POLISH ASSOCIATION FOR NATIONAL SECURITY

TERRORIST THREATS IN THE REPUBLIC OF POLAND IN 2021-2022

Polskie Towarzystwo Bezpieczeństwa Narodowego

REPORT PTBN
VOL. IV (2023)

ISSN 2720-037X | ISBN 978-83-962605-2-9

TERRORIST THREATS IN THE REPUBLIC OF POLAND IN 2021-2022

Raport PTBN

Vol. IV (2023)

Polskie Towarzystwo Bezpieczeństwa Narodowego

Warsaw • 2023

PTBN Report, Vol. IV (2023): “Terrorist threats In the Republic of Poland In 2021-2022”

Developed by the team composed of:

Magdalena Adamczuk, PhD
Jarosław Cymerski, PhD
Krzysztof Izak
Maciej Kluczyński
Adam Krawczyk, PhD
Katarzyna Maniszewska, PhD
Daria Olender, PhD
Michał Piekarski, PhD
Anna Rożej-Adamowicz, PhD
Damian Szlachter, PhD
Jarosław Tomasiewicz, Associate Professor, University of Silesia in Katowice
Karolina Wojtasik, PhD

The content of the PTBN Report contains purely personal views of the authors and does not necessarily reflect the official positions of the institutions in which they are employed.

PTBN Report, Vol. IV (2023): “Terrorist threats In the Republic of Poland In 2021-2022” was closed and submitted to print on 20 April 2023. The online version is its original version.

The author of the cover photo is Tomasz Michalak, PhD.

The online version of the Report is available at www.PTBN.online.

ISSN 2720-037X
ISBN 978-83-962605-2-9

Polskie Towarzystwo Bezpieczeństwa Narodowego
(KRS 0000583118)
ul. Odkryta 38A/8, 03-140 Warszawa
e-mail: zarzad@ptbn.online
www.PTBN.onLine

https://www.facebook.com/polskie.towarzystwo.bezpieczenstwa.narodowego/
https://twitter.com/PTBNonLine

ISBN 978-83-962605-2-9

Spis treści

Introduction

Two years have passed since the Polish Association for National Security published its previous Report on terrorism. This has been a period characterised by rapid twists and perturbations, to mention only the outbreak of the COVID-19 pandemic and the war in Ukraine. The speed and unpredictability of change makes it difficult to respond adequately, so unfortunately the situation regarding Poland's internal and international security cannot be said to have improved. The threats signalled in the previous report persist, while the ideological and political polarisation, which is destructive to the functioning of the state and society, has not disappeared or weakened even in the face of external threats. Although the threat of 'imported' terrorism (primarily jihadist terrorism) has fallen from the media spotlight, its potential persists and it is feared that it will increase in the long term. Instead, new threats have added to the previously existing ones. COVID-19 destabilised not only the economy, but also the public's mental health, and the resulting dissatisfaction with restrictions reinforced extremist tendencies. The time of the pandemic has been used by our adversaries to test new methods and tools of warfare below the threshold of war, aimed at undermining the existing order, questioning the effectiveness of international institutions, deepening chaos, creating divisions and increasing influence in specific areas. Times of crisis are conducive to hybrid activities, including in cyberspace and information manipulation. Moreover, the pandemic has confirmed the link between internal and external security that results from the internationalisation of many spheres of state, economic and social activity. The intensifying geopolitical situation has presented Poland with a new challenge: the instrumentalisation of migration. After 24 February 2022, the potential threat of acts of diversion and sabotage came to the fore.

The new, more complex situation necessitates expanding the field of analysis also to include instruments of hybrid warfare, especially in the cyber domain. Cyberspace, on the one hand, and the maritime and coastal area, on the other, have been identified

as key in this context. Cyberspace is a new, relatively under-recognised and rapidly changing theatre of operations, which enables both propaganda and psychological operations, as well as intelligence and sabotage operations. The seacoast and coastal waters appear to be the most vulnerable to enemy penetration, while at the same time the importance of these areas to the economy (if only in terms of energy imports or humanitarian and military support to Ukraine) can hardly be overestimated. This calls for particular concern for the critical infrastructure present in this part of the country – strategic for maritime or rail transport and for Poland's energy security. The blow-up of the Nord Stream II pipeline, the reconnaissance activities in relation to the Baltic Pipe or in the vicinity of the oil transshipment terminal prove this clearly.

The report consists of three chapters. The first describes the existing and potential threats in the areas of terrorism (and its underlying extremism), cybersecurity and maritime security. The second analyses selected elements of the Polish anti-terrorist system. The third contains conclusions and recommendations resulting from the comparison of challenges and responses.

The Report was developed by the PTBN Terrorist and Hybrid Threat Analysis Team based on information materials available in the public space, analytical reports, monographs and post-conference publications, websites of selected state institutions, EU and NATO institutions and organisations, as well as a broad spectrum of national legal acts.

The purpose of this Report is to provoke a constructive discussion on the direction of development of the national anti-terrorist system. The Report is addressed to researchers into the phenomenon of terrorism, journalists dealing with this issue, as well as to those who have developed the Polish anti-terrorist system or are currently working on its improvement and effectiveness. The special addressees of the Report are representatives of all state institutions and bodies that form the "anti-terrorist community of the Republic of Poland" on a daily basis.

The idea of the Polish National Security Association is to build "security beyond divisions", therefore we invite all interested parties to discuss one of the key subsystems of national security, which is an incubator of future standards in this area. The results of this discussion will be presented in subsequent updates of this paper.

1 Characteristics of terrorist threats to Poland in 2021-2022

1.1. Terrorism in European countries

Europol's TE-SAT report for 2022 indicated a significant decrease in the number of terrorist acts in Europe, both committed, failed and stopped by law enforcement agencies of EU member states, compared to previous years. This trend appears to have been mainly influenced by the pandemic and the cyclical restrictions put in place to limit ease of movement, as well as a reduction in the influence of Islamic radicalism following the fall of the Islamic State. In 2019, 55 attacks were carried out or attempted in Europe[1], 57 in 2020 and 15 in 2021, with a decrease mainly in attacks by national liberation and separatist groups (no attacks) and far-left groups (one attack). The report highlighted the regional activities of radical leftist and anarchist organisations in Europe. Polish extremist groups cooperated with their counterparts from the Czech Republic, Germany, Slovakia and Belarus. Europol reports the following statistics for Poland: TE-SAT2020: 1 attack, 4 arrests in 2019; TE-SAT2021: 9 arrests in 2020 and TE-SAT 2022 notes the arrest in 2021 in Poland of three individuals linked to terrorist organisations or activities of unspecified ideology.

Similarly, the *Global Terrorism Index 2020* indicates a low terrorist threat in Poland, which is qualified in 114th place (with an index of 0.239, compared to first place for Afghanistan with a score of 9.592 on a 10-point scale). In turn, the report

[1] The statistics quoted are from the Europol reports TE-SAT2020, 2021 and 2022, which show the number of attacks committed, failed and foiled by the services. Data is presented without UK, which is not included in the Europol report since TE-SAT 2021.

Global Terrorism Index 2022 indicates that there are no acts of violence qualified as terrorist activities in Poland. The report ranked Poland last, 93rd, along with EU countries such as Portugal, Slovakia, Slovenia, Hungary, Estonia and Latvia. Lithuania (ranked 83), the Czech Republic and Denmark (ranked 86), Romania (ranked 78), Sweden (ranked 69), Spain (ranked 55), Austria (ranked 52), Germany (ranked 33), and Greece (ranked 29) ranked higher. The *Global Terrorism Index 2023* report, which was released in March 2023 and presents data for 2022, indicates that this trend has continued: Poland is again ranked among the safest countries in the world in terms of terrorist threats, placing once again in 93rd place.

The pandemic highlighted the polarisation of social life in the EU by intensifying extremist attitudes. According to *TE-SAT Reports 2022 and 2021*, radical groups introduced new ways to recruit members and created a wide base of followers. These groups used slogans of fighting to 'preserve freedom' and 'save the economy' also sending out a call for civil disobedience or even physical resistance to the introduced restrictions due to COVID-19. Often these slogans were linked to conspiracy theories about 5G technology or the QAnon movement. Such actions have been noticed across Europe (also in Poland), where arson or vandalism of telecommunications infrastructure has occurred.

Funding for extremist groups in Poland has often been through legitimate businesses selling accessories, clothing, music, etc., as well as through online collections.

