Eng. Fight against terrorism. Polish solutions versus French experience), Warszawa 2021.

Plan d'action contre le terrorisme, Paris 2018.

Plan Vigipirate. Foire aux Questions, Paris 2016.

Rapport: Conference sur la lutte contre le terrorisme et la prevention de la radicalisation violente, Paris 2016.

Rekawek K. et al., *Who are* the *European jihadis? Project Midterm Report*, Bratislava 2018.

Skryabina E i in., *UK healthcare staff experiences* and *perceptions* of *a mass casualty terrorist incident response: a mixed-methods study*, „Emergency Medicine Journal" 2021, vol. 38, no. 10, pp. 756–764.

Sulzer L., *Loi Renforçant La Securite Interieure Et La Lutte Contre Le Terrorisme.*

Analyse juridique critique – Mise en œuvre – Suivi du contentieux constitutionnel, 30 octobre 2017 – 29 octobre 2018, H. Decoeur (ed.), Paris 2018.

Thachuk K., Bowman M., Richardson C., *Homegrown Terrorism. The Threat Within*, Washington 2008.

Internet sources

Así funcionan los protocolos sanitarios en caso de atentados en España, https://www.consalud.es/pacientes/asi-funcionan-los-protocolos-sanitarios-en-caso--de-atentados-en-espana_22428_102.html?fbclid=IwAR0fqXimun7oK2vbK7U-CiFddJqSYfGbLRc0BKRHQ2ec_ZRuTF8Uw4LQZ41w [accessed: 21 XI 2021].

Association 13 novembre: fraternité et vérité, http://13onze15.org/ [accessed: 8 XI 2021].

Association française des Victimes du Terrorisme, https://www.afvt.org/ [accessed: 8 XI 2021].

Association IMAD pour la jeunesse et la paix, https://association-imad.fr/en/association-for-youth-and-peace/ [accessed: 8 XI 2021].

Association Montjoye, https://montjoye.org/ [accessed: 8 XI 2021].

Attentats: „L'opération Sentinelle coûte 1 million d'euros par jour", http://www.leparisien.fr/faits-divers/le-drian-l-operation-sentinelle-coute-1-million-d-euros-par-jour-08-02-2015-4515903.php [accessed: 4 XI 2021].

Bachner M., *Hundreds* of *thousands more Israelis okayed to carry guns under new rules*, https://www.timesofisrael.com/hundreds-of-thousands-more-israelis--okayed-to-carry-guns-under-new-rules [accessed: 13 XI 2021].

Blondelle K., *Attaque de policiers à Cannes: pas de saisie du parquet national antiterroriste*, francebleu.fr/infos/faits-divers-justice/cannes-pas-de-saisie--du-parquet-national-antiterroriste-apres-l-agression-de-policiers-au-coute-au-1636728441 [accessed: 23 XI 2021].

Comprendre le plan Vigipirate, https://www.gouvernement.fr/risques/comprendre-le-plan-vigipirate [accessed: 4 XI 2021].

Cottineau C., *Justice antiterroriste post-sentencielle: la tentation de la résignation*, https://www.dalloz-actualite.fr/node/justice-antiterroriste-post-sentencielle-tentation-de-resignation#.YaPYadDMI2w [accessed: 18 XI 2021].

Czy polscy ratownicy są przygotowani na udzielenie pomocy po ataku terrorystycznym? (Eng. Are Polish rescuers prepared to help after a terrorist attack?), https://www.infosecurity24.pl/czy-polscy-ratownicy-sa-przygotowani-na-udzielenie-pomocy-po-ataku-terrorystycznym?fbclid=IwAR2S8FsK2p2wHhVPrU99lvUJrf9LcLnZf6fmpOhORB1RhV14NT4s3u2eJeU [accessed: 18 XI 2021].

Deux ans après: l'image de la Défense améliorée par la présence des militaires en rue, https://www.rtbf.be/info/dossier/explosions-a-brussels-airport/detail_deux-ans-apres-l-image-de-la-defense-amelioree-par-la-presence-des-militaires-en-rue?id=9505164 [accessed: 13 XI 2021].

E-learning „Znaj, wykrywaj i zgłaszaj zjawiska radykalizacji" (Eng. "Know, detect and report radicalisation phenomena"), https://www.youtube.com/playlist?list=PL2VXuAZDO9kb6gI8u4GT0v-J8nrXitELO [accessed: 22 XI 2021].

Faire Face Ensemble, https://vigipirate.gouv.fr [accessed: 22 XI 2021].

Fédération nationale des victimes d'attentats et d'accidents collectifs, https://www.fenvac.com/ [accessed: 8 XI 2021].

https://infosecurity24.pl/specjalna-komorka-wieziennictwa-z-prawem-do-inwigilacji [accessed: 27 XI 2021].

https://learning.tpcoe.gov.pl/ [accessed: 27 XI 2021].

https://www.reseau-canope.fr/prevenir-la-radicalisation/ressorts-et-etapes.html [accessed: 22 XI 2021].

La France dénombre „648 détenus radicalisés" dans ses prisons, affirme Éric Dupond-Moretti, https://www.lci.fr/justice-faits-divers/terrorisme-islamisme-la-france-denombre-648-detenus-radicalises-dans-ses-prisons-affirme-eric-dupond-moretti-2195734.html [accessed: 18 XI 2021].

Lagneau L., *Terrorisme: Engagée dans l'opération «Temperer», la British Army devra faire face à de nouveaux défis*, http://www.opex360.com/2017/05/24/terrorisme-engagee-dans-loperation-temperer-la-british-army-devra-faire-face-un-defi-nouveau [accessed: 13 XI 2021].

Leclerc J., *L'inquiétante défaillance du suivi des terroristes sortant de prison,* https://www.lefigaro.fr/actualite-france/l-inquietante-defaillance-du-suivi-des-terroristes-sortant-de-prison-20201109 [accessed: 28 XI 2021].

Le dispositif territorial de prévention de la radicalisation violente, https://www.cipdr.gouv.fr/wp-content/uploads/2019/06/Dispositif-territorial-de-pr%C3%A9vention-de-la-radicalisation-violente-1.pdf [accessed: 22 XI 2021].

Le parquet national antiterroriste, une force de frappe judiciaire, https://france3-regions.francetvinfo.fr/paris-ile-de-france/le-parquet-national-antiterroriste-une-force-de-frappe-judiciaire-1881258.html [accessed: 22 XI 2021].

Les services judiciaires anti-terroristes, https://www.dgsi.interieur.gouv.fr/la-dgsi-en-clair/decouvrir-la-dgsi/nos-missions/police-judiciaire-specialisee/services-judiciaires [accessed: 24 XI 2021].

Les statuts du Fonds de Garantie des Victimes des actes de Terrorisme et d'autres Infractions (FGTI), https://www.fondsdegarantie.fr/fgti/statuts/ [accessed: 18 XI 2021].

Lutte contre la radicalisation et le séparatisme islamiste: la ville agit pour votre sécurité!, https://www.vernon27.fr/actualites/lutte-contre-la-radicalisation-et-le-separatisme-islamiste-la-ville-agit-pour-votre-securite [accessed: 19 XI 2021].

Ministère de l'Intérieur, *Premier bilan de l'application de la loi renforçant la sécurité intérieure et la lutte contre le terrorisme,* Communique de Presse, 12 II 2019.

Ministère de l'Intérieur – Alerte, https://twitter.com/Beauvau_Alerte [accessed: 19 XI 2021].

Olech A., Counterterrorism Strategies in Poland and France, https://warsawinstitute.org/counterterrorism-strategies-poland-france [accessed: 15 XI 2021].

Patard A., *Chiffres clés d'Internet et des réseaux sociaux en France en 2021,* https://www.blogdumoderateur.com/chiffres-internet-reseaux-sociaux-france-2021 [accessed : 22 XI 2021].

Programme de suivi des individus radicalisés: „On n'a abolument pas à rougir de ce qu'on fait en France par rapport à ce qui est fait à l'étranger", www.ifri.org/fr/espace-media/lifri-medias/programme-de-suivi-individus-radicalises-na-absolument-rougir-de-quon [accessed: 2 XI 2021].

Reconnaître les signes de la radicalisation violente, https://www.dgsi.interieur.gouv.fr/la-dgsi-a-vos-cotes/lutte-contre-terrorisme/sinformer/reconnaitre-signes-de-la-radicalisation [accessed: 22 XI 2021].

Renoir P., Azur F., *Cannes forme ses policiers municipaux à intervenir en cas d'attaque terroriste,* https://www.francebleu.fr/infos/faits-divers-justice/cannes-forme-ses-policiers-a-intervenir-en-cas-d-attaque-terroriste-1574963396 [accessed: 10 XI 2021].

Rome déploie 4 800 soldats autour de sites sensibles, https://www.ouest-france.fr/europe/italie/antiterrorisme-rome-deploie-4-800-soldats-autour-de-sites-sensibles-3195080 [accessed: 13 XI 2021].

Rubinich H., *Überlebende von Terroranschlägen. Der schwierige Weg aus dem Trauma,* https://www.deutschlandfunkkultur.de/ueberlebende-von-terroranschlaegen-der-schwierige-weg-aus-100.html [accessed: 20 XI 2021].

Simulacro antiterrorista, https://www.diariodesevilla.es/vivirensevilla/Simulacro-antiterrorista_0_1131787221.html [accessed: 21 XI 2021].

Tarihi G., *Hastanemiz çalışanlarına Adıyaman Emniyet Müdürlüğü Terörle Mücadele Daire Başkanlığı Büro Amirliği tarafından „Terörle Mücadele" eğitimi verildi,* https://besnidh.saglik.gov.tr/TR,36418/hastanemiz-calisanlarina-adiyaman-emniyet-mudurlugu-terorle-mucadele-daire-baskanligi--buro-amirligi-tara-findan-terorle-mucadele-egitimi-verildi.html [accessed: 21 XI 2021].

Wicky L., *Le plan Vigipirate et ses trois niveaux d'alerte,* https://www.lemonde.fr/les-decodeurs/article/2016/12/20/en-france-le-plan-vigipirate-et-ses-trois-niveaux-d-alerte_5052094_4355770.html [accessed: 4 XI 2021].

Zoom sur le nouveau Parquet national antiterroriste, http://www.justice.gouv.fr/justice-penale-11330/zoom-sur-le-nouveau-parquet-national-antiterroriste-32661.html [accessed: 10 XI 2021].

Legal acts

Arrêté du 29 mai 2019 portant création et organisation d'un service à compétence nationale dénommé „Service national du renseignement pénitentiaire" NOR: JUST1911857A, JORF n°0125 du 30 mai 2019.

Code de la sécurité intérieure.

Code de l'organisation judiciaire.

Code de procédure pénale.

Code des assurances, Version en vigueur au 17 novembre 2021.

Comité interministériel de prévention de la délinquance et de la radicalisation, „Prévenir Pour Protéger" Plan national de prévention de la radicalisation, Communiqué du Premier ministre, vendredi 23 février 2018.

Décision n° 2017-624 QPC, 16 mars 2017.

Déclaration de M. Manuel Valls, Premier ministre, en réponse à diverses questions portant sur la lutte contre le terrorisme depuis 2012, l'attentat de Nice, la prorogation de l'état d'urgence et les opérations extérieures menées par la France contre Daech, à l'Assemblée nationale le 20 juillet 2016.

Décret n° 2014-474 du 12 mai de l'article 6 nonies de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement 2014 pris pour l'application des assemblées parlementaires et portant désignation des services spécialisés de renseignement.

Décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement, NOR: SSAP1811219D, JORF n°0117 du 24 mai 2018.

Décret n° 2019-628 du 24 juin 2019 portant entrée en vigueur des dispositions relatives au parquet antiterroriste, JORF n°0145 du 25 juin 2019 texte n° 4, NOR: JUSD1917754D.

Décret n° 2020-867 du 15 juillet 2020 modifiant le décret n° 2002-1392 du 28 novembre 2002 instituant une mission interministérielle de vigilance et de lutte contre les dérives sectaires, NOR : INTX2004492D, JORF n°0173 du 16 juillet 2020.

L'ancrage territorial de la sécurité intérieure – Rapport final, n° 323 (2020-2021), Date de remise: 29 janvier 2021.

Loi n° 2017-1510 du 30 octobre 2017 renforçant la securite interieure et la lutte contre le terrorisme, JORF n°0255 du 31 octobre 2017 texte n° 1.

Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, NOR: JUST1806695L, JORF n°0071 du 24 mars 2019.

Loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence

Rapport d'information fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur le contrôle et le suivi de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme. Rapport d'information n° 348 (2019-2020) de M. Marc-Philippe Daubresse, fait au nom de la commission des lois, déposé le 26 février 2020

DOI: 10.4467/27204383TER.22.014.15430

ORCID: 0000-0003-4649-589X

ANNA ROŻEJ

The role and importance of information from open sources in increasing vulnerability to security threats in cyberspace, with particular reference to cyberterrorism

Abstract

The aim of the article is to present how the role and importance of open source information has increased in recent years as a significant part of the functioning of societies has moved to the world of Internet. Unfortunately, along with this trend, new threats have emerged, including those of a cyberterrorist nature, which require immediate action to limit their impact on information security.

Keywords:

information security, open source, infosphere, threats, information warfare, critical infrastructure

Over the past decade or so, the dynamically changing environment in which people function has led to radical changes in almost every environment, including the security environment. The memorable attacks on the World Trade Center in New York and the Pentagon in Washington, D.C., over 20 years ago, should be considered a marker of change in the perception of security on a global scale. Immediately after the attacks, most NATO member states, including Poland, were forced to implement elements of their national defence preparedness systems. This tragedy also became a source of deep reflection for the international community, encompassing both the causes and consequences of this event, which, in terms of international relations, can be considered a watershed. The attacks on the World Trade Center and the Pentagon caused a thorough reorientation of all the national systems of Western countries, especially in terms of cooperation with other states and international organisations, including NATO. It can be said that this was a kind of breakthrough since the Cold War. It was not until the attacks of 2001 that the need for reform of the national security systems, which were stuck with 20th century solutions and were unsuited to the challenges of the post-millennium world, was recognised.

The assassination of the symbols of American power proved unequivocally that "(...) today's threats are of a different nature and scale than before, and the contemporary response to these threats is inadequate. Weapons designed to counter threats at the end of the last millennium will not be able to meet them in the first decades of the 21st century. New, often asymmetric, threats to global security require new thinking"[1].

At the same time, legitimate organisations operating across state lines are also gaining in power and influence, with the technical capabilities to adapt to the new security environment. Stock speculators, traders, multinational corporations, and Internet service companies now have the potential to have a significant global impact on the daily lives of citizens in many countries. Globalisation and the revolution in information technology have given these institutions an advantage. Their control is exercised more through financial markets than through

[1] Hall R., Fox C., *Ponownie przemyśleć bezpieczeństwo* (Eng. Rethinking security), „Przegląd NATO" zima 2001/2002, p. 8.

global structures, and distortions arise along the same lines. It should therefore come as no surprise that the traditional mechanisms of the state based on the idea of borders, order, authority, police, and force structures are under threat. They also seem inherently incapable of countering contemporary security challenges. As this incapacity becomes more apparent, disillusionment with the previous system grows and a belief can arise that everything in the security field is heading for the worse, which of course cannot be allowed to happen.

More often than not, it is very difficult to identify a leader or region on which to focus attention to counter threats. Moreover, the scale of these threats is so large that it is becoming dangerous for many countries. Indeed, these threats know no national or continental boundaries. There is also a fundamental difficulty in properly identifying phenomena (organisations, leaders) in order to counter them effectively. These threats can undermine the essence and foundations of the functioning of national and international institutions, and destroy the economies of many countries.

The need for a new approach to security was pressing, as terrorism is only one of many non-traditional security challenges. Ethnic and religious conflicts, drug trafficking, mass migration, regional instability, money laundering, the activities of various extremist groups, information theft, and disinformation itself also pose them. Meanwhile, the cybersphere has just emerged, and it has reached a tremendous growth rate, causing selected powers to recognise the need to reform their defence systems. As a result, separate types of army - cyber armies, among others - began to emerge. The cybersphere has shifted the focus of security from physical warfare to response and the development of resources to counter cyber attacks, as well as pre-emptive action in cyberspace.