The services point out that as a result of restrictions and lockdowns, which have reduced the mobility of group members, their communication has almost entirely moved to the Internet. In Poland, too, extremists have used it to maintain national and international relations with groups in other countries. The TE-SAT 2021 report indicates that despite restrictions on travel and meetings and concerts, contacts between the Polish faction of the Blood & Honour group and counterparts from other countries continued and even intensified. One of the axes of narrative linking right-wing extremists from different European countries is a dislike of the European Union perceived as a 'common enemy'.

As a security threat, the *TE-SAT 2021 Report* identified the increasing participation of members of radical groups in paramilitary camps, survival workshops, firearms training and hand-to-hand combat training. The report notes a significant increase in interest in such activities among right-wing extremists in Poland.

1.2. Hybrid threats and terrorist threats in the context of Russia's aggression against Ukraine

The aggression against Ukraine, which began on 24 February 2022, is a factor intensifying the Russian hybrid campaign in Poland. The object of this campaign is primarily Poland's assistance to Ukraine, including support for refugees from Ukraine, the transfer of military and humanitarian aid and the presence of significant allied forces in Poland. The war in Ukraine also increases the risk of a terrorist or sabotage event in Poland inspired by the Russian Federation with the possibility of the use of third country resources. On 28 February 2022, the BRAVO alert level was introduced on the territory of two voivodeships – Podkarpackie and Lubelskie – and on 15 April 2022 its duration was extended until 28 February 2023 and its territorial coverage was extended to the entire country. From 6 October 2022, the BRAVO level also covers Polish energy infrastructure outside Poland, including oil rigs and other facilities located outside Polish territorial waters.

In Ukraine, Russia has failed to achieve its political objectives by military means. Revealed weaknesses in the Russian armed forces and arms supplies from the West have resulted in frontline failures. In addition to actions of a strictly military nature, the Kremlin continues its hybrid campaign to weaken the will to fight in Ukrainian society, confidence in the authorities and democratic state institutions. These actions – below the threshold of war – focus primarily on disinformation, cyber attacks, forcible deportations and attacks on critical infrastructure. It is possible that Russia, looking for new ways to compensate for its own deficits in conventional armed forces and the ineffectiveness of hybrid measures, will undertake terrorist and sabotage actions in countries that act as Ukraine's frontline logistical base, such as Poland and Romania. Similar actions have already taken place, for example, in 2014 there were attacks on ammunition depots in Vrbětice in the Czech Republic.

Such attacks may be aimed at disrupting logistical processes (transport of military aid), influencing Polish society and the societies of Western countries, or causing disruptions in Poland's economy and political system to such an extent as to force Poland to behave in line with Russia's interests.

In particular, assaults or acts of sabotage against the following targets are possible:

1. Attacks on critical infrastructure, especially energy and transport infrastructure (rail, sea, air, road). The aim may be to render it unusable (e.g. airports and seaports, or railway yards) and to demonstrate the ineffectiveness of its protection and

the state's inability to cope with an attack-induced domestic or international crisis of a political, economic or environmental nature (in the case of sabotage or terrorist actions that result in an environmental disaster such as an attack on a transport or fuel storage facility).

2. Attacks on military facilities, equipment and personnel of Poland and NATO allied countries temporarily present on the territory of Poland: destruction of important and difficult to replace military equipment, killing or abducting soldiers, contamination of the area of deployment of military units. The purpose of such an attack would be to demonstrate the inability of the armed forces to protect their own personnel and installations. In the case of an attack on soldiers of allied states, it may be linked to an informational impact targeting the societies of both Poland and those states. In Poland, the adversary may seek to provoke negative sentiment towards foreign armed forces, while in the Allies it may provoke a reluctance to engage forces and resources in actions that do not directly affect the societies of these countries.

3. Attacks on a well-known person or a symbolic target. Such an attack could aim to provoke public reactions, in particular to deepen political polarisation. In order to give the impression that the perpetrators of the attack are persons not linked to Russia, it could have the character of a so-called 'false flag' provocation.

In particular, it should be noted that the above actions are likely to be carried out using both terrorist methods and hybrid tools. For example, an attack targeting critical energy infrastructure (e.g. a transhipment terminal, a fuel depot, a seaport, a mining platform, an electricity grid, a strategic rail transport corridor) may be supported by a disinformation campaign suggesting the threat of fuel unavailability in the market. An attack that targets military infrastructure may be supported by a demonstration of military force or other actions creating the impression that Poland is particularly vulnerable to attack at any given time. It is also possible to create panic with false bomb alarms (as during the May 2021 graduation exams).

The risk of such threats is increased by the fact that Russia has to modify the nature of its operations. The rapid abandonment of imports of eastern energy raw materials by western countries has meant that Russia may try to disrupt other routes of their supply, not only those of the Middle East, but also those of the Baltic. This would then allow economic and political pressure to be applied in the form of an offer of gas supplies in exchange for political concessions.

In 2023, we should expect a further intensification of the Russian disinformation campaign against Poland, aimed at further polarising society, undermining trust in state institutions and, above all, in democratic electoral processes.

1.3. Use of methods of a terrorist nature by domestic radical circles

Hubert C., a resident of the Lubelskie Voivodeship, set fire to a vaccination point at COVID-19 and the headquarters of Sanepid in Zamość in August 2021. A year earlier, he also set fire to two 5G mobile network masts in his home town of Złojec. Hubert C. fled to Switzerland in 2021, but was apprehended a few months later in the Podkarpackie Voivodeship by the Police. In his trial, Hubert C. was described as an adherent of conspiracy theories radicalised by material sourced on the internet about the alleged harmfulness of 5G technology and the movement's propaganda against sanitary restrictions related to the COVID-19 outbreak.

The District Prosecutor's Office in Zamość accused Hubert C. of setting fire and causing considerable material damage (totalling PLN 370,000), but also of acting in a terrorist capacity. According to the prosecution, these acts were carried out with the aim of intimidating many people. In court, the arsonist pleaded guilty and expressed remorse by voluntarily submitting to the sentence. He was found guilty in September 2022 and sentenced to five years in prison. Hubert C. was exempted from court costs, but must additionally cover the financial losses incurred by sanitary inspection and the Lublin Voivodship Office, as well as the operator of the attacked mobile network.

1.4. Selected incidents related to the activities of foreign terrorist organisations

In 2021, the spokesman for the Minister of the Coordinator of Special Services Stanisław Żaryn stated: "ABW's findings indicated [...] that people providing logistical support for

jihadists are located in Poland. Since 2016, ABW has detained several times people: preparing terrorist attacks, involved in financing ISIS, spreading jihadist propaganda, radicalising other people or raising funds for the Islamic State. ABW's activities were also directed at identifying and expelling from Poland those foreigners who actively

participated in or supported ISIS militant activities. At the request of the ABW, dozens of foreigners associated with Islamic terrorism have left Poland in recent years"[2].

a. The case of an Afghan national involved in an attack on a Polish military patrol in Ghazni in 2011.

On 21 December 2011, an improvised explosive device (IED) detonation occurred in the village of Rawza in Afghanistan's Ghazni province. The attack resulted in the deaths of five soldiers from the 20th Mechanised Brigade from Bartoszyce. It was the deadliest attack on a patrol of Polish soldiers on a stabilisation mission in Afghanistan. The Taliban claimed responsibility for the attack. As a result of an investigation conducted by the Military Counterintelligence Service (SKW) with the support of the Military Intelligence Service (SWW), at the beginning of 2012, the Afghan authorities arrested 5 terrorists co-responsible for the attack. Information provided to Afghan law enforcement authorities contributed to their arrest. Information gathered in the case indicated that the Taliban commander Eid Mohammad, who was hiding in Pakistan, was the main suspect in organising the attack. He was eventually shot dead on 7 February 2020 by Afghan security forces (NDS) during an attempted arrest.

Among those detained in 2012 who were involved in the preparation of an attack on a Polish military patrol entering the town of Rawza was an Afghan interpreter employed at a base in Ghazni who had cooperated with the Taliban. After his release, the interpreter sought evacuation to Poland after the Taliban took power in Afghanistan in August 2021, but this was successfully blocked thanks to the negative stance of the SKW.

b. The case of the Palestinian in Olsztyn

On 24 May 2021, the Border Guard, acting at the request of the Internal Security Agency, detained a religiously radicalised man from the Palestinian Authority with a propensity for violence against bystanders. The man posed an imminent threat to the internal security of the Republic of Poland, as he possessed skills in chemistry, technology or the handling of firearms and maintained relations with members of terrorist organisations. Pursuant to a court decision, the Palestinian was placed in a guarded centre of the Border Guard and from there the foreigner was deported from Poland.

[2] S. Żaryn, *Terroryzm aktualnym wyzwaniem* (Eng. Terrorism as a current challenge), "Biuletyn Analiz i Reagowania RCB", no. 32, Warszawa 2021, p. 3.

c. The case of a citizen of Georgia

In July 2022, the Internal Security Agency, in cooperation with the Border Guard, detained a citizen of Georgia, Mamuka T. alias Abubakar T., on suspicion of conducting terrorist activity on the territory of Poland. The legal basis for the apprehension of the Georgian was a decision of the Minister of the Interior and Administration on obliging the foreigner to return and prohibiting his entry into the Schengen area for 5 years. The foreigner was in contact with persons involved in terrorist activity who took part in armed actions in support of the Islamic State (ISIS). Abubakar T. was involved in the illegal migration of Arab nationals in Poland for the purpose of trafficking them to Western European countries, as well as being a member of a criminal group trafficking drugs and carrying out extortionist robberies in Poland. Abubakar T. was deported from Poland to Georgia several days after his arrest.

d. Migration crisis at the EU's eastern border and terrorist threats to Poland

Against the backdrop of the migration crisis on the EU's eastern border caused by Alexander Lukashenko's regime against Poland and Lithuania, the results of an in-depth verification of the identities of more than 200 foreigners detained in the Border Guard's guarded centres were presented at a press conference of the Minister of the Coordinator of Special Services and the Minister of National Defence on 27 September 2021. At the time, a spokesman for the Minister of the Coordinator of Special Services, Stanisław Żaryn, noted that "the information concerning one in four of those investigated indicates their dangerous connections and their involvement in illegal practices. The findings made so far show that one in ten has possible links to terrorist organisations, criminal offences, human smuggling, as well as falsification of documentation"[3]. Additionally, 20 per cent of the illegal immigrants detained in Poland had permanent ties to the Russian Federation.

Data made available to PAP on 19 August 2021 by Stanisław Żaryn shows that on the basis of the Act on anti-terrorist activities, in the first half of 2021, the ABW placed foreigners 14 times on the list of undesirable persons in Poland of the ABW's Counter-Terrorism Centre (CAT). In addition to this, one application by the Head of the ABW concerned the issuing of a decision to oblige a foreigner to return due to fears that he or she may carry out terrorist activities on the territory of the Republic of Poland, and another concerned the revocation

[3] S. Żaryn, *Napięta sytuacja na granicy* (Eng. Tense situation at the border), "Polskie Radio 24", 27.11.2021, in: https://polskieradio24.pl/5/1222/artykul/2815251,napieta-sytuacja-na-granicy-zaryn-wsrod-zatrzymanych-osoba-posiada-jaca-kontakty-z-panstwem-islamskim (accessed: 21.12.2022)

of refugee status on the territory of Poland. In comparison, 14 foreigners posing a terrorist threat were expelled from Poland between 2015 and 2019 on the basis of ABW materials.

In the long term, the potential for a terrorist threat from this direction will depend not only on the effectiveness of the services, but also on the capacity of the Polish state and society to integrate immigrants in order to counteract their radicalisation.

The case of a citizen of Tajikistan

In April 2021, Odilkhon S., a citizen of Tajikistan, entered Poland through an illegal migration route organised by Belarusian services. He was subsequently detained by the Border Guard and placed in a guarded centre for foreigners. The detainee's activity in the centre indicated his religious radicalisation. The ABW, in the framework of countering terrorist threats, established that the above-mentioned man is a sympathiser of the Islamic State. Odilkhon S. received a decision from the commanding officer of the Border Guard post in Płaska to oblige him to return to his country of origin and to ban him from re-entering Poland and Schengen countries for a period of 3 years. The **man** was recognised by the ABW as a threat to the security of the Republic of Poland and deported on 10 November 2021 from Poland.

The case of an Iraqi national

In the course of the migrant crisis on the Polish-Belarusian border, an Iraqi citizen, Husham M.H., was brought to Poland, who during his stay in a centre for foreigners run by the Border Guard was proven to have contacts with a person with links to terrorism. That person was an explosives specialist, a member of the Islamic State, detained in 2021 on the territory of one of the European Union countries. Husham M.H. was deported from the Republic of Poland on this basis in 2022.

1.5. Terrorist threats against Polish citizens abroad

On 23 May 2021, a Ryanair flight from Athens to Vilnius (flight no. FR4978), carrying Belarusian opposition blogger Roman Protasevich and 100 other people, was forced to land at Minsk airport. Polish citizens were also among the hijacked passengers.

Evidence collected by Polish law enforcement authorities and the services of the countries conducting their investigations in this case (including the USA, Lithuania, Greece)

and the ICAO (*International Civil Aviation Organisation*) shows that at the time of the incident, an officer of the Belarusian civilian special service (KGB) was in the operations room of Minsk's air traffic control tower, making decisions for the air traffic controller at the crucial moment. It was from the KGB officer that the instructions and decisions to bring the aircraft to Minsk airport, escorted by military MIG-29s, were coming, allegedly due to a bomb threat allegedly received by email from the terrorist organisation Hamas (a Hamas spokesperson denied the organisation's connection to the message).

According to the Polish services (Civil Aviation Authority, ABW), the whole situation was provoked by the Belarusian side in order to hijack flight FR4978 and bears the hallmarks of state terrorism. According to Ryanair airline chief executive Michael O'Leary, the whole affair is a diversion and 14 times "state-sponsored piracy". The US Department of Justice (federal court in New York State) charged four Belarusian nationals with unlawfully diverting a passenger flight with US citizens in order to arrest a Belarusian dissident.

1.6. Radicalisation as a potential source of terrorist threat

a. Radicalisation

Acts of politically and/or ideologically motivated violence, which pose an immediate threat to public safety, are generally the end result of a long-term radicalisation process. Radicalisation does not necessarily culminate in violence, but it is always a potential threat that requires monitoring (spontaneous, impulsive acts of violence also occur, but their significance is marginal). Violence can be the work of (a) individually radicalised individuals, (b) individuals radicalised in a group but acting individually, (c) radical groups acting spontaneously (e.g. demonstrations) or (d) in an organised manner.

Radicalisation is not a one-off action, but a process that can go faster or slower. The individual goes through stages that form a sequence. **The process of radicalization** involves the adoption by an individual or group of views and attitudes that are considered extreme, that is, significantly divergent from the mainstream consensus, challenging the foundations of the social order. Radicalisation can take place roughly speaking in two ways: (1) through the adoption of radical views from the grassroots by a previously apolitical individual, (2) through the gradual radicalisation of previous beliefs, manifested in an escalation of demands, a reduced willingness to compromise, a tendency to resolve disputes by legal or non-legal coercive methods (violence).

Ultimately, this can lead to violent actions, both in the symbolic and physical spheres. Radicalisation can take place under the influence of a group (environment, organisation) to which the individual belongs or maintains contact, as well as individually, when the radicalising person initiates the process himself, without interaction with other extremists (self-radicalisation).

Reasons for radicalisation can be: (a) deterioration of an individual's status, (b) fear of deterioration of status, (c) failure to improve status to a degree consistent with aspirations. This applies both to material status (disposable income, which is important – in the context of wealth stratification) as well as intangibles: freedoms (including a sense of agency, control over one's own life, influence on one's environment) and prestige (including identity issues).

Lack of satisfaction in any of these aspects leads to feelings of harm, exclusion and injustice. Research (e.g. by the Dialogue about Radicalisation and Equality programme) shows that the key issue is not the objective status of the individual, but his or her subjective feeling (especially in the non-material sphere). This is particularly relevant in the case of the youngest age group (so-called zoomers), who attach great importance to individual well-being, which can be violated not only by aggression in the broadest sense (action), but also by lack of attention or respect (failure to act). As a result, radicalisation can be triggered not only by systemic injustice (the legal state, the functioning of public institutions), but also by ideological injustice (symbols important to an individual's identity, including language) and contextual injustice (the various environmental and situational factors that make up the environment of an individual's everyday life). Many theories of radicalisation also mention the moment when the individual finds a 'culprit' for his or her condition and it is towards this person/group/institution that violent actions are directed. The individual may perceive a threat to his or her status in both internal and external factors.

Radicalisation takes place in a certain external environment that can either favour or counteract it. We can divide the **conditions** accompanying radicalisation into three groups: macro-structural (the political and economic situation in the country), micro-structural (the individual's immediate environment: family, social, neighbourhood, professional groups) and individual (individual characteristics: personality, experiences).