Taking into account the considered issue, it was assumed that the subject of research conducted within the framework of this article will be the information from open sources analysed in the context of potential threats. The presented object of research is a determinant of the goals of the research process, which are seen in theoretical and practical terms. The theoretical objective is to develop and complement the content relating to both the theory and practice of cyber security in the specific case of using online open sources. The achievement of the theoretical goal is to contribute to the practical

goal, which will provide useful solutions for ensuring and maintaining information security. The presented problem situation, the subject of the research and its goal clearly define the main research problem, which boils down to answering the following question: has the global publicity and general accessibility for all Internet users at the same time of information from open sources concerning state security increased their vulnerability to cyber attacks? The solution to the research problem will depend on the solution to specific problems, which boil down to answering the following questions:

1. What changes have occurred in the security environment?
2. How have attitudes towards the Internet changed over the last few years?
3. What is open source and what are its specificities?
4. What are the potential risks of using information from open sources?
5. What preventive measures are possible to prevent information security risks?

Preliminary conclusions from observations and analysis of available documents and literature on the subject, as well as the stated aim of the research and research problems determined the working hypothesis, thanks to which it will be possible to carry out the research process: the development of the Internet and the increased interest in open sources are connected with the increase in threats of a cyberterrorist nature.

As Henry Kissinger - prominent American politician and diplomat, national security advisor to President Richard Nixon - used to say: "Security is the foundation of everything we do"[2] and it is hard not to agree with this argument. However, in the era of enormous technological development, access to advanced processes and equipment, it may seem that security concerns are receding into the background. It is the tools and capabilities that are important, rather than one of the most important values - safety. As almost every aspect of life has moved to the internet, we are exposed to many cyber threats, and the level of feeling of security, especially ICT security, has decreased significantly. There is a huge risk that the data we collect and the information we process will become the target of cybercriminals.

[2] Kissinger H., *Dyplomacja* (Eng. Diplomacy), Warszawa 2016.

One of the first theorists of the art of war, Sun Tzu, who lived 25 centuries ago in China, in his treatise *The Art of War*, states that "(...) the highest skill in the art of war is to subdue the enemy without a fight"[3]. At the same time, he gives many tips on how to achieve this desired state. Aiming to achieve success in war, one should, among other things, discredit everything that is good in the enemy's country, involve the representatives of the enemy's ruling classes in criminal enterprises, tear up their good name and, at the right moment, throw them into the mercy of the compatriots' contempt. It is also legitimate to disorganise the activities of the adversary government and to cause feuds and discord among the citizens of the enemy country. The Indian treatise *Arthashastra* by Chanakya Kauṭilya should also be noted. This Indian philosopher and war theorist, apart from assigning a major role in foreign policy to spies and traitors, introduced a rule of warfare according to which it should be permissible to start a war only when comparative analysis of both sides shows that victory is certain. Factors such as wisdom, plan, a strong and well-trained army, high morale and overall potential are the guarantors of success. Kautilya also pointed out that the conquered population must be treated gently in order to have lasting control over them.

In the information security environment, the underlying cause of change can be traced in particular to the information revolution, which introduced various technologies that allowed for the acquisition and distribution of information on a mass scale. This phenomenon had a breakthrough character, due to the global scale of influence of these technologies. The above-mentioned consequences of the information revolution causing immense changes made the infosphere, understood as a synonym of information space and information environment, a subject of security sciences[4]. In the scientific environment the infosphere is understood as the entirety of information resources to which a given entity has access. The analysis of the information society in the aspect of cybernetic system indicates that the infosphere is divided into a local layer, which corresponds to local information resources created along with the development of the local community,

[3] Sun Tzu, *Sztuka wojny* (Eng. Art Of War), Gliwice 2004.

[4] Sosińska-Kalata B., *Obszary badań współczesnej informatologii* (*nauki o informacji*) (Eng. Research areas of contemporary informatology (information science)), „Zagadnienia Informacji Naukowej" 2013, no. 2, pp. 9–41.

and a global layer composed of global resources, which is much more than the information sum of local resources[5]. The beginning of the information society is seen in the 1960s and 1970s. It emerged as a result of the industrial revolution, during which computers were introduced and computerisation developed[6]. For the first time the term "information society" (Jap. *johoka shakai*) was first used by Tadao Umesao, a Japanese scientist, to describe a society that started using computers for communication in the era of digital and microelectronic development. The concept was later developed by Daniel Bell, who believed that for the society of that time the strategic resources were knowledge and information rather than labour and capital[7].

In recent years the infosphere, apart from becoming a permanent feature of globalisation, has become enormously more important by encompassing a much greater amount of available information of a universal nature than just a few years ago. The challenge has become not only the mass and excess of information, but above all its characteristics, such as unreliability, irrelevancy and untruthfulness. The multiplicity of information channels and sources means that the aforementioned characteristics are now intensifying.

Moreover, the information revolution and the accompanying intensely developing technology, the dynamics of life, and more recently the pandemic caused by the SARS-CoV-2 virus have meant that almost all of everyday life has been transferred to the world of the Internet, which on the one hand offers great opportunities, but on the other generates many security risks, on a national and international scale. "As soon as new information techniques spread and were adopted by different countries, different cultures, different organisations and different purposes, there was an explosion of different types of behaviour and uses, which in turn contributed

---

[5] Sienkiewicz P., *Społeczeństwo informacyjne jako system cybernetyczny*, w: *Społeczeństwo informacyjne. Wizja czy rzeczywistość?* (Eng. Information society as a cybernetic system, in: Information Society. Vision or Reality?), vol. 1, L.H. Haber (ed.), Kraków 2004, s. 79.

[6] Nowak J.S., *Społeczeństwo informacyjne – geneza i definicje*, w: *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz* (Eng. Information society - origins and definitions, in: Information Society. One step forward, two steps back), P. Sienkiewicz, J.S. Nowak (ed.), Katowice 2008, p. 25.

[7] http://www.bbc.uw.edu.pl/Content/20/08.pdf [accessed: 25 XI 2021].

to technological innovation, accelerating the pace and extending the reach of technological change, as well as diversifying its sources"[8]. The quoted statement of the Spanish sociologist Manuel Castells proves that the contemporary society is indeed an information society, which has been almost entirely dominated by telecommunication systems used for sending, receiving and processing information. Information is now an integral part of social and economic life and is present in every area of human functioning.

It should be noted that the manifestations of social life are most intense in large spaces, such as, for example, urban centres, airports or transport routes. Modern societies, on the other hand, prove that these places do not have to exist in reality, because it is enough that they are only an infrastructure or a communication platform that creates the conditions for organisations or various other entities to connect with each other in real time. Communication theorist Marshall McLuhan also recognised the changes in society during the information revolution. He believed that thanks to close online relationships, the world is becoming a global village where people can connect and communicate in real time[9]. We did not have to wait long, and the era of personal computers, the Internet and smartphones arrived, without which no one can imagine functioning today. Thanks to the technological solutions that have emerged, it is possible to communicate with anyone regardless of their location.

As a result of the enormous dynamism of the processes which have taken place over the last few decades, the Internet is now the largest source of information, which consists of an open part - publicly accessible, and a dark part - the so-called Darknet, access to which is somewhat limited, but with the use of appropriate technologies also possible.

The desirability of the Internet as a source of information is demonstrated by data froma report published in 2018 by the ITU (International Telecommunication Union)[10]. Well, already then, more than half of the world's population had access to the Internet.

[8] Elliott A., Castells M., *Społeczeństwo sieci,* w: Elliott A., *Współczesna teoria społeczna. Wprowadzenie* (Eng. Network society, in: Contemporary social theory. Introduction), Warszawa 2011.

[9] Ibid, pp. 311–319.

[10] *Measuring the Information Society Report*, t. 1, Geneva 2018.

At the end of 2018, almost 51.2 per cent, or 3.9 billion people, were using it. This represented a significant step towards even greater development of the global information society. It was estimated that in developed countries, 4 out of 5 people had direct and unlimited access to the web. In developing countries, about 45% of the population had access to the Internet, and in the least developed countries only 20%. However, according to ITU predictions, there is a continuous upward trend in access to the Internet. This is confirmed by the data given in the Global Digital Report[11] on the state of digitisation of society in January 2021, which is presented in Figure 1.

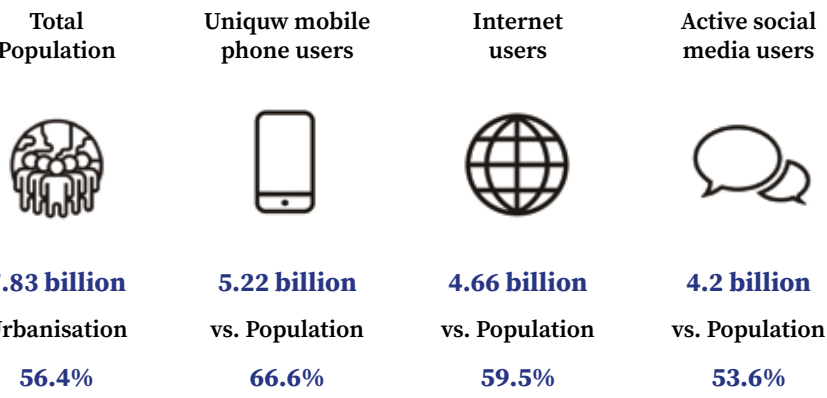


Fig. 1. Global digitalization in January 2021.

Source: DataReportal - Global Digital Insights.

Characterizing the data presented in Figure 1, it is important to note that:

- **Population**: the global population was 7.83 billion.
- **Mobile**: 5.22 billion people used a mobile phone, representing 66.6 per cent of the global population. The number of mobile users increased by 1.8 per cent since January 2020. The total number of mobile connections increased by 72 million to reach 8.02 billion by early 2021.

[11] https://datareportal.com/reports/digital-2021-global-overview-report [accessed: 26 XI 2021].

- **Internet**: 4.66 billion people worldwide used the Internet, accounting for 59.5 per cent of the global population. This represents an increase of 316 million over the year.
- **Social media**: there were 4.2 billion social media users worldwide. This number has increased by 490 million since January 2020. The number of social media users accounted for more than 53 per cent of the global population.

Furthermore, the following facts also prove that the Internet is one of the most common sources of data:

- The number of social media users is constantly increasing. It currently stands at around 4.48 billion (Figure 2).
- The platforms belonging to the Facebook family (Facebook, WhatsApp, Instagram, Messenger) are hugely popular (Figure 3).
- The time spent using the Internet is increasing (Figure 4).
- The time spent using social media is increasing (Figure 5).

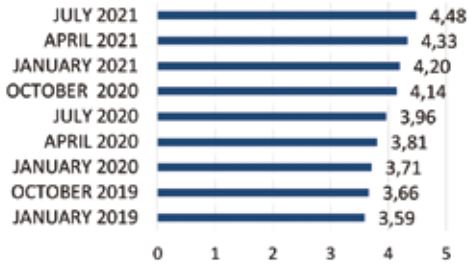


Fig. 2. The increase of social media users between 2019 and 2021 (in billions).

Source: DataReportal, DataReportal - Global Digital Insights.

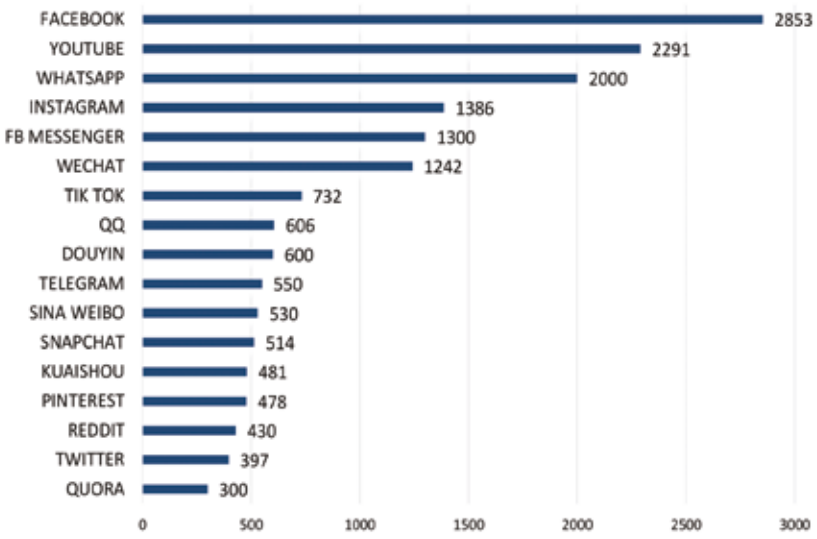


Fig. 3. Users of most popular social media in millions (updatet in July 2021).

Source: DataReportal, DataReportal - Global Digital Insights.

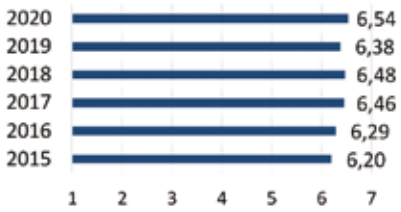


Fig. 4. The increase of time spent daily on using the Internet (in hours) by users at the age of 16–64 in the years 2015-2020.

Source: DataReportal, DataReportal - Global Digital Insights

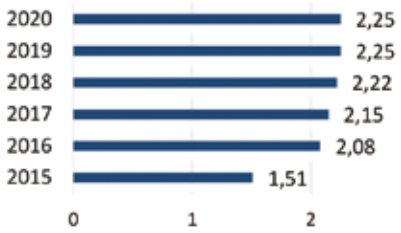


Fig. 5. The increase of time spent daily on using social media (in hours) by users at the age of 16–64 in the years 2015-2020.

Source: DataReportal, DataReportal - Global Digital Insights.

The most popular reasons why people go online include:
- seeking information;
- staying in touch with friends and family
- having up-to-date data and information;
- looking for tips on how to perform certain activities;
- watching movies, television.

Detailed data is shown in Figure 6.

Fig. 6. Primary reasons for using the Internet by users at the age of 16–64.
Source: DataReportal - Global Digital Insights.

On the basis of the data presented above indicating the enormous activity of the global society on the Internet and its constant growth, it should be stated that the aforementioned network is the largest collection of information, often of a strategic nature. No wonder that information has become the most important resource determining the functioning and success of almost every organisation or enterprise. It is a resource that constitutes the basis of activity, ensures competitive advantage and gives a sense of security. The universality of information and its almost unlimited availability result, among other things, from the fact that its source is often open. Researchers and experts in the area of intelligence activities define open source as an entity or object characterised by qualities that enable it to generate information

allowing for its legal processing, including its recording, transmission or collection[12]. Information from open sources is of primary or secondary nature, which may also generate certain limitations. Information originating from a primary source may have limitations related to the possibilities of its dissemination, if, for example, it is classified or private information. However, if the information is obtained from secondary sources - publicly available, its openness is no longer a problem[13]. It should be noted that although information from open sources is available, the recipient rarely has full knowledge of its sources and characteristics. Another definition points out that open sources are all written, audiovisual or IT means of disseminating information[14]. Open information sources can be classified in several ways, taking into account the relationship between the importance of the information and the value of the source. In practice, however, what is most often taken into account is the type of medium used to convey the information, which may be due to the fact that media vary in quality and titles are published in different ways. For example, on the Internet the user may find information that appeared on television or in newspapers, and vice versa. However, this information may appear in articles with different titles.

Technological development, as well as increased access to the Internet, has meant that open sources of information have also evolved. Examples of open sources are presented in the table.

Table. Examples of open sources.

OPEN SOURCES			
Domains (e.g. registers, lists, WHOIS)	Maps (e.g. Provincial Spatial Information Systems)	Individuals (e.g. surnames - surnames-polskie.pl, Public Information Bulletin)	Users/logins (e.g. Albicla, Allegro, Fotka)

[12] Saramak B., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy* (Eng. The use of open sources of information in intelligence activities: history, practice, perspectives), Warszawa 2015 pp. 22–23.

[13] West Ch., *Competitive intelligence,* New York 2001, p. 50.

[14] Oleński J., *Ekonomika informacji* (Eng. Economics of information), Warszawa 2001, p. 49.