At all these levels, a deterioration/increase in the potential for radicalisation in society could be observed in 2021. The main factor of a macro-structural nature remained the COVID-19 pandemic, which, after a summer of calm, took on a new dynamic

in the autumn. Despite the good economic situation, the pandemic continued to threaten the functioning of certain areas of the economy, especially small business and the service sphere; in turn, accelerating inflation hit primarily the incomes of employees in the budgetary sphere. Poland's international situation was determined to the greatest extent by the migration crisis provoked by the Belarusian authorities, when, in the second half of the year, there were organised violations of the state and EU border on an unprecedented scale. Characteristically, even the pandemic and migration crisis did not lead to the development of a consensus, as both sides of the political conflict were only interested in pursuing their own goals (above all – weakening the opponent). The inability to reach a common compromise position even on the fundamental issue of the external threat, contrasting even with the national consensus towards the migration crisis in Lithuania, is very worrying.

At the micro-structural level, a continuation of previous trends could be observed: the disintegration (or at least weakening) of previous interpersonal ties was accompanied by a search for and formation of new ties on the basis of political and world-view convergence, which was facilitated by the transfer of activity to the Internet during the lockdown of the previous year. The Internet provides a sense of anonymity and impunity, offers a wealth of unverifiable information in which everyone can find confirmation of their beliefs; it allows one to find like-minded people and, consequently, an environment that provides different types of support, a sense of participation and spiritual leadership. With its algorithms, social media facilitate the formation of 'filter bubbles' (creating a kind of information barrier, preventing alternative information from entering a closed environment), which sometimes become so-called 'echo-chambers', amplifying the message of extremists.

One might venture to say that also at the individual level one can perceive an increased vulnerability to radicalisation. Typically, young people are most susceptible to succumbing to extremism, as they are building their own identity by revising existing values ('youthful rebellion'). The effect of the pandemic, as observed by psychologists, is a destabilisation of the psyche of many people (also adults) caused by a loss of lifestyle and fear for health and life, manifested in irritability, hyperactivity and a tendency to paranoia (belief in conspiracy theories).

Radicalisation is a mental, internal process, but different **manifestations** can be observed. They are most easily seen on the Internet. While malicious presentation of the opponent, biased selection of facts, replacement of factual arguments with demagogic ones should be considered a natural, common element of political propaganda, the following are undoubtedly symptoms of radicalisation: (1) use of emotionally

charged (e.g. vulgar) insults; (2) dehumanisation of the opponent (also through, e.g. insults, deformation of names and surnames); (3) approval of violence, and even more so incitement to it. Even a cursory review of the Polish Internet reveals that all these phenomena have become commonplace in social media, online commentary and even some, for the time being, niche portals and blogs. Radicalisation can also be observed in the icon-graphic layer (avatars, overlays), and – in the most tangible manner – in the frequency of visits to extremist websites or the number of likes on profiles and posts on Facebook, Twitter, Instagram or Youtube. Radicalisation can also be seen in public spaces, where symbols, images and slogans associated with extremism appear on clothing, cars, walls, etc.

The above-mentioned manifestations of radicalisation can pose a threat to public safety by fuelling the spiral of aggression and, as the French sociologist Gilles Kepel argues in his research, can directly lead to acts of violence, including terrorist attacks. In particular, belonging to a radical group (including a virtual one) is conducive to violent actions, as it strengthens group bonds (group actions) and ensures individual acceptance (individual actions). Writing a slogan or drawing a symbol on the façade of someone else's building can already be considered a manifestation of symbolic violence, while destroying a symbol or propaganda medium (e.g. a poster) of an opponent manifests a readiness for destructive actions. This applies not only to strictly political symbols, but also – in connection with a conflict of world views – also historical and religious symbols (Christian, Judaic, Muslim). Buildings of this nature may also become objects of aggression (arson attacks on a church in Lublin in February 2021, on a cathedral in Opole on 19 December 2021).

The next step becomes verbal and physical violence directed directly at political opponents (and sometimes random representatives of hated communities – but here it is sometimes difficult to distinguish from common crime). Violence against people has so far tended to be dispersed, spontaneous and chaotic. Its most frequent manifestation is verbal attacks. The most worrying form of these are threats (sometimes taking the form of 'death sentences'), and it should be stressed that the threat does not become less when the perpetrators are unbalanced individuals. It is a comforting symptom that, in contrast to the previous year, more serious acts of violence during mass street demonstrations were avoided in 2021.

While in the 1990s and early 2000s the main causes of radicalisation were economic (pauperisation of large social groups as a result of political transformation), and in 2014-17 radicalisation was triggered by fear of external factors (including: aggressive policies of the Russian Federation, Islamic terrorism associated with non-European

immigration), in 2021 other factors became the drivers of radicalisation: (1) internal political polarisation, (2) the pandemic and related restrictions. It is important to note that the radicalisation processes signalled in the previous Report have worsened in 2021.

In the case of polarisation, the conflict is not only between feuding political groupings. Improvements in the status of some groups are perceived by others as a threat to their own status; this applies both to the material (poor/rich) and immaterial spheres (traditionalists/progressives). As a result, it is not only politicians but entire social groups (professional, worldview, age, territorial, etc.) associated with support for the opponent that are subject to hostility. Resentment towards the government, towards the ruling political orientation is transferred to other state institutions, especially the police. These phenomena may increase the deficit of social trust to a level that anarchises the state, paralysing the functioning of its apparatus. The scenario that, regardless of the actual outcome of the next elections, the losing side will not recognise their legitimacy is becoming increasingly real. It is not difficult to see that such a situation can easily be exploited by external opponents.

b. Political and social radicalism in Poland in 2021-2022

Polarisation leads to a situation in which there are no institutions, symbols or values that can unite the whole society or at least a significant majority of it. Each of the parties to the conflict has its own media and scientific and moral authorities, allowing them to operate in closed systems. The parties to the conflict even have an interest in fuelling radicalisation, as this maintains a high level of mobilisation of their own supporters, while allowing them to shift responsibility for the conflict onto the opponent. The violent behaviour of their own extremists is passed over in silence, downplayed (generally described using different language to the same acts of their opponents) and even excused ('I disapprove, but I understand'), although, it should be noted, still not condoned. The main political camps have become hostage to their own extremists, who are indispensable in order to muscle in on their opponents. The result was an increasing number of violent incidents in 2021 (e.g. vandal-type attacks on MPs' offices).

However, extremists as a centrifugal force are becoming uncontrollable, which is beginning to be a threat to the cohesion of the main political forces. The propensity to use violence starts to be transferred even to their own milieu (vide the clashes between different groups of left-wing extremists in March 2021 in Poznań (PyRa collective vs Roz-brat) – or in Warsaw on Wilcza Street in December 2021. (Syrena squat and Stop Bzdurom collective vs Przychodnia squat). The phenomenon of the "relay of extremisms" (the emergence of ever more radical factions) is leading to a fragmentation of the political scene,

a kind of 'reproduction by division and budding'. There has been a revival of seemingly extinct forms of extremism, such as pan-Slavic anti-Semitic nationalism or the Stalinist variant of communism. These have survived in virtual space, sustained at times by trolling, to gather followers under favourable conditions and go out into physical space (a similar phenomenon could be seen earlier in the case of the American Alt-Right).

Further deepening of these trends may lead to a 'Balkanisation' of the Polish political scene, providing extremists with a disproportionately large role. This can be called the "centrifugal effect", when the erosion of the political centre is accompanied by an increase in the importance of extremists, the centre of gravity of the political scene shifts to its periphery. Under conditions of extreme polarisation, the extremists marginalise or even eliminate the moderates in their own camp (historians refer to this as 'the revolution devours its own children').

The protest movement against pandemic restrictions, commonly referred to as the anti-vaccine movement or (more correctly) the coronasceptic movement, is specific in nature. It is a leading representative of a growing segment of extremism in recent years, which consists of believers in conspiracy and/or para-scientific theories. Closely linked to the coronasceptic movement – through the pseudo-scientific theory of "torsion fields" – is the anti-5G movement, which raises the dangers of the development of new technologies. Its agitation can also lead to the use of violence (generally sabotage). Due to the amorphous structure of these communities, which are mainly active on the Internet, they provide a convenient environment for disinformation and destabilisation operations (although the PTBN Report "5G Technology and Information Threats to Critical Infrastructure" of 2022 notes that "The data obtained is also insufficient to determine whether the phenomenon had the character of inauthentic interference in the information space, e.g. by a foreign entity acting on orders from foreign secret services").

The 'anti-vaccine' movement is worldwide, but noticeable mainly in countries in the wider West, associated with radical right-wing organisations (although left-wing extremists are also sometimes involved). The activities of coronasceptics involve not only disinformation, spreading fake news online, but also acts of violence, vandalism, threats against politicians and doctors, demonstrations and picketing. With the increase in criminal acts by these groups in European countries, it is suggested that they should be recognised as criminal or even terrorist organisations. There is also a process of politicisation of the demands of the anti-vaccine movement, by extreme sections of the political scene. In Poland, this phenomenon, although associated with the radical right, basically remains in opposition to the ruling camp, contesting even the mildest manifestations of anti-covid policy and even the reality of the pandemic itself.

The activity of radical 'anti-vaccine' groups in Poland in 2021 increased dramatically. The demands proclaimed by them mainly concerned: the abolition of restrictions or their non-imposition (lockdown, wearing masks, social distancing, the functioning of the so-called 'covid passport') and the non-use of Covid-19 vaccines or their non-imposition as mandatory. This is sometimes combined with anti-Semitic and pan-Slavic slogans. Anti-vaccine organisations operate on the basis of an unguided resistance strategy: it is a loose network of local groups with no unified leadership. Most of its participants are non-violent, but distribute fake news about the pandemic on the Internet and deny the achievements of modern medicine, creating an atmosphere of ideological support for extremists and conspiracy theorists.

However, the radical part of the coronasceptic movement uses demonstrations of force (e.g. anti-vaccinationists in paramilitary uniforms organised a demonstration on 4 August 2021 discouraging vaccination at the market square in Poznań), verbal violence (threats against health professionals and state institutions) and even physical violence (arson, devastation). Aggression starts with hate speech on internet portals or incitement to anti-state actions and ends with acts of physical violence. In December 2021, threatening letters and accusations of treason were sent to politicians of various political options declaring support for pandemic restrictions. These were signed by the Sovereign of the Polish Nation, the Polish National Tribunal and the Committee for the Prosecution of Crimes against the Polish Nation. 'Death sentences' and threats of deprivation of life were received by the presidents of Białystok, Gdańsk, Wałbrzych and Wrocław, among others. Anti-vaccinationists made death threats against the head of the Polish People's Party (PSL) and the spokesman for the Ministry of Health on the streets of Karpacz during the XXX Economic Forum. Coronasceptics are also likely to be responsible for dozens of bomb alarms in schools and offices across Poland. On 8 August 2021, a threat to blow up the Malta Thermal Baths and aquapark in Poznan (1,800 people were evacuated) was sent by email, due to the opening of the ticket offices to the vaccinated which was supposed to relieve queues before entering the facility.

In July 2021, anti-vaccinationists tried to force their way into a vaccination centre in Grodzisk Mazowiecki. When they failed to do so due to security measures, a brawl ensued in which two people were injured. The attackers shouted "Murderers, genocidaires!". There was an attempt to block a police car and an ambulance was attacked. Two people were arrested on charges of violating an officer's bodily integrity and insulting and making criminal threats against police officers. In August 2021, a group of 16 people attacked a 'vaccination bus' in Gdynia: it was surrounded and insults such as "murderers" and "children of Dr Mengele" were used

against the medical service. In the same month, members of the Nationwide Association of Vaccination Awareness STOP NOP disrupted a lactation picnic in Poznań organised at the Gynaecology and Obstetrics Hospital, as a vaccination centre was about to open there. A group of about 30 people with banners and megaphones attended the gathering, after which several people broke into the hospital and its buildings. The picnic was ended prematurely. A group of members of the Bydgoszcz Camaraderie of Compatriots forced their way into an orphanage in Aleksandrów Kujawski on 26 July, demanding that the vaccination of the centre's wards be stopped ("camaraderie" stood "in defence of the rights of a father" whose two children were in the centre).

Another category consists of cases of spontaneous individual violence – insults, threats and even beatings of people demanding to wear a mask: in April 2020 in a supermarket in Leszno, in August 2020 in front of a supermarket in Gdańsk and Bydgoszcz, in September 2020 a knife attack in a shop in Łódź, in October 2020 beating of a driver of the Warsaw Trams, in November 2020 in Łódź, in January 2021 assaults in a supermarket in Warsaw and a trolleybus in Gdynia, in March 2021 beating of a guard at Jasna Góra, in May 2021 beating of a bus driver of the Grodziec-Opole line, in June 2021 beating of a passenger on a bus in Bydgoszcz, in November 2021 beating of a postal agency employee in Zabrze, in December 2021 beating of a police officer and a municipal guard in Zamość and of a pharmacy employee in Zgorzelec.

The situation changed significantly in 2022. The end of pandemic restrictions reduced the dynamics of the anti-vaccine movement, with only the most determined core of activists remaining. At the same time, the outbreak of war in Ukraine led to the consolidation of the vast majority of the population on an anti-Russian platform. At the same time, no new violent outbreaks of social conflict comparable to the Constitutional Court ruling on abortion in October 2020 have emerged. These phenomena have weakened the potential for political extremism.

Extremism, however, did not disappear. Above all, inter-party antagonisms have not disappeared – even in the face of war. A manifestation of their persistence in 2022 is the (generally harmless) attacks on MPs' offices and their staff. The actions of extremists are generally limited to mutual confrontations and occasional acts of sabotage (or rather vandalism – such as the destruction of developer banners in Łódź in February 2022 or an ATM and ticket machine in Wrocław in December 2021). Sometimes, however, the association of extremism with the use of violence leads to apolitical crimes (the case of Antifa sympathiser Mikołaj J. from Inowrocław; neo-Nazi groups are also known to have links with organised crime).

The threat of extremism may increase significantly with the deterioration of the economic situation, especially if the reduction in living standards is associated with aid to Ukraine and the influx of refugees from that country. On this level, consolidation and mobilisation of the anti-system opposition is possible.

1.7. Cybersecurity threats

Cyber threats, including cyber terrorism, can today reach almost any organisational unit and any state or international organisation. Considering the threats of cyber-terrorist attacks, the highest vulnerability of the following systems can be identified:

- military systems,
- enterprise systems,
- systems belonging to critical infrastructure facilities – i.e. banking and finance, energy, telecommunications, water supply, transport, emergency response services, resources storing information important to state security.

The European Union Agency for Cyber Security – ENISA has produced the next version of its cyber security threat landscape report. The analysis covers the period between April 2020 and July 2021 and is based on open sources (media articles, expert opinions, incident analysis, reports), as well as interviews with members of ENISA's cyber threat working group. The report distinguishes the 9 most serious threats to ICT systems: ransomware (attacks using malware combined with data locking with ransom demands, attacks using malware to encrypt data with ransom demands, with the possibility of data exfiltration); malware (malicious software, e.g. stealing data or establishing permanent access of an adversary to infected workstations); theft of cryptocurrencies; threats related to e-mail (phishing, spearpshishing, exfiltration of correspondence); threats to data availability and integrity (e.g. DDoS attacks); misinformation/intentional misrepresentation; attacks on supply chains; other (human error, system misconfigurations, accidents affecting IT systems). The following trends were observed during the period analysed:

1. Ransomware is the most serious threat in the reported period.

2. The number of cyber-attacks (primarily ransomware) on critical infrastructure (primarily healthcare facilities, emergency services and pre-enterprises from transport and energy systems) is increasing.

3. Carrying out cyber attacks has become a service that is in demand, making this type of activity profitable, so the supply is growing and entities offering this type of service are being established. In addition, hackers are constantly improving their skills, using new or unusual programming languages.

4. Cryptocurrencies are becoming more widespread as a means of payment for illegal transactions related to ordering attacks or paying ransom to hackers; at the same time, cryptojacking attacks involving the use of an unwitting victim's computer to generate cryptocurrencies have increased. The number of cryptojacking infections reached a record high in the first quarter of 2021 compared to recent years.

5. COVID-19 pandemic-related threads are the predominant lure for email inbox attacks. In addition, an increase in non-malicious non-malicious incidents has been observed in 2020 and 2021, as the COVID-19 pandemic has become a proliferator of human error and system misconfigurations to the extent that the majority of breaches in 2020 were caused by such errors. Cyber attacks targeting supply chains can have catastrophic consequences, which is why ENISA has produced a separate report on this category of threats.

The key document depicting the state of cyber security in Poland is the *Report on the State of Cybersecurity of the Republic of Poland in 2021* prepared by the CSIRT GOV Computer Security Incident Response Team.

In 2021, the CSIRT GOV team recorded 762,175 reports of a potential ICT incident, of which 26,899 reports were classified as actual incidents.

Table 1. Number of reported incidents

YEAR	REPORTED INCIDENTS	ACTUAL INCIDENTS
2021	762.175	26.899
2020	246.107	23.309
2019	226.914	12.405
2018	31.865	6.236
2017	28.281	5.819

Source: own elaboration based on data from the 2020 and 2021 Reports.