Social networking sites (e.g. Facebook, Albicla, Fotka)	Dating sites (e.g. Sympatia, eDarling)	Companies/organisations (e.g. CEIDG, eKRS, Rejestr.io)	Society (e.g. Local Data Bank - CSO, Demography Database - CSO)
Business/economy (e.g. Allegro, WSE)	Archives (e.g. IPN Archive Inventory, National Digital Archive)	Translation (e.g. Electronic Dictionary of the Polish Language)	Public registers (e.g. Data Bank, Public Procurement Bulletin)
Law (e.g. Official Journals, Internet System of Legal Acts)	Universities (e.g. POL-on, RAD-on)	Transport (e.g. CEPiK API, EPKT Spotters)	Dark web (Active TOR Sites)
Documents (e.g. chomikuj.pl)	Video (e.g. Kamery.edu.pl)	Photos (e.g. Fotosik.pl)	Telephone numbers
Phone books (e.g. Service provider, Who called)	SIGNIT (e.g. WebSDR)	OpSec (e.g. IT Generators, GenApps)	Knowledge base (e.g. blogs, courses, presentations)

Source: Own elaboration.

Each of the above sources can be divided into individual subcategories, and the element which links them all is the Internet. However, when looking for reliable information on the Internet, one should approach it with great caution and not forget about other sources from the printed categories, such as books, newspapers or magazines. Moreover, it is worth noting that the Internet is not only information services, but also very popular and widespread social networking sites that ensure the functioning of various thematic environments, interest groups, as well as dictionaries, encyclopedias, forums or blogs. All these sources contain a wide variety of information. In addition, open sources allow access to private photos, satellite images and geolocation data. Although these sources are primarily open, accessible and public, it is prudent to keep a reasonable distance from them and to verify them.

It is worth being aware that search services, one of the most popular functionalities of the Internet, are based on the use of specialised software, which is responsible for exploring Internet databases. The most popular mechanisms include:

- mechanical indexing of words and phrases – AltaVista/Yahoo, Google, HotBot;

- arbitrary cataloguing of documents according to an accepted thematic classification - Yahoo;
- services that search documents from discussion groups - AltaVista Usenet;
- metasearch - a tool using individual search engines - MetaCrawler, MetaFIND;
- search using specialised databases - Alphasearch;
- others.

Despite the existence of such specialised technology, when reviewing open sources, including websites, it is important to assess them each time for credibility. To do this, it is useful to ask yourself five basic questions: who?, what?, where?, when?, why?

In order to find the answer to "who?" - you can analyse the site to look for authors, specific names or detailed information. It is also good practice to check domain types - .com/.org/.gov/country code - and assess whether the type is appropriate for the content presented. If the site from which the information is taken is a personal site or a user's social networking site, it would be useful to identify who is responsible for entering the content and, if possible, analyse the source code of the site, where the author's name is often written. Then, in order to verify the reliability of the information, it would be necessary to check who owns the server on which the page is hosted and whether the information gathered is consistent. A good method to check the credibility of the given content is to look for opinions of other users, as well as to trace the distribution of the information, for example by verifying the number of shares.

When checking a given website, you should pay attention to the content it contains, i.e. try to answer the question "what?". In order to be able to assess the truthfulness of the posted content, it is necessary to verify sources, dates, and whether the content is not changed with respect to, for example, quoted sources. A very important feature of information is its timeliness, i.e. answering the question "when?". Therefore, one should check when the information was posted, when it was updated or how often it is updated. Gathering answers to the above questions will make it possible to assess whether the information coming from open sources is, above all, true, reliable and up-to-date.

The statistical data presented in the first part of the article show that with the growing number of population with access to the Internet, it is a tool for posting, searching and exchanging information. Moreover, Internet resources are easily and quickly supplemented by Internet users. Therefore, anyone can be both a recipient of information and its author. In order to identify the attributes of open sources, it is necessary to indicate:

- availability,
- low cost of acquisition,
- uncertain reliability,
- lack of dependence,
- low risk,
- openness.

The above features, in a way, answer the questions about the number of open sources and, above all, the amount of information collected and processed in them. One example is the social networking site Facebook.com, which currently has around 2.8 billion active users monthly, with around 1.84 billion daily visitors. Since the beginning of 2021, the number of Facebook users has increased by around 12 per cent. This scale illustrates how much information appears on the portal at the same time.

The information presented so far indicates that the reach and accessibility of open sources is enormous. Today, more than half of the world's population has access to the Internet through computers, smartphones or other devices. The technological revolution that has taken place in this field has undoubtedly increased the quality of life and thus also the digital competences of international society. It is now difficult to imagine professional or private life without access to the web. Looking from the perspective of development in the economic and social area, the current situation should only be a reason for satisfaction and pride. After all, access to so much information is the basis for further development, new opportunities and chances.

Unfortunately, the development of cyberspace, in which a huge amount of information is processed, also brings with it the development of cyberterrorism. Just as cyberspace has no borders, terrorism has an unlimited range, which allows cybercriminals to undertake and successfully carry out cyber-terrorist activities on the Internet. A permanent feature of cyberterrorism is the invisibility of its actions

and, to some extent, its effects, which cannot be said of terrorism in its conventional form. Most often, the Internet user does not notice the cyber attack and is not aware of it. An attack becomes apparent when, for example, the ICT systems of strategic facilities responsible for critical infrastructure are blocked. Unfortunately, these threats are very poorly measured or not measured at all. The problem also lies in the fact that cyber-terrorists are adversaries against whom it is difficult to apply any international conventions on military action by states, as it is not really clear who the adversary is. The need for legislation in this area is certainly a priority for every state, as well as international organisations. The development of cyberspace has meant that states have lost the ability to fight this invisible adversary, and there is no legal basis to trigger international cooperation to identify the enemy and their status.

Only a dozen or so years ago, we as a society were very impressed by ICT developments and the digitisation of many areas. However, new threats to 21st century security, such as cybercrime as well as cyberterrorism, among others, have led to a review of such an enthusiastic attitude. 'Cybercrime' is defined as any illegal behaviour carried out by means of electronic activities targeting the security of computer systems and the data they contain. It also includes illegal activities carried out on or in relation to a computer system or network, including crimes such as illegal possession, offering or distribution of information via a computer system or network. Such crimes may include, but are not limited to, fraud, forgery, industrial espionage, sabotage and extortion through computer piracy and other intellectual property crimes. Cyberterrorism, on the other hand, includes attacks on public safety, life and electronic warfare against critical infrastructure. Cyberterrorism also uses new information technologies or cyberspace for traditional activities[15].

Previously, cyberterrorism was more associated with banking systems, identity theft or computer system viruses. An example of the scale of cyberterrorism at the time can be seen in the events that took place in Estonia in 2007. A cold war of a cyber nature was fought over the attempt to move a monument to the so-called Bronze Soldier, which commemorated Soviet servicemen. At the time, it was not the conflicts

[15] http://unicjin.org/documents/congr10/10e.pdf [accessed: 27 XI 2021].

in the streets that were the major threat, but the massive attacks on government and private servers. They caused widespread paralysis by blocking banking systems, information services and government websites. The scale of these events is reflected in the words of former Estonian President Toomas Hendrik Ilves, who stated that: "These days you don't need missiles to destroy infrastructure. You can do it online". Estonian society learnt then that the Internet offers many opportunities, but it can also take away the ability to function properly. The transfer of life to the world of the Internet means that cyberterrorism is constantly evolving and extending its reach into new areas of operation. According to the literature on the subject, "cyberterrorism" "(...) is a politically motivated attack or threat of attack aimed at an information system, specific data. The purpose of an attack can vary from destroying information to, for example, making it available to achieve political or social goals. Nowadays, cyberterrorism is not only typical terrorist attacks in cyberspace, nowadays it also includes such activities as propaganda, disinformation, espionage, online surveillance, manipulation of information, called soft cyberterrorism"[16].

It should be noted that all the negative phenomena that can be encountered every day in "real life" can occur in cyberspace. Theft, fraud, manipulation, espionage are just examples of the threats that can be faced in cyberspace. Physical destruction of servers contributing to disruption of systems can be an example. Hackers can achieve a similar goal by introducing malware. This malware can be a virus, Trojan horse, ransomware, exploit, rootkit, keylogger or backdoor. All of these examples of malware are capable of blocking ICT systems, depriving users of access to information. At the same time, their mode of action is secret, which makes them very difficult, and in some situations even impossible to detect.

It is worth noting that information and data in open sources, often made available on a mass scale, remain in cyberspace forever and cannot be permanently deleted. This also applies to data about ourselves posted on various social networking sites, offices that make

[16] Grzelak M., *Szpiegostwo i inwigilacja w Internecie*, w: *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji* (Eng. Espionage and surveillance on the Internet, in: Network-centric security. War, peace and terrorism in the information age), K. Liedel, P. Piasecka, T. Aleksandrowicz (ed.), Warszawa 2014, pp. 164–181.

public data available, or any other organisations. This set of data is later publicly accessible, easy to obtain without leaving virtually any traces. This means that it can take criminals literally no time at all to obtain the information they need to carry out attacks. In a way, people have already got used to posting information on the Internet without thinking about the impact on their private security. In addition, social networks, but also websites, have accustomed web users to express their reactions and emotions under posts or articles. However, not many people check whether the post they have liked has not been transformed into a post with negative or criminal content and whether it is not being used to commit criminal acts. Charity campaigns, for example, are used to convince the user that for every "like" a certain amount of money is donated for the treatment of a particular person. In this way, massive fraud takes place and the money gained is used for completely different purposes.

Another threat to information is the flow of information generated by particular social networks or open source information retrieval tools. The available documentation of some portals indicates that the requests sent are not directed to the target data sources, but to intermediary servers. Very often these servers are located in the United States, which, for legislative reasons, may have a negative impact on the information security attribute of confidentiality. Furthermore, sending requests to proxies raises the question of whether requests are inadvertently directed to undesirable locations. Due to the possible existence of proxies, the user has no assurance that the results returned are not modified or partially filtered. The transmission of information in text form also creates the risk of it being easily intercepted by hackers. This is especially dangerous if the leak concerns strategic information or information processed by entities responsible for ensuring national security[17].

Social networking sites have become one of the primary channels for exchanging information. We are often even assured of encrypted communication, otherwise known as secure communication. However, it should be noted that this is not the safest way to exchange information. It is not a secret that the administration of Internet, social networking sites reviews and uses them according to their needs. An example is Cambridge Analytica, which used the data of about 87 million Facebook users. This action consisted of transferring photos

[17] Documentation review conducted by analysts at Inseqr sp. z o.o.

and private conversations to a department that deals with personality analysis and strategies for influencing mass population behaviour.

Unfortunately, the disclosure of private messages even by the unknown administration of websites or social networks is not a positive prospect. An additional threat is the possibility of transmitting information, messages to various institutions, including governmental ones, or to foreign services.

It is worth being aware that in case of actions of cyber criminals or, what is worse, cyber terrorists, they may have access to the following data:

- telephone numbers
- bank account numbers;
- logins and passwords to computers, bank accounts, domains;
- private information;
- information on industrial and intellectual property rights;
- knowledge of planned projects.

In the least harmful case, the data obtained, originating from private conversations on communication platforms, information from social networks or various other websites, are used to prepare and then present the most varied products in the form of advertisements appearing on the websites viewed. These actions are obviously aimed at stimulating the user's interest and, consequently, persuading him to make a purchase. Artificial intelligence mechanisms now allow various Internet assistants to eavesdrop on our conversations in order, for example, to tailor advertisements for products that may be of interest to us. It is therefore worth paying attention to the confidentiality of our conversations and considering securing smartphones during important meetings. An example of a product that can ensure the confidentiality of our conversations are the so-called 'hummers' already available on the market. These are acoustic boxes that act as a safe depository for devices that can capture or transmit sound. Such solutions very often prevent eavesdropping by means of electronic devices equipped with a voice recorder function. In addition, they also prevent eavesdropping that may be carried out by assistants embedded in mobile systems.

A serious interdisciplinary threat to open-source information is the spread of disinformation, primarily because of the extent of its impact. When the terms 'disinformation', 'fake news' appear, people

usually think of social media posts with rather fantastic, improbable stories. However, fake news is much more than exaggerated social media article titles. Disinformation may seem like a new phenomenon, but the only novelty is the platform used and the environment in which it is spread. In fact, it has been around for centuries and the internet is just a newer means of communication that can be used to spread lies and disinformation.

The essence of disinformation is a way of communicating information - true or false - in such a way as to mislead an opponent or competitor and induce them to behave as we expect and in our favour. Disinformation is not a simple lie, i.e. the communication of false information, but a real deception. Typically, a disinformation campaign involves the transmission of multiple pieces of information, most of which are true, while only one - the key piece of information to produce the intended effect - is false. It is also sometimes the case that a disinformation campaign is conducted on the basis of information that is true but presented in such a way that a competitor believes it to be false. In addition, several independent sources and channels of information are used to increase the effectiveness of disinformation. Although, as mentioned above, disinformation is not a new phenomenon, its importance has undoubtedly increased with the emergence of mass media. As Tomasz Aleksandrowicz rightly pointed out, there has been a weaponisation of information, which has contributed to the creation of weapons of mass manipulation[18]. A perfect example of the use of this weapon was the leak of confidential information via the WikiLeaks website. This case shows perfectly well that keeping data secure on the Internet is a real challenge.

Similarly to the fire triangle, which assumes that three factors - oxygen, fuel and energy - are required for a building fire to spread, disinformation also requires three different elements to succeed. Together they form the fake news triangle, and the absence of at least one of them will result in fake news not being able to spread and reach its intended audience.

[18] Aleksandrowicz T. R., *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze* (Eng. Threats to the state's information security from a systemic perspective. Building defensive and offensive capabilities in the infosphere), Warszawa, 2021, pp. 32 – 49.

Fig. 7. Fake news triangle.

Source: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media [accessed: 26 November 2021].

The first element is the tools and services for manipulating and spreading news in the relevant social networks. There is a wide range of tools and services available in the world, some of them are relatively simple (paid likes/observers etc.), others are more complicated - some services promise to provide online surveys, others force site owners to delete stories.

Of course, for these tools to be useful, social networks must exist as a platform for spreading propaganda. Since people spend a lot of time in them to get the latest news and information, their importance in spreading fake news cannot be underestimated. However, there is a difference between simply publishing propaganda and turning it into something that the target audience consumes. The study of social media also gives an idea of the relationship between bots and recipients of social media promotions, such as Twitter, and thus gives an idea of the scope and organisation of campaigns attempting to manipulate public opinion.

Finally, a propaganda campaign always brings with it the question: why? The motives of those spreading fake news vary: sometimes it is simply to gain money through advertising, but it can also be for criminal or political purposes. Whatever the motive, the success of any propaganda campaign is ultimately measured by how much it affects the real world.

In summary, disinformation can be said to exist when the information disseminated:

- is totally or partially false, manipulated or misleading;
- concerns a matter of public interest;
- is intended to create uncertainty or hostility, polarisation or disruption of democratic processes;
- is disseminated or amplified through automated and aggressive techniques such as social bots, artificial intelligence (AI), microtargeting or trolling.

Disinformation can destabilise a country, exert a destructive influence on its administrative and decision-making structures, and undermine its social, economic and cultural foundations. According to the report Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy[19], more and more countries around the world are using social media for disinformation activities - both to shape their internal policies and to influence other countries. Countering disinformation is becoming a challenge facing not only individual states, but also international institutions and organisations. The need to counter disinformation campaigns in Europe was first highlighted by the European Council in March 2015. Since then, several teams have been established within the structures of the European External Action Service to analyse disinformation in the European Union and neighbouring countries.

The problem of disinformation - on the state-wide and strategic level - was raised in the National Security Bureau (BBN) during work on recommendations to the new National Security Strategy. It was also discussed on the international forum and during numerous expert meetings organised at the BBN. From the discussions held, the biggest challenges in the information environment at present are:

- lack of understanding of the importance and nature of the problem;
- lack of an efficient system of strategic communication and coordination of activities in combating disinformation at the national level;
- low levels of media literacy among selected social groups;

[19] https://freedomhouse.org/article/new-report-freedom-net-2017-manipulating-social-media-undermine-democracy [accessed: 28 XI 2021].