The high number of reports in 2019-2021 is a result of the entry into force of the Act on the National Cyber Security System, making incident reporting mandatory, on the other hand, the global trend shows an annual increase in such incidents. An important factor was the start of the COVID-19 pandemic and the transition of many companies to a remote mode of operation. The highest number of actual incidents in 2020 (7,957) was registered in Q2 2020, coinciding with the start of the so-called lockdown. Although the pandemic restrictions are now over, many companies have permanently switched to a remote or hybrid mode of operation. In contrast, the threefold increase in the number of notifications in 2021 compared to 2020 is due to the high detection rate of incidents by the continuously updated ARAKIS GOV system.

When looking at the types of attacks, in 2021, the largest number of incidents were classified among the following three categories: "virus" (24,171 incidents), "vulnerability" (1,148), and "social engineering" (904). The "vulnerability" category is defined as: "ICT system weaknesses, configuration errors and lack of appropriate security policies related to updating and verifying correctly implemented ICT solutions" (Report... p. 17). Incidents from the "social engineering" category include phishing campaigns, impersonation and attacks from the scope of the so-called "social engineering", i.e. the use of various forms of manipulation in order to induce the user to perform a specific action. They are most often aimed at phishing for confidential information, infecting a computer with malware or inducing a user to perform a specific action, e.g. to disclose a login and password, make a bank transfer or grant access to an IT system. In this category, the highest number of incidents concerned impersonation of websites using the image of an entity, often aimed at phishing for funds or login data.

The most common form of phishing attacks were emails, whose senders impersonated the helpdesk, IT administrators, or used logos of public administration institutions or CI operators to further authenticate the correspondence. The message was formulated in such a way as to encourage the recipient to open the link contained in it and enter their e-mail login details. More often than not, the owner of the address was informed of a technical problem, an alarm, a full email inbox or a necessary update, in each of which cases it was necessary to log in to the email immediately. The aim of these campaigns was to obtain the credentials of public administration mailboxes (login, password) and take over the information contained therein, as well as to obtain the ability to send correspondence from them. The consequences could have been serious, as in the case of the hacker takeover of the email account of the head of the Prime Minister's Office, Michał Dworczyk, in June 2021.

In 2020, phishing attacks furthermore used elements of the visual identification system of courier companies (e.g. Poczta Polska, InPost) and telecommunications operators (e.g. Orange and Play); in 2021, the practice of impersonating the operator Play continued. Mail senders impersonated these operators and sent emails with information about an unpaid invoice, a pending shipment, the need to pay a surcharge for courier/postal services. The purpose of these attacks was to try to infect people with malware or obtain authorisation details for e-banking services and steal funds.

The COVID-19 outbreak, uncertainty, fear, and the need to quickly reorganise offices and switch to remote working were all factors used by cybercriminals. Attacks made use of an interactive map of the spread of the virus, fictitious emails from the World Health Organisation (WHO), messages with offers from companies offering personal protective equipment (masks, suits) or fictitious fund-raisers. The aim of such attacks was to infect the system or steal credentials. In 2021, the COVID-19 pandemic theme continued to be used, entities such as the Chief Sanitary Inspectorate and Orlen S.A. were used in phishing campaigns, and a phishing campaign involving the sending of messages between public authorities and CI operators also emerged. The mail came from the address vddoming@sct.gob.mx. and the aim was to steal login details.

In 2020, ICT incidents involving government offices ranked first among the most frequently attacked sectors, with 8,356 incidents.

In addition, incidents were recorded in ICT systems of critical infrastructure (2,626 incidents) and public institutions (2,518). Importantly, in 2020, there was a significant increase in the number of incidents at state offices (by 118%), critical infrastructure operators (by 283%) and services and the military (311%) compared to 2019. 2021 was characterised by an increased number of cyber attacks on CI operators' ICT systems (9,196 recorded incidents); thus, facilities, facilities and services that are essential to the functioning of the state and society became the most frequently attacked entities. In second place in terms of the number of attacks were the systems of institutions (7,203 reports), followed by government offices with 5,563 incidents. Other categories of entities were: ministries (3,056), services and military (1,237), others (644).

ARAKIS-GOV is an early warning system for threats occurring at the interface between the internal network and the Internet. In 2021, 1,758,708,908 flows were recorded in the ICT networks of entities participating in the ARAKIS 3.0 GOV project, which translated into 3,366,360 alarms generated by the system. Of the alarms recorded, 1,170,136 were of 'urgent' priority, i.e. requiring an immediate threat response from administrators, as they carried a high risk of a security breach.

The system allows the classification of alarms. In 2020, 32.35 % of all alarms were type 1 ("communication from malicious addresses") and resulted from attempts to establish communication with IP addresses or domains deemed malicious or likely to pose a threat. Most, 49.26 %, of the alarms were of type 2 ("scanning"); the highest number of such incidents was recorded in institutions defined as critical infrastructure (31.81 %). Type 3 alarms – "known attacks detected" – accounted for 4.94% of the notifications, type 4 – "undescribed attacks detected" – 10.04%, and the lowest values were recorded under type 5 ("internal infections", identified by unwanted communication with network elements covered by ARAKIS 3.0 GOV) and amounted to 0.21%.

Most flows were generated from the Russian Federation (25% of flows) and the USA (15% of flows); 12% of flows came from addresses belonging to Poland. This was followed by China, the UK, France and Germany with 5-7%.

The juxtaposition of cyber threats cannot ignore campaigns aimed at disinformation or deliberate misrepresentation. The digitisation of the press and the continued rise in popularity of social media mean that more and more people are getting their knowledge and information from the internet, which encourages disinformation campaigns and the spread of so-called fake news. Campaigns aimed at spreading fake news are part of hybrid attacks and support other threats, causing distrust and confusion, a decline in trust in democratic institutions and the disintegration of societies. The relatively high number of attacks using social engineering is worrying, as they most often target rank-and-file employees who have little knowledge of cyber security and are rarely trained in cyber attack methods and resilience. Raising the awareness of employees (primarily CI employees, as this sector is attacked most often) should be a training priority.

An important element in ensuring the security of an organisation's ICT systems and networks is also the constant updating of the software of elements inserted into the Internet. Exploitation of software vulnerabilities can have significant consequences, such as exfiltration of data from systems, ransomware infection or the use of a compromised system for further attacks. The Log4j library vulnerability, discovered in 2021, was identified as one of the most critical vulnerabilities in recent times, and the consequence of exploitation could be remote code execution with the privileges of the vulnerable application. Microsoft Exchange vulnerabilities, also identified in 2021, could have resulted in compromised servers being attacked.

It is advisable for IT administrators to continually improve their competence and knowledge of the software used in the organisation.

1.8. Characteristics of maritime threats

a. Terrorist threats to Polish citizens in international waters

History shows that Poles as crew members and passengers have already experienced terrorism. One should also not forget the unsuccessful hijacking attempts when Polish crews skilfully waited out or successfully repelled pirate aggression, including MV *ESL Australia* (20 May 2020) and MV *Port Gdynia* (21 December 2020). The most recent such incident took place on 13 December 2021 in the waters of the Gulf of Guinea, where seven crew members of the container ship MV *Tonsberg*, including a Polish national, were abducted. On 17 January 2022, the Pole and the accompanying crew members were released.

It is worth noting at this point that the latest International Maritime Bureau data shows a significant decrease in kidnappings for ransom (from 135 in 2020 to 57 in 2021). Nevertheless, according to the US Office of Naval Intelligence, there were seven incidents in the Gulf of Guinea and 11 in Southeast Asia from January to February 2022 alone.

b. Characteristics of threats in Polish maritime areas

Poland's security is also threatened by maritime terrorism. Both countering it and fighting its effects should not be taken less seriously than other direct threats. The globalisation process is intensifying the development of international maritime trade, forcing an increase in the number of sea routes and, above all, an increase in the frequency of ships carrying goods, which is threatened by maritime crime. The growing demand for energy increases the number of offshore platforms, whose facilities and installations are particularly vulnerable to acts of terrorism. A natural consequence of the rapid growth in passenger traffic, successive increases in turnover and port area, is a significant increase in the flow of people through the area. In addition, a specific feature of Polish seaports is their urban integration with urban agglomerations, which requires improved security procedures in the event of a security threat. Seaports, shipyards, state and local administration facilities and places of significant concentrations of people (railway stations, transport routes, shopping centres) all form a kind of whole. The location of port facilities of importance to the Republic of Poland is undoubtedly a factor facilitating the actions of potential terrorists.