- striking a balance between freedom of expression and countering disinformation;
- building a positive narrative and promoting the state externally.

All these challenges are universal and to a large extent also concern Poland as a country belonging to the community of Western civilisation, which shares democratic values. Internationally, disinformation most often targets democratic procedures and seeks to undermine citizens' trust in the state. Such action also threatens national security. Disinformation activities mislead citizens and often create uncertainty in them. Among other things, this prevents them from making sovereign electoral decisions based on reliable information.

Countering disinformation requires first and foremost:

- raising citizens' awareness of disinformation threats;
- building institutional capacity;
- undertaking cooperation between various institutions and strategic communication units in EU and NATO countries and institutions;
- designing and implementing active measures, i.e. conducting projects and information campaigns;
- supporting Polish NGOs and undertaking cooperation with them.

To identify disinformation, one should:

1. Get to know the source of information (understand its goals and intentions), find out who is responsible for this source, who owns it, etc.
2. Read the whole article, not just the headline (to understand the whole material).
3. Check the authors to verify that they are credible. This is not always possible because not all articles are signed by name and not all authors - even in credible content - are signed. If it is possible, it is a good idea to search for the name of the author or authors and see other content that this person creates.
4. Check this information with other sources (make sure they give the same information).
5. Find the date of publication (to check that the information is up to date).
6. Think about your own biases (to see if they affect your judgement).

7. Ask experts (to get confirmation from independent people with knowledge of the subject).

Faced with the huge amount of information that is processed in open sources on a daily basis, there is a problem in distinguishing truth from falsehood. Very often we are dealing with the creation of certain visions, especially by the media, instead of presenting reliable information. In addition, the dynamic pace of life means that the information life cycle is very short. The information which appeared today and moved the public opinion will be replaced the next day by another, equally important one. Additionally, the overabundance of various information makes decision-making processes extremely complicated, and people are guided not by the real state of affairs, but rather by the social perception of given facts. In addition, information is manipulated to achieve certain benefits. The spread of disinformation by Russia during the 2016 US presidential election can serve as an example. This state of affairs is a huge problem in modern societies. Currently, it is very difficult to control the circulation of public information, there are many manipulative tools that greatly undermine the credibility of the information presented. Additionally, the situation in which information attacks become recognisable only at the moment when the attacker reaches his goal or are not recognised at all is very worrying. The words of Sławomir Zalewski, who said: "(...) the statement of the absence of threats does not eliminate them in the future, but also does not exclude the possibility that actions constituting a threat are undertaken here and now, only that they have not yet been recognised"[20].

Considering the numerous threats to information in cyberspace, it should be noted that the largest countries in the world have introduced special legal regulations to protect ICT resources and counter threats in this area. Among others, Russia in the Law on the Protection of Personal Data and its subsequent supplements introduced the order to store personal data of Russians only on the territory of their country[21]. The United States has enacted the CLOUD Act[22], which compels US providers of electronic services to disclose, upon request

[20] Zalewski S., *Bezpieczeństwo polityczne. Zarys problematyki* (Eng. Political security. Outline of issues), Siedlce 2013.

[21] https://gdpr.pl/panstwa-spoza-ue-a-rodo-czesc-i-rosja [accessed: 28 XI 2021].

[22] https://epic.org/wp-content/uploads/privacy/cloud-act/cloud-act-text.pdf [accessed: 28 XI 2021].

by a US court, information on users of those services, regardless of whether it is processed in the States or in any other country in the world. It is also worth noting the Cyber Security Law introduced in China and the law setting the National Information Security Standard. These documents sanction the principle that all hardware and software supplied to government entities or critical infrastructure entities must be audited by designated and prepared entities. The source code of any software purchased for the needs of the above entities must also be checked.

In 2014, the process of effectively establishing a cyber security system began in Ukraine. The most important impetus for such measures was the cyber attacks on the electricity grid, which led to temporary disruptions in electricity supply. In 2016, the Cyber Security Strategy of Ukraine was approved, which stressed the need for legislative work on the national cyber security system[23]. It was recognised that the above activities are the basis of national security. In addition, it focused on the interaction between actions taken by state bodies, local authorities, military formations, scientific institutions, as well as commercial entities. However, despite the introduction of legislative documents, there are huge problems with the development of cyber security strategies in Ukraine. These are due to, among other things, the lack of effective implementation of cyber security policy, lack of awareness of cyber threats and insufficient human potential. Problems are also created by: lack of legal and organisational framework for the protection of critical infrastructure, lack of up-to-date cyber security standards and weak national legislation on cybercrime[24].

Noteworthy is the action taken in Estonia, which can be a model for other countries. Estonia should be regarded as a pioneer of digitalisation in Europe, as evidenced by the introduction of a cyber security strategy back in 2008[25]. This was the first document of its kind in the world.

[23] Semeniy J., Glushchenko S., Makarevich O., *Ukraine,* [w:] *Cybersecurity* 2018, B.A. Powell, J.C. Chipman (ed.), Law Business Research, London, p. 99.

[24] Boiko V., *Comparison of the Polish and Ukrainian cybersecurity system,* „Teka of Political Science and International Relations" 2019, t. 14, no. 2, pp. 119–137.

[25] Narodowa Strategia Cyberprzestrzeni Estonii (Eng. Estonia's National Cyberspace Strategy), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia, [accessed: 28 XI 2021].

Estonia is constantly working to increase the level of cyber security. This is primarily due to highly developed e-services, and preventive measures are aimed at countering online crime. Estonia is in favour of a single digital market within the European Union, which is expected to translate into tangible benefits in terms of the development of the e-economy. In addition, it is pushing the Member States to take joint action for digitalisation and security in cyberspace. The protection of personal data in mobile networks and on websites, the free movement of non-personal data and the taxation of Internet services are among the areas of interest. Estonia's cybersecurity policy primarily seeks to clean up existing regulations and adapt them to dynamically changing circumstances. It also continues to improve the technology supporting the response to cyber incidents by, among other things, improving the network infrastructure, coordinating the administration of IT systems and strengthening the IT department in the administration[26].

A tangible action within the European Union in the field of cyber security was the adoption of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)[27], the so-called GDPR, which is binding on all processors of personal data in connection with their business activities. By means of the aforementioned regulation, many changes and increased obligations for data controllers and processors have been introduced.

As cyber security is currently one of the biggest challenges facing ICT network administrators and users, the EU's response to it is also Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of IT networks

[26] Raś K., *Estonia jako lider w zwiększeniu cyberbezpieczeństwa* (Eng. Estonia as a leader in increasing cyber security), „Biuletyn – Polski Instytut Spraw Międzynarodowych" 2018, no. 68, pp. 20 – 22.

[27] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the EU L of 2016, No. 119/1 of 27 April 2016.

and systems within the Union[28]. In Poland, this Directive was implemented by the Act of 5 July 2018 on the National Cyber Security System. The Act imposed new obligations on entities that have an impact on state security. Among other things, internal audits of ICT systems, the development of relevant documentation, the implementation of security management systems, as well as carrying out activities to detect, record, analyse and classify incidents became a requirement. Poland also enacted the Act of 10 June 2016 on anti-terrorist activities[29]. By virtue of this document, the tasks of the Internal Security Agency (ABW) include, among others: the identification and detection of threats to the security of the ICT systems of public administration bodies or the system of ICT networks included in the uniform list of objects, installations, devices and services constituting critical infrastructure, as well as the ICT systems of the owners and holders of objects, installations or devices of critical infrastructure, which are important for the continuity of the state's functioning, and the prevention of such threats. The Head of ABW is responsible for keeping a central register of terrorist incidents which breach the security of ICT systems of particular importance to the state security or ICT networks. Moreover, in order to prevent and counter terrorist incidents in cyberspace, the Internal Security Agency may assess the security of ICT systems by conducting security tests in order to identify vulnerabilities. A vulnerability is understood as a weakness of a resource or security of an ICT system, which can be exploited and threaten the integrity, confidentiality, accountability and availability of that system.

The presented examples show how important it is to protect information resources in the international arena and which security measures will allow to counteract any threats related to the flow of information.

It is also worth noting that the actions of cyber criminals have a major impact on critical infrastructure facilities. Their aim is primarily to undermine public confidence in civil society and the foundations of democracy. It is also a threat to sovereignty, which gives terrorist organisations and criminals the opportunity to operate anonymously using techniques and effective methods to influence the policies

[28] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of networks and information systems within the Union. OJ. EU. L. 2016.194.1 of 6 July 2016.

[29] Act of 10 June 2016 on anti-terrorist activities. Journal of Laws of 2021, item 2234.

and strategies of other states. An example is the actions of Russia, which is one of the most active perpetrators of cyber attacks, during the illegal annexation of Crimea in 2014. Another example is China, which has actively engaged in carrying out cyber attacks and disinformation campaigns against members of the NATO alliance and poses a very serious threat to critical energy infrastructure, as highlighted in the NATO 2030 expert report[30].

The cyber attacks carried out in the last 15 years prove that they affect both those who carry them out - the cyber criminals - and the environments that try to defend the network. Today, the cybersecurity defence environment requires many tools and solutions, which are usually very expensive. Attacks conducted on a smaller scale are just a bridgehead to larger attacks and, going forward, to the development of cyber defences. The development of cyber attacks has led cybersecurity professionals to consider them as an everyday phenomenon and to focus their efforts on network defence. The methods of ensuring cyber security, as well as the way to respond to attacks, must evolve in line with the development of intrusions. As the commercial sector is mostly responsible for the Internet environment, state organisations and private entities should consider cooperation in network security. However, this requires broad legislative changes in terms of proactive and reactive measures against cyber threats.

It seems reasonable to develop an operational doctrine implemented by national cyber forces, which should be developed, tested and modified depending on threats. The organisation of bilateral exercises seems to be a good introduction to further cooperation. Subsequently, representatives of the commercial community responsible for protective measures should also take part in the exercises. Representatives of individual countries should not be afraid of cyber experts from the private environment, as they have already taken the initiative and are conducting pre-emptive actions. Moreover, the global nature of the Internet requires international cooperation. Individual state solutions to cyber threats will not be effective, as combating these threats requires a coherent and flexible approach. NATO as an international organisation has years of experience

[30] https://nato.int [accessed: 29 XI 2021].

in developing policies and operations against conventional threats. However, the time has now come to apply the experience and expertise gained to ensure and maintain cyber security[31].

In conclusion, it should be stated that the assumed hypothesis has been verified. Well, in the last few decades there has been a huge technological progress related to the development of modern technologies, and above all the emergence of an advanced information society. Currently, no one can imagine life without access to the Internet, and thus to information from open sources. Their universality, accessibility and low cost make them the first source of information to be used. However, along with their development, new threats have emerged, often of a cyberterrorist nature, which pose a great danger to people as individuals, all organisations and state structures. Information security is an area that requires radical and immediate action, as cybercriminals are able to secretly access any system to achieve their planned goal. The situation is not helped by a dynamically changing environment, the coronavirus pandemic and the transfer of life to the world of the Internet, as well as by conflicts between states aimed at gaining an advantage in the international arena. Implemented legal regulations appear to be insufficient in protecting information. It is necessary to create a synergy effect by combining international actions, as well as actions at the level of individual states, in order to permanently ensure network security, both at national and international level. It is important to be aware that cyber-terrorist attacks will occur and even increase. They can range in scale from the manipulation of information and the spreading of disinformation to attacks on critical infrastructure ICT systems. Although the complete eradication of cyber terrorism is not feasible, preventive measures should be taken, as well as measures aimed at detecting attacks of a cyber terrorist nature as soon as possible and minimising the losses caused by them.

[31] W.E. Leigher, *Cyber conflict in a hybrid threat environment: Death by a thousand cuts*, Helsinki 2021.

Bibliography

Aleksandrowicz T. R., *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym. Budowanie zdolności defensywnych i ofensywnych w infosferze* (Eng. Threats to the state's information security from a systemic perspective. Building defensive and offensive capabilities in the infosphere), Warszawa, 2021, pp. 32 – 49.

Boiko V., *Comparison of the polish and Ukrainian cybersecurity system*, „Teka of Political Science and International Relations" 2019, vol. 14, no. 2, pp. 119–137.

Elliott A., Castells M., *Społeczeństwo sieci,* w: Elliott A., *Współczesna teoria społeczna. Wprowadzenie* (Eng. Network society, in: Contemporary social theory. Introduction), Warszawa 2011.

Grzelak M., *Szpiegostwo i inwigilacja w Internecie,* w: *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji* (Eng. Espionage and surveillance on the Internet, in: Network-centric security. War, peace and terrorism in the information age), K. Liedel, P. Piasecka, T. Aleksandrowicz (ed.), Warszawa 2014, pp. 164–181.

Hall R., Fox C., *Ponownie przemyśleć bezpieczeństwo* (Eng. Rethinking security), „Przegląd NATO" zima 2001/2002, p. 8.

Kissinger H., *Dyplomacja* (Eng. Diplomacy), Warszawa 2016.

Leigher W.E., *Cyber conflict in a hybrid threat environment: Death by a thousand cuts*, Helsinki 2021.

Measuring the Information Society Report, vol. 1, 2018.

Nowak J.S., *Społeczeństwo informacyjne – geneza i definicje,* w: *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz* (Eng. Information society - origins and definitions, in: Information Society. One step forward, two steps back), P. Sienkiewicz, J.S. Nowak (ed.), Katowice 2008, p. 25.

Oleński J., *Ekonomika informacji* (Eng. Economics of information), Warszawa 2001.

Raś K., *Estonia jako lider w zwiększeniu cyberbezpieczeństwa* (Eng. Estonia as a leader in increasing cyber security), „Biuletyn – Polski Instytut Spraw Międzynarodowych" 2018, nr 68, pp. 20 – 22.

Saramak B., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy* (Eng. The use of open sources of information in intelligence activities: history, practice, perspectives), Warszawa 2015.

Sienkiewicz P., *Społeczeństwo informacyjne jako system cybernetyczny*, w: *Społeczeństwo informacyjne. Wizja czy rzeczywistość?* (Eng. Information society as a cybernetic system, in: Information Society. Vision or Reality?), vol. 1, L.H. Haber (ed.), Kraków 2004, p. 79.

Semeniy J., Glushchenko S., Makarevich O., *Ukraine*, [w:] *Cybersecurity* 2018, B.A. Powell, J.C. Chipman (ed.), Law Business Research, London, p. 99.

Sosińska-Kalata B., *Obszary badań współczesnej informatologii (nauki o informacji)* (Eng. Research areas of contemporary informatology (information science)), „Zagadnienia Informacji Naukowej" 2013, no. 2, pp. 9–41.

Sun Tzu, *Sztuka wojny* (Eng. Art Of War), Gliwice 2004.

West Ch., *Competitive intelligence*, New York 2001.

Zalewski S., *Bezpieczeństwo polityczne. Zarys problematyki* (Eng. Political security. Outline of issues), Siedlce 2013.

Internet sources

https://datareportal.com/reports/digital-2021-global-overview-report [accessed: 26 XI 2021].

https://epic.org/wp-content/uploads/privacy/cloud-act/cloud-act-text.pdf [accessed: 28 XI 2021].

https://freedomhouse.org/article/new-report-freedom-net-2017-manipulating-social-media-undermine-democracy [accessed: 28 XI 2021].

https://gdpr.pl/panstwa-spoza-ue-a-rodo-czesc-i-rosja [accessed: 28 XI 2021].

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia, [accessed: 28 XI 2021].

https://nato.int [accessed: 29 XI 2021].

http://unicjin.org/documents/congr10/10e.pdf [accessed: 27 XI 2021].

http://www.bbc.uw.edu.pl/Content/20/08.pdf [accessed: 25 XI 2021].

Legal acts

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the EU L of 2016, No. 119/1 of 27 April 2016.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of networks and information systems within the Union. OJ. EU. L. 2016.194.1 of 6 July 2016.

Act of 10 June 2016 on anti-terrorist activities. Journal of Laws of 2021, item 2234.