Maritime critical infrastructure facilities may include ports, berths, gas terminals, passenger terminals, pipelines, drilling platforms, submarine cables and other hydrotechnical structures. It should be borne in mind that interference with their smooth functioning carries the spectre of a breakdown in the system for the transport of goods

vital to the functioning of the state or, for example, an ecological disaster and, as a result, economic losses. The undermining of the position of the Republic of Poland in the international arena should also not be forgotten. Hence, maritime critical infrastructure facilities require due attention, supervision and control.

The challenge in the area of Polish maritime security remains the development of a logistical infrastructure to enable the enhancement of *Host Nation Support* (HNS) capabilities and a protruding maritime presence of NATO in the Baltic Sea area and expanding the space for deepening NATO's cooperation with the EU.

Polish ports have great potential. Poland's favourable coastal location at the intersections of important transport corridors raises many challenges and opportunities, but also poses risks. An efficient, safe and attractive port infrastructure is essential for the competitiveness criterion of the facility. Dynamic development, expansion and modernisation concern not only loading quays, approach fairways, bases or even terminals, but also the improvement of road and rail access to individual facilities (motorways, railways, inland waterways). The *Strategy for the Sustainable Development of Transport up to 2030* emphasises the key role of seaports as nodal points influencing the efficiency and effectiveness of the national transport system, while the improvement of access to ports (both from land and sea) appears as one of the basic operational objectives of the above-mentioned *Strategy*. The modernisation and expansion of the maritime transport infrastructure (both linear and point-to-point) must meet national and EU standards, also in terms of protecting the marine and coastal environment. No less important, when we talk about maritime critical infrastructure, is the maritime communication system, which requires special care in the face of modern cyber threats. Investments centred around maritime ports of vital importance to the national economy are to help them all achieve the status of hubs, i.e. commodity ports.

The list of major seaports of fundamental importance to the national economy includes the port of Gdańsk, the port of Gdynia, the port of Szczecin and the port of Świnoujście. These facilities, together with their entire infrastructure, are located along the main European transport routes and in the EU's transport development strategy, forming important links in the *Trans-European Transport Networks* (TEN-T).

Due to the area it occupies and the diversity of its terrain, the Port of Gdansk is divided into two key areas: the inner port (extending along the Martwa Wisła River and the port channel) and the outer port (located on the waters of the Bay of Gdańsk). Gdansk is home to Poland's only offshore oil transshipment terminal and one of the largest terminals for transshipment of refined oil products. In 2021, it handled 17,898 million tonnes

of crude oil and fuels (more than 6% more than in the record year 2019). Importantly, in terms of diversification of energy raw materials, around two-thirds of Poland's oil supply is by sea, mostly from non-Eastern directions. The Naftoport liquid fuel transshipment depot has the capacity to receive – in an emergency situation – up to 60 million tonnes of oil per year.

In turn, the port of Gdynia is experiencing record growth in ro-ro cargo turnover, which is facilitated by its location in one of the TEN-T Baltic-Adriatic Core Network Corridors, whose extension is the Gdynia-Karlskrona Motorway of the Sea connecting Gdynia with Sweden. Further dynamic development of the port implies the need to build new deep-water terminals. By 2030, the construction of 4 new quays and the reconstruction of existing quays is planned, as well as the creation of a reserve for the construction of an LNG-FSRU terminal and the expansion of the liquid fuel handling terminal. The programme for the construction of a *Floating Storage Regasification Unit* (FSRU) assumes the location in the Bay of Gdańsk of a facility capable not only of unloading, in-process storage and regasification of LNG, but also to provide other additional services, e.g. enabling efficient gas transmission from the Tri-City area to the whole of Poland. This is another recent gas supply diversification project, in addition to the construction of the Baltic Pipe gas pipeline.

However, the gas port in Świnoujście, located on Poland's western coast, remains an important complex of strategic importance in this respect. The unquestionable advantage of the port in Świnoujście is its location – it is the westernmost port in Poland and the shortest route connecting Central and Eastern Europe with Scandinavia. An external port with an LNG terminal located in this area is a key investment from the point of view of Poland's energy security (diversification of gas supplies). The first commercial delivery of liquefied natural gas took place in June 2016. Since then, over 150 deliveries have been recorded, resulting in 27.2 million m3 of LNG reaching Poland by sea, while the total volume of LNG after the regasification process has exceeded 16 billion m3. The construction of 3 new berths is expected by 2030. In turn, in nearby Police, Grupa Azoty is continuing the construction of a petrochemical complex, which, together with the LNG terminal in Świnoujście and the transmission of gas through a submarine pipeline on the Norwegian-owned North Sea shelf, will provide a powerful facility for receiving and transporting raw materials by sea across the Baltic Sea. The Baltic Pipe pipeline will be an access gateway to the LNG terminal for Sweden and Denmark, allowing these Scandinavian countries to diversify their sources of gas supply from outside Europe.

Given our geopolitical location, the problem of maritime crime is extremely important. Developed coastal tourism and a gas or oil port make our country a potential

target for terrorists. A terrorist attack on these ports would allow terrorists to gain publicity. A particularly vulnerable segment is the critical infrastructure of the energy system. A successful attack on its facilities creates the possibility of driving up the price of energy raw materials as well as triggering a major ecological disaster through an oil or petroleum materials spill. The Świnoujście gas port ranks as an attractive target for a terrorist or diversionary attack due to the fact that it is a critical infrastructure of European significance, while at the same time the LNG transport system provides convenient conditions for a spectacular act of terror.

In addition to the previously known elements of offshore critical infrastructure, innovative offshore wind turbine complexes with associated infrastructure have emerged. The first phase of offshore wind energy development included the Baltic I, II and III offshore wind projects. The Baltic Sea has very good wind conditions, making it a stable source of renewable energy.

c. Terrorist threats in maritime areas

Peacetime threats

These threats are caused primarily by the activities of non-state actors, not supported by any state. These may be activities undertaken for ideological reasons or out of a desire to obtain financial gain. It should be borne in mind that, due to the specific nature of the functioning of the maritime economy, an act with criminal intent may be carried out in a manner justifying the suspicion of a terrorist act (Article 115 § 20 of the Criminal Code). In particular, this concerns the modus operandi of the perpetrators and the tools and technical means they use.

In the case of actions undertaken by individuals or groups without state support, threats to maritime critical infrastructure and navigation are determined by the financial resources, weaponry and equipment available to them and their ability to use it, as well as their organisational and information-gathering capabilities. It is possible for such actors to acquire improvised explosive devices, small arms and civilian-marketed vehicles and vessels and civilian-accessible underwater work equipment or unmanned aerial vehicles. A significant barrier for underwater equipment, including unmanned underwater vehicles, is the cost of acquisition.

Therefore, it is possible for non-state actors to carry out attacks on targets to which perpetrators have the easiest access. With Polish maritime areas in mind, these are primarily land-based facilities (ports) and passenger and recreational vessels. Another

situation is an insider attack – i.e. a threat caused by a person employed at a given facility, acting alone or in agreement with others (voluntarily or under coercion).

The perpetrators of such attacks may be guided by ideological motives, in particular related to Poland's foreign policy. Actions by radical environmentalist organisations are also possible, in particular attacks on the extraction and transport of energy resources. There may also be incidents involving attempts by perpetrators to infiltrate into or leave (escape) Poland.

Several possible scenarios for an attack on shipping as well as on maritime critical infrastructure can be identified in this context.

The first is the perpetration of a traditional attack using an explosive device, firearms or other dangerous tools within a port facility. This can take the form of a bomb attack, an "active shooter" attack or hostage-taking; other than where it occurs, it will be no different from other such incidents at critical infrastructure facilities. All that needs to be borne in mind is the specificity of the individual facility, due to the goods handled in the ports, including dangerous cargoes, and the possibility of the perpetrator getting on board a vessel moored in the port.

The second is to carry out an attack – either a bombing or hostage-taking attack, or an attack with a dangerous instrument on board a vessel or on board an offshore installation (e.g. an oil rig). In particular, the scenario of taking control of a vessel in order to fulfil the demands made by the perpetrators (political concessions, payment of a ransom) is likely. In Polish maritime areas possible targets of such attacks may be passenger vessels (especially sea ferries) and outside the Baltic Sea – commercial vessels in areas threatened by criminal groups.

A third possible scenario is to attack port facilities or vessels using unmanned aerial vehicles. These can be used in particular to carry small explosive devices. It is likely that commercially available devices will be used, which translates into ease of use but relatively little damage (see Security of critical infrastructure against threats from unmanned platforms, "PTBN Report", Volume II.2)

The fourth scenario is the use of a watercraft as a means of terrorist attack. Specifically, this could be a readily available watercraft (e.g. a speedboat) carrying an explosive device. The attack could be suicidal or carried out with the help of a remotely operated or self-propelled craft. Given the availability of technical means, it is possible (although less likely) to use a purchased or self-constructed unmanned underwater

vehicle. In addition, a surface craft allows for the placement of a heavier explosive charge on it and therefore a greater ability to strike.