DOI: 10.4467/27204383TER.22.015.15431

ORCID: 0000-0002-2174-6966

ARTUR SYBICKI

Anti-terrorist protection of places of worship

Abstract

Terrorist attacks in Europe, which targeted religious sites, forced the security policy of the EU Member States on whose territory they occurred to develop and implement solutions (legal, substantive, technical and physical) proportionate to the nature and type of the facility inquestion. The purpose of their introduction is to strengthen the level of anti-terrorist protection both for the religious site itself and for those in direct contact withit (clergy and participants in liturgical gatherings). The factors proving the attractiveness of religious sites as targets for terrorist attacks, including the main threats to their security, and the required elements of their anti-terrorist protection system remain the same in many countries. It is also important to note that Polish places of religious worship have many characteristics that place them among the public facilities at risk of possible terrorist incidents. However, one can get the impression that the issues concerning their anti-terrorist protection are not treated systematically on the territory of the Republic of Poland. There is a lot of discussion about the security of public facilities, but Polish researchers and practitioner experts in the field of terrorist security have not focused their attention on them in a comprehensive way. A breakthrough in the development and construction of anti-terrorist security systems for places of worship, both in the European and Polish dimensions, is the year 2021, because the European Commission finances six projects

Keywords:

religious facilities, places of worship, anti-terrorist protection system for religious facilities, terrorist safety of places of worship

in this area (one under the leadership of the University of Lodz, implemented in the territory of Poland), which aim to systematize the problems of anti-terrorist protection of religious facilities, and in the future to increase the level of their protection against dangers. The intention of the author of this article is to present solutions in this field, which are being prepared by the European Commission, and to obtain an answer to the question, to what extent Polish religious facilities are prepared for dangerous incidents, especially those of a terrorist nature.

The *modus operandi* of the perpetrators of terrorist events in Europe is evolving. There is a noticeable tendency for terrorist organisations to withdraw from the concept of large-scale attacks and to adopt a dispersed formula of activity. Terrorist groups are moving away from complicated and sophisticated methods of activity and are focusing on the activity of individuals (*lone wolf, solo terrorist*) or a small number of people using simple means of action, easily available and not requiring significant logistical preparation[1]. Often the perpetrators of terrorist attacks use the same methods and tools as those used by criminal gangs. Despite the diversity of their actions, the main targets of their activity remain the same. They still usually attack innocent and defenceless people and their places of stay, including public facilities, which are the so-called soft targets, with a low level of protection against threats and having a symbolic and defined value for a given society. This methodology of operation results in the emergence of new, hitherto unknown or incidental ways of mobilising attackers and creates a much greater threat to public safety. Terrorist security experts agree that due to the unpredictability of the attackers' behaviour, the public authorities tasked with combating and preventing terrorism are being forced to face a much more difficult and dangerous adversary (a concept known as 'new terrorism')[2].

---

[1] T. Aleksandrowicz, *Bieżące zagrożenia, terrorystyczne, cz. 1. – Doświadczenia ostatniego dziesięciolecia* (Eng. Current threats, terrorist, part 1 - Experience of the last decade), „Przegląd Policyjny" 2017, no. 4 (128), p. 38.

[2] T. Aleksandrowicz, K. Jałoszyński, *Cechy charakterystyczne organizacji terrorystycznych w XXI wieku* (Eng. Characteristics of terrorist organisations in the XXI century),

One of the targets of attacks are places of religious worship, including both religious sites associated with Christianity, Islam, Buddhism and Judaism, and the worshippers who attend them. In Europe, there are many deliberate attacks on these places every year, during which clergy and participants in liturgical gatherings lose their lives and health. These attacks are often classified as terrorist or extremist incidents and are the result of the behaviour of perpetrators acting out of religious hatred.

Due to the cyclical rise in attacks on places of religious worship across Europe, members of the European Union are increasingly considering what their anti-terrorist protection system should look like. In many countries of the Community, especially those with a high level of risk of a terrorist event whose target was, is or may be, among others, places of worship, solutions are being developed for their effective protection. All such systems, which have been systematically developed and improved over the years, are intended to respond to possible incidents of both a terrorist and extremist nature. From the perspective of the European Union, the subject of terrorist security of public buildings, including places of religious worship, is considered to be very important and is therefore included in the EU Security Strategy for 2020-2025 as one of the strategic priorities of the security union[3].

Taking into account the above information, the author of the article focused in the publication on the characteristics of the solutions for terrorist security of European places of worship, which are under way by the European Commission. An important element of the article is also an attempt to assess the system of anti-terrorist protection of Polish religious facilities and to answer the question to what extent

in: *Bezpieczeństwo państwa a zagrożenie terroryzmem. Terroryzm na przełomie XX i XXI wieku*, K. Jałoszyński, T. Aleksandrowicz, K. Wiciak (ed.), Szczytno 2016, p. 47.

[3] Komisja Europejska, *Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie strategii UE w zakresie unii bezpieczeństwa (Eng. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy for a Security Union),* Bruksela 2020, pp. 11–13, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605 &cookies=disabled [accessed: 30 XI 2021].

they are prepared for dangerous incidents, especially those of a terrorist nature.

From the information contained in the bulletins published on the official website of the SOAR - *Protecting Places of Worship in Europe* project funded by the European Commission, it appears that only from July 2 to October 22, 2021 there were many dangerous incidents in Europe targeting places of worship or people associated with them[4]. On the basis of the article's author's own study, carried out on the basis of data found in the content of the aforementioned publications, it was determined that out of 116 incidents, the largest number occurred in France, Germany and the UK (82 in total). The services of the remaining 12 countries, where such incidents also took place (including Poland), recorded several incidents of this type. During the period in question, five crimes were committed on the territory of Poland, which the Polish law enforcement authorities - in most cases - qualified as prohibited acts committed out of religious hatred. A numerical comparison of these incidents with a breakdown by European countries is presented in Figure 1.

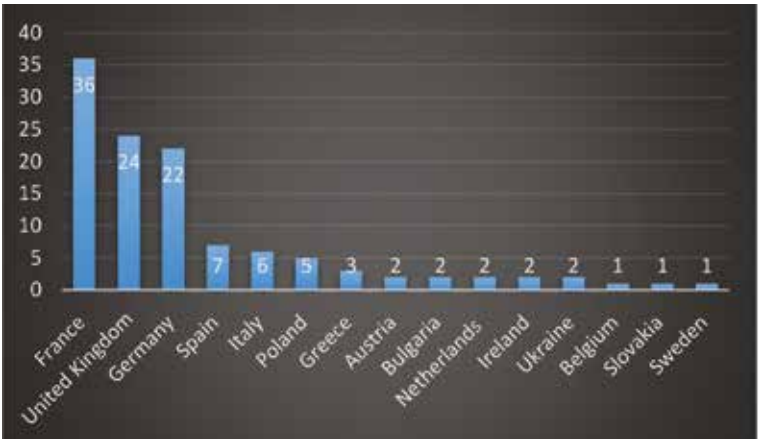


Fig. 1. Number of attacks on places of religious worship in Europe between July 2 and October 22, 2021.

Source: Own elaboration based on information bulletins posted on the official website of the SOAR project,, https://soarproject.eu/resources/ [accessed: 11 December 2021].

[4] https://soarproject.eu/newsletter/ [accessed: 11 XII 2021].

In the same way, the author of the article analysed which groups of religious communities were most frequently attacked in Europe. The information obtained shows that in the period presented, the most frequent targets of the perpetrators were places and people associated with the Christian religion. A total of 72 cases of aggression were identified, which represents 62,07 percent of all attacks on European religious sites. Attacks on places and persons associated with other religious communities were respectively: 30 incidents against the Jewish community (representing 25,86 percent of all incidents within Europe), 13 acts of aggression against sites associated with Islam (representing 11,21 percent of all incidents within Europe) and one incident targeting a site associated with Buddhism (representing 0.86 percent of all incidents)[5]. A breakdown by religion is shown in Figure 2.

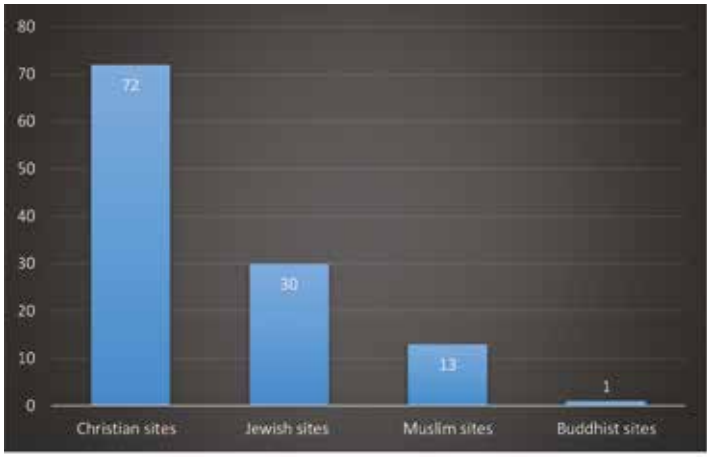


Fig. 2. Number of attacks on persons and places associated with a particular religion that occurred in Europe between July 2 and October 22, 2021.

Source: Own elaboration based on newsletters posted on the official website of the SOAR project, https://soarproject.eu/resources/ [accessed: 11 December 2021].

[5] An attack on a Buddhist-related site occurred in September 2021 on British soil, www.swindonadvertiser.co.uk/news/19590833.hundreds-march-town-centre-solidarity-hindu-community-temple -break-ins/ [accessed: 12 XII 2021].

The offences that the detained persons committed against places associated with Christianity were mostly acts of vandalism and consisted, inter alia, of damaging property located in buildings, vandalizing and stealing religious symbols, using a vehicle as a tool of attack (France, Sarthe)[6], firing a firearm at a church building (Slovakia, Bratislava)[7], attempting to use an aircraft to attack a facility (France, Paris)[8]. There were two cases of homicide, which the anti-terrorist services assessed as religiously motivated acts of violence. One of them was committed in August 2021 on French territory. A mentally disturbed perpetrator - who had been arrested by police services in the past on suspicion of setting fire to a religious building - carried out the murder of a Catholic clergyman using a dangerous bladed object[9]. The second incident was identified in October 2021 in the UK. It concerned the murder of a Conservative British politician with close links to the Catholic religion[10]. The British services classified this crime as a terrorist incident and the perpetrator himself as an Islamic radical.

The author's own study further shows that the countries with the highest number of attacks on places of worship and people associated with the Christian religion were France, the UK, Germany, Spain and Italy. These incidents accounted for 87,5 percent of all incidents in Europe targeting Christian sites. This group also included the territory of Poland, where three acts of aggression took place. A numerical summary in this respect is presented in Figure 3.

6 https://actu.fr/pays-de-la-loire/beille_72031/sarthe-un-camion-fonce-dans-l-eglise-son-chauffeur-s-enfuit-le-maire-lance-un-appel-a-temoins_45259304.html [accessed: 11 XII 2021].

7 https://www.kath.net/news/76584 [accessed: 11 XII 2021].

8 https://www.leprogres.fr/faits-divers-justice/2021/10/10/il-projetait-de-percuter-la-cathedrale-notre-dame-en-avion-un-homme-interpelle [accessed: 11 XII 2021].

9 https://www.europe1.fr/faits-divers/un-pretre-assassine-en-vendee-annonce-darmanin-4061489 [accessed: 11 XII 2021].

10 https://www.bbc.com/news/uk-58935372 [accessed: 11 XII 2021].

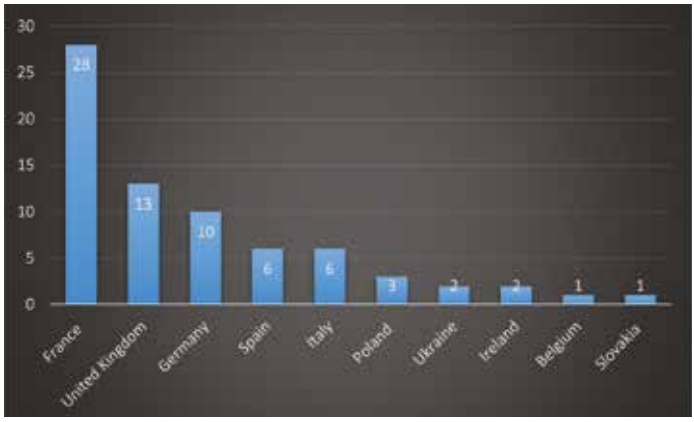


Fig. 3. Number of attacks on Christian sites in Europe between July 2 and October 22, 2021.

Source: Own elaboration based on information bulletins posted on the official website of the SOAR project, https://soarproject.eu/resources/ [accessed: 11 December 2021].

The offences committed against places associated with Judaism, Islam and Buddhism - as well as against Christian sites - were motivated by extremist and criminal motives of religious hatred. These included acts of vandalism involving the destruction and devastation of property, including arson, placing offensive inscriptions on religious symbols (Great Britain, Essex)[11], criminal threats directed for racist reasons and religious affiliation (France, Strasbourg)[12], threats of using dangerous bladed objects (France, Villeurbanne)[13].

The author's own study of the article shows that the countries with the highest number of attacks on places of worship and people associated with Judaism and Islam were Germany, the United Kingdom and France. The number of such acts accounted for 63,33 percent of incidents in Europe targeting Jewish sites and 84,61 percent targeting Muslim sites. A summary of the figures in this regard is presented in Figures 4 and 5.

[11] https://muslimnews.co.uk/news/islamophobia/france-3-mosques-face-islamophobic-attack/ [accessed: 11 XII 2021].

[12] https://actu.fr/grand-est/strasbourg_67482/mosquee-a-strasbourg-l-association-derriere-le-projet-menacee-d-attentats_45450694.html [accessed: 11 XII 2021].

[13] https://www.jpost.com/diaspora/antisemitism/teenager-arrested-after-waving-knife-in-front-of-french-jewish-school-684430 [accessed: 11 XII 2021].

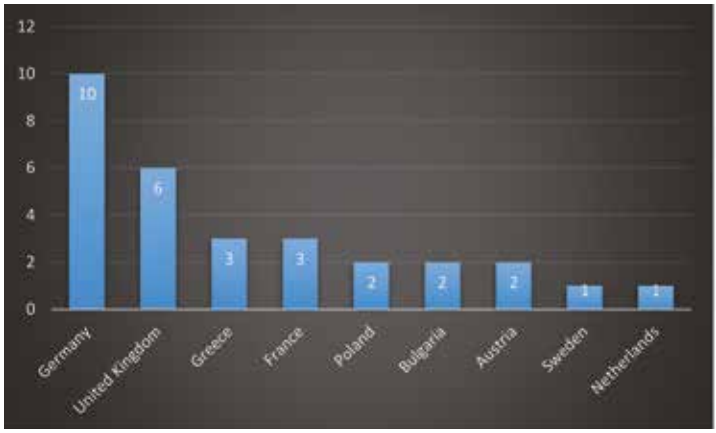


Fig. 4. Number of attacks on Jewish sites in Europe between July 2 and October 22, 2021.

Source: Own elaboration based on information bulletins posted on the official website of the SOAR project, https://soarproject.eu/resources/ [accessed: 11 December 2021].

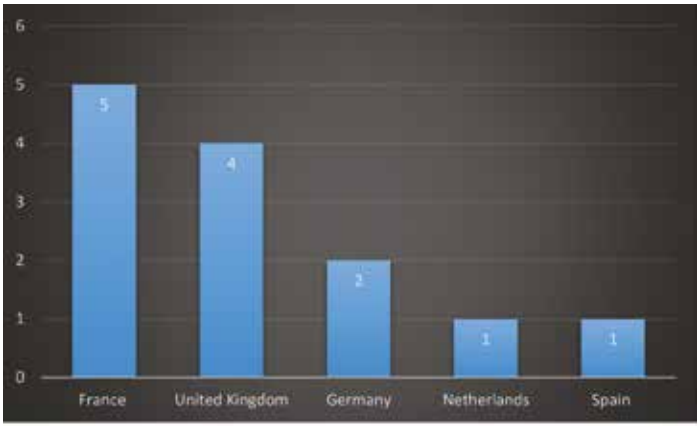


Fig. 5. Number of attacks on Muslim sites in Europe between July 2 and October 22, 2021.

Source: Own elaboration based on news bulletins posted on the official website of the SOAR project, https://soarproject.eu/resources/ [accessed: 11 December 2021].

Supporting the projects undertaken on the protection of places of worship is the activity of the European Commission's Directorate-General for Migration and Home Affairs (DG Home), which implements a number of initiatives to increase the level of security in the area

of terrorist threats to places of public interest, including places of worship. In 2017, the European Commission adopted an action plan to support EU Member States in protecting these sites. Following a completed consultation, a document entitled *Good practices to support the protection of public spaces* was issued in 2019. In the area of securing public facilities, a number of practices of a general nature have been identified as a starting point for building systems to secure them by those responsible for the process in individual entities[14]. In addition, in May 2021, representatives of the DG HOME's Protective Security Advisory team, with the participation of representatives of police forces affiliated since 2018 within the EU High Risk Security Network, produced a publication entitled *EU Quick Guide to support the protection of places of worship*. It identifies additional good practices for the protection of places of worship which can be considered as low risk from terrorist events[15].

The authors of the handbook stress that it provides factual support to members of all religious communities and encourage its use in the process of assessing the terrorist threat level of places of worship. In the opinion of DG Home experts, this publication is less applicable when assessing incidents whose nature indicates that they were part of pre-planned actions by the perpetrators of attacks. In this context, it is not widely applicable to places of worship characterised by a high level of vulnerability, resulting, inter alia, from their location (often of a symbolic nature), important religious events taking place on their premises or the presence of VIPs during such events. It is particularly important to emphasise that the *EU Quick Guide to support the protection of places of worship* serves to raise awareness and assess the resilience of sites to a limited number of forms of terrorist incidents, i.e. incidents where the perpetrator(s) uses vehicles, firearms, dangerous bladed objects and explosives (referred

[14] European Commission, Commission Staff Working Document, *Good practices to support the protection of public spaces, Accompanying the document, Communication from the Commission to the European Parliament, the European Council and the Council Eighteenth Progress Report towards an effective and genuine Security Union*, Brussels 2019, pp. 4–5, https://op.europa.eu/en/publication-detail/-/publication/998aeb09-4be6-11e9-8ed-01aa75ed71a1/language-en [accessed: 16 XI 2021].

[15] European Commission, DG Home, *EU Quick Guide to support the protection of Places of Worship, 2021*, pp. 4–5, https://ec.europa.eu/home-affairs/whats-new/publications/eu-quick-guide-support-protection-places-worship_en [accessed: 27 XI 2021].

to by the author as the instrumentarium of the perpetrator)[16] as tools of attack. The most important part of the guide are the principles for assessing the level of possible dangers, based on the search for answers to the auxiliary questions included in the content of the document, in areas relevant to the security of places of worship[17].

In June 2020, the European Commission, under the Internal Security Fund - Police, issued a call for proposals to EU members for projects to enhance the security of places of worship. The planned activities within the framework of the project were to include:

- establishing or strengthening cooperation between public entities and religious leaders of a given religion;
- creating channels for the exchange of information between these entities on possible threats of a terrorist and criminal nature (hate crimes)
- developing and implementing public awareness campaigns against terrorism for EU citizens;
- sharing of knowledge, good practices on solutions used by different Member States;
- developing, implementing and delivering concepts, security programmes and training[18].

On this basis, in 2021, the European Commission financially supported six independent projects to improve the terrorist security of religious sites, namely:

- *ProSPeReS - Protection System for large gatherings of People in Religious Sites* - at present the only project for anti-terrorist protection of places of religious worship implemented on the territory of Poland[19];

---

[16] European Commission, DG Home, *EU Quick Guide to support the protection of Places of Worship, 2021*, p. 5, https://ec.europa.eu/home-affairs/whats-new/publications/eu-quick-guide-support-protection-places-worship_en [accessed: 27 XI 2021].

[17] European Commission, DG Home, *EU Quick Guide to support the protection of Places of Worship, 2021*, pp. 7–22, https://ec.europa.eu/home-affairs/whats-new/publications/eu-quick-guide-support-protection-places-worship_en [accessed: 27 XI 2021].

[18] ISF Police, 2020 Call for proposals: ISFP-2020-AG-PROTECT, https://ec.europa.eu/research/participants/data/ref/other_eu_prog/home/wp/call-fiche_isfp-2020-ag-protect_en.pdf [accessed: 28 XI 2021].

[19] Among the project beneficiaries were the following Polish entities: The Main School of Fire Service, the Warsaw Metropolitan Police Headquarters, the Provincial Police Headquarters in Łódź, the Provincial Police Headquarters in Wrocław, the WSB

- *SASCE - Safer and Stronger Communities in Europe;*
- *SHIELD - Solutions to Enhance Interfaith Protection of Places of Worship from Terrorist Danger;*
- *PROTECTOR - Protecting Places of Worship;*
- *PROSECUW - Protection and Security for Places of Worship;*
- *SOAR Project - Protecting Places of Worship in Europe*[20].

The aim of the above mentioned initiatives is to increase the level of anti-terrorist protection of places of worship by developing their terrorist security system/systems, counteracting and responding to possible terrorist threats, including with the use of CBRN means[21] (the *ProSPeReS* project). The above assumptions are to be implemented on the basis of cooperation between European scientists, experts and practitioners in the field of security of places of public interest, i.e. representatives of state administration bodies and religious institutions[22]. The projects assumes the analysis of pilot case studies that occurred in the above-mentioned facilities in European countries, identification of gaps in their protection systems and, on this basis, the development of recommendations to increase terrorist security of these facilities. The results are expected to lead to the development of targeted training, instructional materials and best practice information on terrorist security at places of worship as well as to the implementation of high impact public awareness campaigns.

The project partners stress that the most important element of their activities will also be to increase the protection of places of worship through the implementation of a security concept called *security by design*. This model is in line with the general assumptions

Academy, the Social Observatory Foundation, the Space Research Centre of the Polish Academy of Sciences, the Jewish Community in Warsaw, the Archdiocese of Łódź, Dynamic Safety Corporation Sp. z o.o. and European partners from Finland, Greece, Cyprus, the Netherlands and Slovakia.

[20] TOPIC ID: ISFP-2020-AG-PROTECT https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/isfp-2020-ag-protect [accessed: 11 XII 2021].

[21] Abbreviation denoting hazards involving chemical, biological, radiation and nuclear agents.

[22] *Funding & tender opportunities*, http://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/31077817/101034230/ISFP [accessed: 11 XII 2021].

indicated by the experts of the European Commission, who are of the opinion that the minimisation of the effects of the perpetrators of terrorist events can be achieved already at the stage of designing and construction of a given facility, creating such parts of it or spaces for its functioning that at the time of an attack will ensure the minimum number of damages and will effectively prevent its significant damage[23].

Experts from DG Home and representatives of the US Department of Homeland Security, which is responsible for the security of, among others, places of worship, point to factors which increase the likelihood of a terrorist attack on religious sites[24].

As the first element they mention the open access and free participation in religious services of clergy and participants of liturgical gatherings (often with VIP status). This fact makes it possible for a predictable number of participants to gather in the interior or exterior of the facility in connection with religious events and rituals to take place anywhere at a fixed time. On this basis, both the place itself and the people in it become ready and easy targets for an adversary with free and unrestricted access to almost any church, mosque or synagogue[25].

Religious sites have religious, historical, cultural or social significance for many faith communities. The symbolic value of a site is another element that increases the likelihood of a terrorist or extremist event occurring on its premises[26]. For fundamentalist religious

---

[23] European Commission, Commission Staff Working Document, *Good practices to support the protection of public spaces, Accompanying the document, Communication from the Commission to the European Parliament, the European Council and the Council Eighteenth Progress Report towards an effective and genuine Security Union*, Brussels 2019, pp. 4–5, https://op.europa.eu/en/publication-detail/-/publication/998aeb09-4be6-11e9-8ed-01aa75ed71a1/language-en [accessed: 16 XI 2021].

[24] U.S. Department of Homeland Security, *Houses of Worship Security Practice Guide*, May 2013, p. 6, https://www2.illinois.gov/ready/plan/documents/dhs_houses_of_worship_security_practices_guide.pdf [accessed: 20 XI 2021].

[25] European Commission, *Protection of Places of Worship,* 2020, https://ec.europa.eu/newsroom/pps/item-detail.cfm?item_id=696367&utm_source=pps_newsroom&utm_medium=Website&utm_campaign=pps&utm_content=Protection%20of%20Places%20of%20Worship&lang=en [accessed: 27 XI 2021].

[26] U.S. Department of Homeland Security, *Houses of Worship Security Practice Guide*, May 2013, p. 6, https://www2.illinois.gov/ready/plan/documents/dhs_houses_of_worship_security_practices_guide.pdf [accessed: 20 XI 2021].

ideologues, attacking a symbol becomes a basis for achieving political goals and, by promoting hatred and fear among religious opponents, an incentive to take control of a selected community, to defeat it and gain power over it[27]. For perpetrators of hate crime, the factor that defines their behaviour is most often the so-called prejudice motivation against people and their widely understood differences[28].

Another factor identified that increases the likelihood of an attack on a religious site is the unrestricted access of both people and vehicles to its peripheral areas. Through the multitude of objects adjacent to religious buildings (urban properties, especially institutions and important public places) and their location (centre, periphery of the city), the number of people who may be there and among them potential aggressors increases[29]. The freedom to park vehicles without control in any place of this zone, e.g. in car parks, nearby streets, entrances to the site, and many times the lack of physical barriers limiting the movement of cars increases the risk of using a vehicle as a tool of attack (e.g. by detonating explosives hidden in the vehicle, using the vehicle to ram people moving in the traffic routes)[30].

The limitations and financial difficulties of places of worship are also factors which increase their attractiveness as objects of attack. The main purpose of their functioning is religious activity for the benefit of individual religious communities and satisfying their spiritual needs. Low income significantly restricts those responsible for their administration from accessing desirable solutions to increase their

[27] K. Izak, *Nie tylko islam. Ekstremizm i terroryzm religijny* (Eng. Not only Islam. Extremism and religious terrorism), „Przegląd Bezpieczeństwa Wewnętrznego" 2015, no 12, p. 209.

[28] A. Mazurczak, *Przestępstwa motywowane uprzedzeniami. Analiza i zalecenia* (Eng. Crimes motivated by prejudice. Analysis and recommendations), „Biuletyn Rzecznika Praw Obywatelskich" 2017, no. 6, p. 10.

[29] European Commission, *Protection of Places of Worship,* 2020, https://ec.europa.eu/newsroom/pps/item-detail.cfm?item_id=696367&utm_source=pps_newsroom&utm_medium=Website&utm_campaign=pps&utm_content=Protection%20of%20Places%20of%20Worship&lang=en [accessed: 27 XI 2021].

[30] U.S. Department of Homeland Security, *Houses of Worship Security Practice Guide*, May 2013, p. 6, https://www2.illinois.gov/ready/plan/documents/dhs_houses_of_worship_security_practices_guide.pdf [accessed: 20 XI 2021].

security level, including, for example, purchasing physical security equipment or hiring experts to build appropriate security systems[31].

In the policy of terrorist security of places of worship, the most important element is to achieve and maintain a high level of situational awareness of people associated with the facility and their understanding of what is happening both in its internal environment and around it. This is achieved by developing a culture of safety both among those responsible for the management of the site (the clergy) and among the staff and other participants in liturgical gatherings. Each of them must understand that terrorist threats exist, and that ignoring them significantly reduces the chance of their prompt recognition. An important factor in a crisis situation is for all those involved to take responsibility for their own safety, the safety of those around them (the facility and the people), and in a threatening situation to take appropriate protective and defensive action[32]. Such actions should be supported by anti-terrorist education carried out by developing educational programmes raising anti-terrorist awareness among the mentioned people. Only by combining theory and practice can people be prepared for possible threats and answer questions on how to identify dangers, how to defend against them and how to behave in a crisis situation[33].

Experts of the European Commission in the manual *EU Quick Guide to support the protection of places of worship* emphasize that at the level of designing the system of anti-terrorist protection of places of worship it is necessary to take into account a number of important elements and on the basis of information on the identified basic threats to carry out a process of risk assessment of their occurrence. It is also important

---

[31] Ibid.

[32] K. Liedel, P. Piasecka, *Bezpieczeństwo w czasach terroryzmu. Jak przeżyć zamach terrorystyczny* (Eng. Safety in times of terrorism. How to survive a terrorist attaca), Warszawa 2018, p. 42.

[33] B. Wiśniewska-Paź, J. Stelmach, *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej. Założenia i rekomendacje do prowadzenia działań antyterrorystycznych w wybranych kategoriach obiektów* (Eng. Anti-terrorist security of public utility buildings. Assumptions and recommendations for conducting anti-terrorist actions in selected categories of facilities), in: *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej*, vol. 4 – *Założenia i rekomendacje do prowadzenia działań antyterrorystycznych w wybranych kategoriach obiektów*, B. Wiśniewska-Paź, J. Stelmach (ed.), Toruń 2019, p. 8.

to find out what kind of risk of a given threat can be considered acceptable and what kind of measures can be taken in the facility to minimise the likelihood of the threat occurring[34].

The process of assessing the risk of a terrorist event occurring in places of worship is part of a multi-component risk management process, which is the most important component of the anti-terrorist security system for both the facility and the people in it. According to NaCTSO experts, a number of important elements should be taken into account when managing risk in a facility, which, among others, in March 2019, the European Commission identified as good practices to strengthen the anti-terrorism protection of public places[35]. In this respect, the above-mentioned *EU Quick Guide to support the protection of places of worship* is also an important support for those carrying out such an assessment, especially in the context of threats related to the above-mentioned perpetrators' instruments used during attacks[36].

The underlying factor of the system is the identification and determination of the level of terrorist risk in the site, which includes an understanding of the intentions and capabilities of the attacker(s) and what they can do and with what attack methodology. UK experts indicate that the following questions are helpful in this area:

- What kind of information can the person responsible for the security of the facility obtain from state institutions, e.g. the Police, about terrorist threats against the facility that may occur locally and nationally?
- Are there elements of the facility's functioning which may attract the attention of perpetrators of terrorist events?

[34] European Commission, DG Home, *EU Quick Guide to support the protection of Places of Worship, 2021*, p. 13, https://ec.europa.eu/home-affairs/whats-new/publications/eu-quick-guide-support-protection-places-worship_en [accessed: 27 XI 2021].

[35] European Commission, Commission Staff Working Document, *Good practices to support the protection of public spaces, Accompanying the document, Communication from the Commission to the European Parliament, the European Council and the Council Eighteenth Progress Report towards an effective and genuine Security Union*, Brussels 2019, pp. 4–5, https://op.europa.eu/en/publication-detail/-/publication/998aeb09-4be6-11e9-8ed-01aa75ed71a1/language-en [accessed: 16 XI 2021].

[36] European Commission, DG Home, *EU Quick Guide to support the protection of Places of Worship*, 2021, p. 5, https://ec.europa.eu/home-affairs/whats-new/publications/eu-quick-guide-support-protection-places-worship_en [accessed: 27 XI 2021].

- Is there a connection between the facility and persons or organisations of VIP status, which may be the target of terrorist attacks? Are there security procedures regulating the participation of the aforementioned entities in events taking place within the facility? How often are they reviewed?
- Are there buildings in the immediate vicinity of the facility which, due to the specificity of their functioning, are places of high terrorist risk and may indirectly pose a threat to the facility itself?
- Are there areas of the facility or its staff that attackers could exploit during an attack, e.g. architectural plans of buildings accessible to third parties, technical expertise, unrestricted access to restricted areas of the facility?[37]

Another element is to identify the entities to be protected, assess their vulnerability and identify the weak points of the facility. In each case, in the context of the security of a place of worship, priority is given to people (clergy, employees, participants in liturgical gatherings), then to material resources (e.g. buildings, their equipment, plans), and finally to information (both electronic and paper data). Identifying weaknesses in the system, both in relation to external and internal threats, provides answers as to what kind of solutions need to be developed to improve the system. One way to improve the system is through close cooperation between facility managers and state counterterrorism units. These bodies should regularly assess the vulnerability of individuals to terrorist threats from inside and outside the site. It is important in this situation to find out why and to what types of threats the protected premises are vulnerable[38].

In the anti-terrorist protection system of a place of worship, it is important to identify measures that reduce or mitigate the risk of a terrorist event occurring there. Once identification has made it possible to conclude that the danger to people and the site is real,

---

[37] NaCTSO, National Counter Terrorism Security Office, *Crowded Places Guidance*, 2020, https://www.gov.uk/government/publications/crowded-places-guidance/managing-risk-business-continuity [accessed: 20 XI 2021].

[38] European Commission, Commission Staff Working Document, *Good practices to support the protection of public spaces, Accompanying the document, Communication from the Commission to the European Parliament, the European Council and the Council Eighteenth Progress Report towards an effective and genuine Security Union*, Brussels 2019, pp. 4–5, https://op.europa.eu/en/publication-detail/-/publication/998aeb09-4be6-11e9-8ed-01aa75ed71a1/language-en [accessed: 16 XI 2021].

the identification and evaluation of the effectiveness of existing security measures should ensue, followed by the implementation of new, additional and proportionate protective solutions adapted to different environments. The aim is to achieve the lowest possible level of any risk[39]. European Commission experts stress that the security measures selected and tailored must always be accompanied by appropriate technical solutions, developed by security specialists, whether in-house or outsourced[40]. Often there is little point in investing in expensive security measures for the operation of a site, and the most effective solutions are the simplest ones. They become all the more effective when the people connected with the facility are characterised by a high culture of security. On such a basis, once the threat is assessed as real, further elements of the facility's security system can be built[41].

The development, regular review and updating of site security plans is the next link in the system. An effective security plan should be simple, clear and flexible in its content. Its primary purpose should be to deter possible threats resulting from external and internal factors (e.g. from persons employed in the facility) and, when they do occur, to mitigate the potential effects of the perpetrator(s). In such a situation it becomes necessary to create a comprehensive strategy which should combine preventive, protective and preparatory actions, basing all its elements on risk analysis, combined with actions increasing the resistance of the facility to possible threats, especially the most serious ones[42]. In the security procedures it is recommended

[39] NaCTSO, National Counter Terrorism Security Office, *Crowded Places Guidance*, 2020, https://www.gov.uk/government/publications/crowded-places-guidance/managing-risk-business-continuity [accessed: 20 XI 2021].

[40] European Commission, Commission Staff Working Document, *Good practices to support the protection of public spaces, Accompanying the document, Communication from the Commission to the European Parliament, the European Council and the Council Eighteenth Progress Report towards an effective and genuine Security Union*, Brussels 2019, pp. 4–5, https://op.europa.eu/en/publication-detail/-/publication/998aeb09-4be6-11e9-8ed-01aa75ed71a1/language-en [accessed: 16 XI 2021].

[41] NaCTSO, National Counter Terrorism Security Office, *Crowded Places Guidance*, 2020, https://www.gov.uk/government/publications/crowded-places-guidance/introduction [accessed: 20 XI 2021].

[42] NaCTSO, National Counter Terrorism Security Office, *Crowded Places Guidance*, 2020, https://www.gov.uk/government/publications/crowded-places-guidance/managing-risk-business-continuity [accessed: 20 XI 2021].

that security plans be systematically reviewed, among other things to assess their accuracy, feasibility and timeliness, and after the audit, conclusions should be drawn, necessary recommendations recommended and implemented.

According to the British concept of the terrorist security of religious sites, responsibility for the preparation of security plans at places of worship should lie with so-called security leaders. These persons on the premises of a religious site shall, among other things, chair a specially established terrorist threat assessment team[43]. As a rule, they should be composed of specialists not only formally authorised to perform security tasks, but above all having knowledge and experience in designing a comprehensive security system[44]. The role of the team members is both the physical protection of the object and the collection of information on the type of threats to its security, an attempt to identify them and assess their nature. Functioning within the places of worship, these people also become involved in the process of anti-terrorist education, the programme of which includes, among other things, identification of possible threats to people and the object, indication of how to react and how to defend oneself when danger occurs.

An important area of the team's activity are constant contacts with representatives of state institutions responsible for terrorist security both on a local, regional, national (e.g. Police, other emergency services) and international level. Maintained relations with state institutions are primarily the possibility of immediate transmission through established communication channels of information about an identified threat, use of expert knowledge, sharing information used in the process of risk analysis and assistance in typing and recognizing internal and external threats to a given religious community[45].

---

[43] U.S. Department of Homeland Security, *Houses of Worship Security Practice Guide*, May 2013, p. 6, https://www2.illinois.gov/ready/plan/documents/dhs_houses_of_worship_security_practices_guide.pdf [accessed: 20 XI 2021].

[44] J. Stelmach, M. Kożuszek, *Założenia i rekomendacje do wykonywania planów ochrony w obiektach podlegających obowiązkowej ochronie* (Eng. Assumptions and recommendations for the implementation of security plans in facilities subject to mandatory protection), in: *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej,* vol. 4 – *Założenia i rekomendacje do prowadzenia działań antyterrorystycznych w wybranych kategoriach obiektów*, B. Wiśniewska-Paź, J. Stelmach (ed.), Toruń 2019, p. 25.

[45] NaCTSO, National Counter Terrorism Security Office, *Counter Terrorism Protective*

The system of anti-terrorist protection of places of worship also includes their physical protection, which - through the use of proportionate protection measures - is intended, among other things, to restrict free access to places that are restricted zones. Closely related to this is also the use of technical detection means, e.g. for the detection of explosives, firearms, dangerous bladed objects. However, the European Commission specialists make the application of such solutions dependent on the assessment of vulnerability of a given facility to possible threats[46].

The last element of the system of anti-terrorist protection of religious facilities is constant and cyclic training of personnel. Regular in-service training for facility personnel (clergy, employees, participants of liturgical gatherings) is becoming a standard in order to raise their level of anti-terrorist awareness, make sure they understand their responsibilities and accept the need to implement the terrorist security measures contained in the security plan. Practical exercises are also an important element of the training system. Their implementation is supposed to reveal possible mistakes and gaps in the existing security procedures, to identify doubts or comments to the security plans, to use by persons connected with a given place the acquired theoretical knowledge to further improve solutions serving the security of a given facility. Exercises are also a constant verification that the security plans developed are feasible and meet expectations. Practical activities should involve all stakeholders of the security system, especially facility administrators, its staff, participants of liturgical gatherings, but also emergency services (e.g. fire brigade, police, special forces) and other relevant entities responsible for security and ensure multiple scenarios, according to the principle "plan-do-check-act"[47].

Security Advice for Places of Worship, ACPO 2009, p. 42, https://www.welhat.gov.uk/media/16407/Crowded-Places-Guidance/pdf/Crowded_Places_Guidance.pdf?m=637242863669130000 [accessed: 20 XI 2021].

[46] European Commission, Commission Staff Working Document, *Good practices to support the protection of public spaces, Accompanying the document, Communication from the Commission to the European Parliament, the European Council and the Council Eighteenth Progress Report towards an effective and genuine Security Union*, Brussels 2019, pp. 4–5, https://op.europa.eu/en/publication-detail/-/publication/998aeb09-4be6-11e9-8ed-01aa75ed71a1/language-en [accessed: 16 XI 2021].

[47] NaCTSO, National Counter Terrorism Security Office, *Counter Terrorism Protective*

Summarising selected issues of solutions proposed by the European Union to increase the level of protection of places of worship from terrorist threats, two additional, often difficult to reconcile, issues should be noted. On the one hand - as mentioned above - the open nature of religious sites, the free and predictable participation of large numbers of people in religious events and ceremonies, and the frequent lack of sufficient security procedures make these places easy targets for attack. On the other hand, it should not be forgotten that in order to preserve their real role and purpose, it is not possible to make them into a typical fortress providing them with absolute security. What can be achieved is to create a system of protection that minimises the risk of attack and reduces to a certain level the possible adverse effects of the perpetrator(s)[48]. In this situation, it must not be forgotten that not every religious site will find the same proposed solutions applicable. Individual sites differ in many indicators, such as size, location, purpose, more or less developed human safety culture, etc. Therefore, solutions to increase the level of their protection should be developed on an individual basis and correspond to the actual purpose and functioning characteristics of the site[49].

Considering the problem of anti-terrorist protection of places of worship in the EU, one cannot help but ask whether Polish religious facilities face similar problems, whether they have been or are the target of attacks by perpetrators of terrorist or extremist events, and therefore what the system of protecting them against such events looks like.

Answering the above, it should be stated that no incidents with a strictly terrorist background have been recorded in Poland. To date,

---

Security Advice for Places of Worship, ACPO 2009, p. 37, https://www.welhat. gov.uk/media/16407/Crowded-Places-Guidance/pdf/Crowded_Places _Guidance.pdf?m=637242863669130000 [accessed: 20 XI 2021].

[48] NaCTSO, National Counter Terrorism Security Office, *Counter Terrorism Protective Security Advice for Places of Worship,* ACPO 2009, p. 6, https://www.welhat. gov.uk/media/16407/Crowded-Places-Guidance/pdf/Crowded_Places _Guidance.pdf?m=637242863669130000 [accessed: 20 XI 2021].

[49] European Commission, Commission Staff Working Document, *Good practices to support the protection of public spaces, Accompanying the document, Communication from the Commission to the European Parliament, the European Council and the Council Eighteenth Progress Report towards an effective and genuine Security Union*, Brussels 2019, pp. 4–5, https://op.europa.eu/en/publication-detail/-/publication/998aeb09-4be6-11e9-8ed-01aa75ed71a1/language-en [accessed: 16 XI 2021].

all incidents targeting Polish places of religious worship have been qualified by Polish services as criminal, including those motivated by religious hatred. The perpetrators of these crimes (both single and acting jointly and in agreement with others), while attempting or carrying out a physical attack on persons and places associated with a given religious community, used as instruments dangerous bladed objects, air weapons, used physical force (beatings) and criminal threats against persons. The basis of the aggressors' activity were associated mental illnesses, aggression due to religious differences or the influence of narcotics. In one case, an attack by an aggressor ended in the death of the victim and injury to a clergyman providing medical assistance to the victim. In the remaining incidents, the injuries sustained by the victims did not pose a threat to their life and health. Most perpetrators were apprehended by law enforcement authorities within a short period of time after the incident. To date, no cases of attacks on Polish religious facilities with the use of explosives, firearms, chemical or biological substances have been recorded, nor have they been targeted by cyber criminals.

Similarly to religious facilities in the world, also Polish places of worship are characterised by features increasing their attractiveness as targets of a possible terrorist attack. To a large extent, they are identical or even identical to those described by representatives of the British NaCTSO in their publication. In the literature on the subject, Polish security experts supplement this catalogue with additional elements and indicate, in addition to those mentioned above, e.g. the low level of anti-terrorist security of a given place, the possibility of increasing the post-explosive impact in the case of bombings threatening the stability of the structure of buildings, limited possibilities of action by rescue services due to the difficulties arising from the capacity of evacuation routes and compact infrastructure around buildings[50].

In considering how to secure places of religious worship in Poland, attention should be drawn to another important problem. Despite the

[50] J. Stelmach, B. Wiśniewska-Paź, *Wprowadzenie – rozważania na temat zagrożenia terroryzmem dla obiektów użyteczności publicznej* (Eng. Introduction - considerations on the terrorist threat to public facilities), in: *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej*, vol. 2 – *Metody i narzędzia zamachów vs działania antyterrorystyczne i kontrterrorystyczne*, B. Wiśniewska-Paź, M. Szostak, J. Stelmach (ed.), Toruń 2018, pp. 9–10.

identification of possible risk factors for religious facilities in the context of a terrorist attack, they still fall into the category of public buildings, where protection is not mandatory. On this basis, there is no legal obligation to develop comprehensive documentation on the anti-terrorist protection system in them. The possession of e.g. physical or technical security measures, preparation and implementation of a security plan, conduct of preventive actions, implementation of training and practical exercises is decided solely by the manager (administrator) of the building, and his decision is most often the result of a risk analysis related to the financial capabilities of a given place[51].

Currently, the issues related to the procedures to be followed on the territory of a place of worship during an armed conflict and crisis situation, including terrorist events, are regulated in Chapter 8 of the *Act of 23 July 2003 on the protection and care of historical monuments*[52]. However, its material jurisdiction covers only those objects which, in accordance with the definition, have the status of a historic monument and their preservation in an unchanged state (as a real property, a part thereof or a complex), due to their historical, artistic and scientific value, constitutes a social interest. On this basis, in line with the executory act to the Act, i.e. the *Regulation of the Minister of Culture of 25 August 2004 on the organisation and manner of protection of historical monuments in the event of armed conflict and crisis situations*[53], the organisation and manner of protection of these places in the organisational units possessing historical monuments are determined, the state of the resources subject to protection is described, as well as potential threats and measures to prevent them. In the plan for protection of monuments of individual organizational units of state and local administration, the bodies responsible for its creation, based on the foreseeable and real threats, determine the necessary forces and resources, time and costs in case of such an incident. Moreover,

---

[51] J. Stelmach, *Kategorie obiektów użyteczności publicznej i stopnie ich ochrony w kontekście zagrożenia współczesnym terroryzmem* (Eng. Categories of public buildings and degrees of their protection in the context of the threat of contemporary terrorism), in: *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej. Analiza – Diagnoza* – Case study, B. Wiśniewska-Paź, M. Szostak (ed.), J. Stelmach, Toruń 2018, p. 31.

[52] Consolidated text: Journal of Laws of 2021, item 710.

[53] Journal of Laws of 2004, item 212, no. 2153.

they include in the content of the document information on the process of implementation of preparatory works and efficient coordination and management of protection during such an incident[54].

The number of terrorist attacks on places of public interest, including places of religious worship, is increasing steadily in the European Union. In the last decade alone, many members of the clergy and participants in liturgical celebrations have died as a result of terrorist attacks in Europe. The frequency and nature of the events have meant that building an anti-terrorist protection system for these sites has become a necessity and a standardised element of the security policy of many states. The European Commission's Directorate-General for Migration and Home Affairs has been involved in the process of creating a level of security for places and people. For many years, its experts - by developing and implementing a number of legislative initiatives, proposing solutions for so-called good practices, financing projects, etc. - have been encouraging EU Member States to include security of places and people. The importance of the issue is also evidenced by the inclusion of the issue in the list of places of worship. The importance of the issue is also demonstrated by the inclusion of the issue of anti-terrorist protection of places of worship in the EU Security Strategy 2020-2025 as one of the priority tasks. The result of the above-mentioned assumptions are projects funded by the European Commission, which, it is hoped, will systematise the issues of securing European places of worship. As mentioned at the beginning of this article, the year 2021 will therefore have a symbolic dimension, because it is in this year that all actions aimed at improving the level of terrorist security of places of worship, including in Poland, were initiated.

Not being indifferent to the difficult experience of the EU countries on whose territory terrorist incidents against places of religious worship occurred, it is necessary to continue the discussion in our country on the issues related to the anti-terrorist protection of Polish religious facilities. It is worth considering the need to regulate in a single legal act the issue of terrorist security of all Polish places of religious worship. Legislative solutions contained in the Act on the protection

[54] A. Ginter, A. Michalak, *Komentarz do art. 88* (Eng. Commentary to art. 88), in: *Ustawa o ochronie zabytków i opiece nad zabytkami. Komentarz*, A. Ginter, A. Michalak (ed.), Warszawa 2016, LEX OMEGA number 500623.

and care of monuments are a certain solution, but limiting them only to objects that are monuments does not solve the said problem in a comprehensive manner. In this regard, it is worth considering a return to the solutions proposed in 2016, when, during the work on the draft law on anti-terrorist activities, the Ministry of the Interior proposed that the document under consideration should include a provision on the inclusion of places of religious worship in mandatory protection plans. After criticism from security experts, the lawmakers withdrew from the implementation of this assumption. The negative comments stressed the significant financial burden that may arise for administrators of these places, the difficulties in implementing physical and technical protection measures, and above all the lack of substantive grounds for action, resulting from the absence of real terrorist threats on the territory of the Republic of Poland[55].

Particular attention should also be paid to the implementation by the University of Łódź and invited consortium members of the first project in our country funded by the European Commission aimed at counter-terrorist protection of places of worship. It is to be hoped that the good practices and experience gained in its implementation will serve to improve the level of terrorist security of these facilities. In addition, a good example would be to invite to Poland in 2022 experts from the European Commission (DG Home) who prepare, in the course of their own training (based on the above-mentioned EU manual on support for the protection of places of religious worship), trainers on securing religious facilities. Such trainers could then cascade to train further national specialists in this field. In the context of the above conclusions, it also seems important to obtain an answer to the question of whether and, possibly, which of the proposed or already existing solutions in the system of anti-terrorist protection of places of worship in Europe can be implemented, improved, modified or adapted on the territory of the Republic of Poland. The foreseeability of threats, the proper selection of measures to counteract them, the minimization of the risk of their occurrence and the consequences of a possible terrorist attack, introduced in time, may save human life and health and protect the object from possible damage. People directly associated

[55] www.pch24.pl/plan-ochrony-dla-kazdego--mswia-stawia-na-profilaktyke-antyterrorystyczna,42810,i.html [accessed: 14 XII 2021].

with places of worship have the right to feel comfortable and safe there, and it is the duty of those responsible for the security of religious facilities, both at the national and local level, to provide these people and places with the expected comfort and security.

Bibliography

Aleksandrowicz T., *Bieżące zagrożenia, terrorystyczne*, cz.1.: *Doświadczenia ostatniego dziesięciolecia*, (Eng. Current threats, terrorist, part 1.: Experience of the last decade), „Przegląd Policyjny" 2017, no. 4, pp. 27–47.

Aleksandrowicz T., Jałoszyński K., *Cechy charakterystyczne organizacji terrorystycznych w XXI wieku*, (Eng. Characteristics of terrorist organizations in the XXI century), in: *Bezpieczeństwo państwa a zagrożenie terroryzmem. Terroryzm na przełomie XX i XXI wieku*, K. Jałoszyński, T. Aleksandrowicz, K. Wiciak (ed.), Szczytno 2016, pp. 46–51.

Ginter A., Michalak A., *Komentarz do art. 88* (Eng. Commentary to art. 88), w: *Ustawa o ochronie zabytków i opiece nad zabytkami. Komentarz*, A. Ginter, A. Michalak (ed.), Warszawa 2016, LEX OMEGA, number 500623.

Izak K., *Nie tylko islam. Ekstremizm i terroryzm religijny* (Eng. Not only Islam. Extremism and religious terrorism), „Przegląd Bezpieczeństwa Wewnętrznego" 2015, no. 12, pp. 183–210.

Liedel K., Piasecka P., *Bezpieczeństwo w czasach terroryzmu. Jak przeżyć zamach terrorystyczny* (Eng. Security in times of terrorism. How to survive a terrorist attack), Warszawa 2018.

Mazurczak A., *Ochrona przed przestępstwami motywowanymi uprzedzeniami w przepisach prawa polskiego i międzynarodowego* (Eng. Protection against crimes motivated by prejudice in Polish and international law), in: *Przestępstwa motywowane uprzedzeniami. Analiza i zalecenia*, „Biuletyn Rzecznika Praw Obywatelskich" 2017, no. 6, pp. 9–13.

Stelmach J., *Kategorie obiektów użyteczności publicznej i stopnie ich ochrony w kontekście zagrożenia współczesnym terroryzmem* (Eng. Categories of public utility buildings and degrees of their protection in the context of the threat of contemporary terrorism), in: *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej. Analiza – Diagnoza – Case study*, B. Wiśniewska-Paź, M. Szostak, J. Stelmach (ed.), Toruń 2018.

Stelmach J., Kożuszek M., *Założenia i rekomendacje do wykonywania planów ochrony w obiektach podlegających obowiązkowej ochronie* (Eng. Assumptions and recommendations for executing security plans in facilities subject to mandatory protection), in: *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej*, vol. IV – *Założenia i rekomendacje do prowadzenia działań antyterrorystycznych w wybranych kategoriach obiektów*, B. Wiśniewska-Paź, J. Stelmach (ed.), Toruń 2019.

Stelmach J., Wiśniewska-Paź B., *Wprowadzenie – rozważania na temat zagrożenia terroryzmem dla obiektów użyteczności publicznej* (Eng. Introduction - considerations on the threat of terrorism to public buildings), in: *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej. Metody i narzędzia zamachów vs działania antyterrorystyczne i kontrterrorystyczne*, B. Wiśniewska-Paź, M. Szostak, J. Stelmach (ed.), Toruń 2018.

Wiśniewska-Paź B., Stelmach J., *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej. Założenia i rekomendacje do prowadzenia działań antyterrorystycznych w wybranych kategoriach obiektów* (Eng. Anti-terrorist security of public utility buildings. Assumptions and recommendations for conducting anti-terrorist actions in selected categories of facilities), in: *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej*, vol. IV: *Założenia i rekomendacje do prowadzenia działań antyterrorystycznych w wybranych kategoriach obiektów*, B. Wiśniewska-Paź, J. Stelmach (ed.), Toruń 2019.

U.S. Department of Homeland Security, *Houses of Worship Security Practice Guide*, May 2013, https://www2.illinois.gov/ready/plan/documents/dhs_houses_of_worship_security_practices_guide.pdf [accessed: 20 XI 2021].

Internet sources

European Commission, DG Home, *EU Quick Guide to support the protection of Places of Worship, 2021*, https://ec.europa.eu/home-affairs/whats-new/publications/eu-quick-guide-support-protection-places-worship_en [accessed: 27 XI 2021].

European Commission, *Protection of Places of Worship*, 2020, https://ec.europa.eu/newsroom/pps/item-detail.cfm?item_id=696367&utm_source=pps_ newsroom&utm_medium=Website&utm_campaign=pps&utm_content=Protection%20of%20Places%20of%20Worship&lang=en [accessed: 27 XI 2021].

https://actu.fr/grand-est/strasbourg_67482/mosquee-a-strasbourg-l-association-derriere-le-projet-menacee-d-attentats_45450694.html [accessed: 11 XII 2021].

https://actu.fr/pays-de-la-loire/beille_72031/sarthe-un-camion-fonce-dans-l-eglise-son-chauffeur-s-enfuit-le-maire-lance-un-appel-a-temoins_45259304.html [accessed: 11 XII 2021].

http://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/31077817/101034230/ISFP [accessed: 11 XII 2021].

https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/isfp-2020-ag-protect [accessed: 11 XII 2021].

https://ec.europa.eu/newsroom/pps/newsletter-archives/35274 [accessed: 11 XII 2021].

https://muslimnews.co.uk/news/islamophobia/france-3-mosques-face-islamophobic-attack/ [accessed: 11 XII 2021].

https://soarproject.eu/newsletter/ [accessed: 11 XII 2021].

https://www.bbc.com/news/uk-58935372 [accessed: 11 XII 2021].

https://www.europe1.fr/faits-divers/un-pretre-assassine-en-vendee-annonce-darmanin-4061489 [accessed: 11 XII 2021].

https://www.jpost.com/diaspora/antisemitism/teenager-arrested-after-waving-knife-in-front-of-french-jewish-school-684430 [accessed: 11 XII 2021].

https://www.kath.net/news/76584 [accessed: 11 XII 2021].

https://www.leprogres.fr/faits-divers-justice/2021/10/10/il-projetait-de-percuter-la-cathedrale-notre-dame-en-avion-un-homme-interpelle [accessed: 11 XII 2021].

ISF Police, 2020 *Call for proposals: ISFP-2020-AG-PROTECT,* https://ec.europa.eu/research/participants/data/ref/other_eu_prog/home/wp/call-fiche_isfp-2020-ag-protect_en.pdf [accessed: 28 XI 2021].

NaCTSO, National Counter Terrorism Security Office, *Counter Terrorism Protective Security Advice for Places of Worship,* ACPO 2009, https://www.welhat.gov.uk/media/16407/Crowded-Places-Guidance/pdf/Crowded_Places _Guidance.pdf?m=6 37242863669130000 [accessed: 20 XI 2021].

NaCTSO, National Counter Terrorism Security Office, *Crowded Places Guidance*, 2020, https://www.gov.uk/government/publications/crowded-places-guidance/introduct ion [accessed: 20 XI 2021].

NaCTSO, National Counter Terrorism Security Office, *Crowded Places Guidance*, 2020, https://www.gov.uk/government/publications/crowded-places-guidance/manag ing-risk-business-continuity [accessed: 20 XI 2021].

www.pch24.pl/plan-ochrony-dla-kazdego--mswia-stawia-na-profilaktyke-anty-terrorystyczna,42810,i.html [accessed: 14 XII 2021].

Legal acts

Komisja Europejska, *Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie strategii UE w zakresie unii bezpieczeństwa* (Eng. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on an EU Strategy for a Security Union), Bruksela 2020, pp. 11–13, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605 &cookies=disabled [accessed: 30 XI 2021].

European Commission, Commission Staff Working Document, *Good practices to support the protection of public spaces, Accompanying the document, Communication from the Commission to the European Parliament, the European Council and the Council Eighteenth Progress Report towards an effective and genuine Security Union*, Brussels 2019, pp. 4–5, https://op.europa.eu/en/publication-detail/-/publication/998aeb09-4be6-11e9-8ed-01aa75ed71a1/language-en [accessed: 16 XI 2021].

Ustawa z 23 lipca 2003 r. o ochronie zabytków i opiece na zabytkami (Eng. Act of 23 July 2003 on the protection and care of historical monuments), Journal of Laws 2021, item 710).

DOI: 10.4467/27204383TER.22.016.15432

TERRORISM PREVENTION CENTRE OF EXCELLENCE

a new department within the counter-terrorism strand of the Internal Security Agency

The Terrorism Prevention Centre of Excellence (TP CoE) of the Internal Security Agency is a typical training department. Its activity is based on the provisions of the Act on anti-terrorist activities of 2016 and is focused on domestic and international cooperation forums remaining outside the sphere of the activity of the Counter-Terrorism Centre of the Internal Security Agency, which serve to acquire and exchange knowledge and good practices in the field of training to increase anti-terrorist awareness of institutions and citizens of the Republic of Poland at home and abroad.

The overt activity of the TP CoE related to training initiatives for the public is facilitated by participation in national and international conferences, workshops and other forms of information exchange that bring together academics and practitioners from different countries, and allows them to operate freely in order to obtain the best possible results from teaching activities.

In 2021, the TP CoE continued to conduct anti-terrorist trainings in the field of terrorism prevention and prophylaxis on three levels: directly by the Centre's trainers, online with the participation of external experts and through an e-learning platform. These trainings were based on a concept developed as a result of cooperation between foreign and national representatives of the academic sector, special services and EU institutions. The recipients of these training courses were other security services, ministries, central offices, government institutions and agencies, universities and business entities of key importance

to Poland's security. Over 3,000 people were trained in the framework of direct meetings.

Due to the very high interest of the entities of the Polish public administration and the private sector, which in the course of last year asked in large numbers for training of their employees, as well as due to the lack of possibility of direct meetings with these persons, the TP CoE trained over 50 thousand persons in 2021 in the framework of an e-learning course on terrorism prevention. This course is available on a website designed for government employees and public officials.

Simultaneously, the TP CoE actively cooperated at the national level by participating in conferences and thematic seminars organised in agreement with, among others, the University of Wrocław (Centre for Security Studies and Education) and the Civil Aviation Authority, as well as by undertaking its own initiatives, i.a. connected with raising the level of knowledge in the field of responding to threats of a terrorist nature in facilities having the status of critical infrastructure.

Conclusions resulting from the aforementioned activities will serve more effective acquisition and expenditure of external financing of projects and undertakings concerning security of CBRN and IED promoted at the European level, as well as support establishment and development of contacts with potential partners interested in project cooperation with the Internal Security Agency.

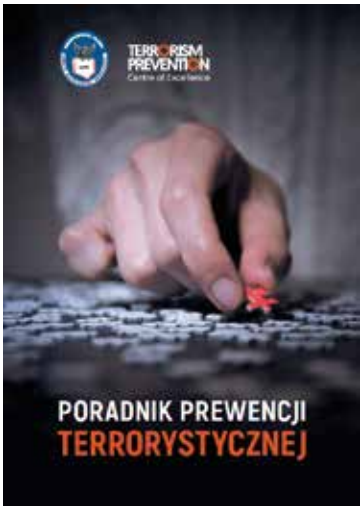
Furthermore, based on the positive reception of the 4U! Social Campaign (Watch out!, Run!, Hide!, Stop the attack!) launched in 2019, the TP CoE, in cooperation with the Ministry of Interior and Administration, presented a unified procedure for providing information in the event of a terrorist incident involving an armed perpetrator in November 2021. The recommended procedure for providing information to the operators of voivodeship emergency notification centres is an important step towards developing a uniform security culture in the emergency notification system related to a possible terrorist incident (covering the entire territory of the Republic of Poland).

The aforementioned initiatives carried out at the national level were based on the activity of the TP CoE abroad, in particular within the framework of European Union bodies (EU Working Party on Terrorism, Steering Board on Radicalisation, Network of Prevent Policy Makers, Radicalization Awareness Network, EU Internet Forum) and other forms of cooperation between EU Member States based on common objectives of project cooperation, inter alia in the area of counteracting radicalisation in penitentiary institutions and schools.

Thanks to the activity of the TP CoE, an agreement on scientific and didactic cooperation in the field of countering radicalisation and terrorist threats was signed by the Head of the Internal Security Agency, Colonel Krzysztof Wacławek, and the Director General of the Prison Service, General Jacek Kitlinski, on 27 October 2021. The TP CoE also actively participated in the works of the Organisation for Security and Cooperation in Europe and the OSCE Steering Committee for Counteracting Terrorism. In turn, activities undertaken in Poland in the area of aviation security would not be possible without cooperation with the European Civil Aviation Commission (ECAC) and the International Civil Aviation Organisation (ICAO).

At the same time, of the TP CoE conducted bilateral cooperation with partners from EU and non-European countries, as well as participated in projects co-financed from external funds, such as: "EU-HYBNET - Empowering a Pan-European Network to Counter Hybrid Threats", "PREVENT PCP - Pre-Commercial Procurement of innovative technology solutions to support security in public transport", "INDEED - Evidence-based model for evaluation of radicalisation prevention", "More efficient identification of asymmetric threats - trends, indicators, dependencies" and "Increasing the competences of state security services, public administration employees

The TP CoE in 2021 – in numbers	
Face-to-face (direct) trainings	103
Persons trained directly	3 150
Persons trained online	53 405
Meetings with foreign partners in Poland	4
Meetings with foreign partners abroad	3
International meetings online	51



and scientific and research centers and the development of their cooperation in the area of national security". Within the framework of the last project a Terrorism Prevention Brochure was developed (in paper and electronic versions), which is distributed to selected representatives of public administration and entities cooperating with the TP CoE. The study is available in Polish and English language versions and constitutes a compendious summary of a five-module training programme, which was prepared by external experts in 2020 in the framework of the EU project PO WER ("Operational Programme Knowledge Education Development").

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 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).

Jędrzej Łukasiewicz, PhD Eng. - Assistant Professor in the Department of Aviation, Faculty of Civil Engineering and Transport, Poznań University of Technology and a flying instructor of unmanned

aircraft at the training centre of Poznań University of Technology. Participant in expert bodies at the EU level (DG MOVE, DG HOME) and at the national, interministerial level for the safety of critical infrastructure and building resilience to threats from unmanned aerial vehicles.

Aleksander Olech, PhD - Director of the European Security Program at the New Europe Institute. Graduate of the European Academy of Diplomacy. He gained his research experience at Université Jean Moulin Lyon 3, Institute of International Relations in Prague, Institute for Peace Support and Conflict Management in Vienna, NATO Energy Security Centre of Excellence in Vilnius and Baltic Defence College in Tartu. Scholarship holder of OSCE & UNODA Peace and Security, the NATO 2030 Global Fellowship and Casimir Pulaski Foundation.

Anna Rożej, 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.

Lieutenant Colonel Artur Sybicki - officer of the Terrorism Prevention Centre of Excellence of the Internal Security Agency, responsible for organizing and conducting anti-terrorist trainings for representatives of the Polish state administration. Since 2005 he has been dealing with issues related to counteracting terrorist incidents on the territory of Poland.