It should be noted that terrorist actions targeting port infrastructure or shipping are relatively rare. The *Global Terrorism Database* contains information on 394 attacks on maritime targets between 1971 and 2019, of which only 33 in Europe and North America. This is probably influenced by the degree of difficulty associated with attacks on maritime targets and ports, as well as the possible influence of the phenomenon of *sea blindness*, i.e. a failure to see the importance of the maritime economy in the public mind. In comparison, an attack on a target such as an international airport is easier for terrorists (as evidenced by the higher frequency of attacks) as well as more media-savvy. The much larger share of passenger traffic in air transport is also significant, so there are more potential witnesses as well as victims of such an attack.

Threats in times of crisis implemented as part of hybrid threats

Hybrid threats have been defined for the purposes of this study as the actions of state actors undertaken to achieve their political, economic and military objectives through the destabilisation of the security environment achieved through the combined overt and covert use of various means of leverage, including military, economic and information, also using or pretending to use the activities of other actors, including non-state actors. The hybridity of the threat means that different means are likely to be used, from different domains (including political, military, economic and social) and in varying degrees of intensity. The most commonly used hybrid tools in recent years include disinformation activities, cyber attacks, interference in electoral processes, economic blackmail and dependence on the supply of raw materials.

In the context of the security of Polish maritime areas and critical infrastructure, the most likely hybrid threat should be considered to be the actions of Russia seeking to influence Poland and other Central European states. The likely aim will be to demonstrate the ineffectiveness of Polish state bodies to counter and respond to threats and, in turn, to complicate Poland's international situation, weaken allied solidarity and force compliance with Russian political, economic and military demands. Situations created in this way will also be aimed at demonstrating Russia's alleged effectiveness and proficiency as an actor capable of ensuring security instead of Poland and organisations such as NATO and the EU, or at least forcing negotiations with Russia. This threat is particularly likely in the context of Russian aggression against Ukraine.

Scenarios for possible crises must take into account Poland's existing and possible vulnerabilities, including in the maritime domain.

The use of hybrid measures in the maritime domain can take the form of one of several scenarios.

1. Questioning of Poland's ability to ensure safety in the exclusive economic zone. This scenario assumes the creation of a situation in which the secutity of navigation, security of pipelines and submarine cables and other installations – e.g. energy and mining installations – located in the exclusive economic zone of the Republic of Poland is threatened in the form of an actual incident, e.g. a terrorist or sabotage event or a threat of such an event. This would be accompanied by an intensive information campaign to, for example, convince the public of the alleged or real consequences of, for example, a maritime disaster. It should be noted that this scenario does not assume a direct impact on Poland, but only a proof of its ineffectiveness. For example, the created threat could harm, for example, commercial shipping serving Russian ports. A variant of this scenario is to create a crisis situation in such a way as to suggest that there was a threat to shipping and installations in other areas of the Baltic, but originating in areas controlled by Poland, e.g. alleged sabotage of a gas pipeline outside the Polish exclusive economic zone by a vessel that had previously called at a Polish port. It should be noted that this scenario, although outside Polish maritime areas, materialised in the form of the blow-up of the Nord Stream and Nord Stream II pipelines in September 2022.

   In these scenarios, the message would be directed both to the Polish public and to a wider audience, including the societies of other European states. Russia's actions would lead to the creation of conditions allowing for extensive activity by Russian naval forces under the guise of an "anti-terrorist operation".

2. Blocking Poland's ability to use maritime transport. This scenario already assumes direct action to hinder or prevent commercial shipping in Polish maritime areas and water bodies strategically important to Poland. In particular, this concerns the import of energy raw materials and the transport of other cargoes important for the Polish economy. This can be achieved through both kinetic and non-kinetic actions. Blocking or impeding maritime transport means increasing Poland's vulnerability to other forms of pressure, including economic pressure. It is also possible, as in the previous scenario, to bring about a situation in which Russia launches a unilateral operation in the Baltic area under the guise of "protecting the safety of shipping".

3. Attack on infrastructure, including critical infrastructure located in maritime areas. This scenario assumes actions against installations located in Polish territorial waters or in the exclusive economic zone, such as mining platforms, offshore wind farms, pipelines and submarine cables. The aim of the perpetrators would be to prevent their use in order to increase Poland's vulnerability to other forms of pressure (especially economic pressure), as well as to create fear of economic crisis or ecological disaster. Actions targeting floating natural gas reloading facilities (FSRU – such a facility is to be located in the Gulf of Gdańsk) fall into this category.

4. An attack on coastal facilities, including critical infrastructure facilities. These could be installations directly related to the maritime economy, such as ports, or facilities close to the coast, such as industrial or energy installations.

In each of these scenarios, the possibility of using a wide range of means must be considered. These may include measures typical of protest movements, terrorist organisations or enemy special forces. It is also possible to deliberately attack vessels, facilities, installations used by state services. This should take into account the risk of using vessels as tools of attack or transport.

In particular, the likely methods of operation include:

- blockades in the form of passive resistance posing as protests by social and environmental organisations, both at sea (using civilian pleasure craft) and on land and in the air, to restrict the freedom of navigation and the operation of transhipment facilities;
- acts of penetration of persons into installations or on board vessels, posing as acts of protest to demonstrate the vulnerability of penetrated targets to acts of diversion;
- persistent harassment of vessels and shore installations by unmanned aircraft or manned and unmanned vessels (including so-called "hull pushing");
- faking or intentionally causing a breakdown of a vessel, e.g. self-sinking of a merchant vessel in order to block a shipping route;
- staging a collision at sea between a manned or unmanned vessel and another vessel or an oil platform;
- placing an explosive device on the premises of a shore facility or vessel by carrying it or bringing it on board a vehicle;
- destroying and damaging navigational aids and technical observation means, including those belonging to government services;
- the use of underwater diversion means to place an explosive device on the underwater part of the hull of a ship, an oil platform, a wind turbine or to disrupt another

installation laid on the seabed e.g. a pipeline or submarine cable. This can be done using divers and/or unmanned vehicles, including single-use vehicles;
- a fire attack using means of destruction such as drones or missile weapons to attack ships or other objects, e.g. harbour or coastal targets. Their carriers may be vessels in particular;
- an attack with the intent to enter an object with the purpose of destroying or gaining control of a vessel or other target (e.g. an oil rig), including to create a hostage situation;
- triggering an environmental catastrophe by releasing chemicals (oil from tankers, sarin at the bottom of the Gulf of Gdańsk) due to sabotage.
- cyber and information attacks, including those aimed at disrupting navigation and nautical support systems (such as GPS and AIS), as well as control systems for vessels (including drones) and the work of shore installations.

Wartime threats

In the event of an open armed conflict, including as a result of an escalation of hybrid activities, including a cyber attack, both shipping and infrastructure may become the target of attacks carried out by adversary armed forces, including surface forces, submarine forces, air forces, missile forces, special forces subdivisions and land forces, including naval landing craft. Countering them therefore requires the use of the Navy's own conventional forces, primarily its own forces and assets. In addition to them, forces and means intended for counter-terrorist activities, especially in the area of detection and combating diversionary and reconnaissance groups, may also play an important role, especially in the area of counter-diversionary activities. In doing so, it should be noted that, by their very nature, adversary special forces can be covertly deployed and prepared for use before the start of hostilities and used in the first moments of an armed conflict.

1.9. Perception of terrorist threat in the EU and Poland

a. Terrorist threat perception in the EU

On 24 January 2023, the Polish Association for National Security participated in a survey of members of the EU PSA (the European Commission's counter-terrorism initiative for the protection of public spaces and critical infrastructure – DG HOME) and representatives of the EU institutions supporting this project with the participation

of strategic partners from the USA[4]. The survey was carried out on the basis of a standardised survey questionnaire with a sample of 55 people. Respondents represented: the EU PSA (83.64%), the EU institutions supporting the above initiative (10.91%) and the EU PSA project's strategic partner, the United States (5.45%).

Terrorist threat experts involved in the EU PSA or supporting this European Commission initiative cited critical infrastructure (63.63% of all responses), public transport systems (60%) and symbolic tourist sites (34.55%) as the most potential targets for a terrorist attack within the EU.

When it comes to the tools that today pose the greatest challenge to the services, authorities and institutions tasked with ensuring the physical security of persons and objects that could be the target of terrorist attacks in the EU, respondents cited unmanned vehicles (air, land, water) with 49.09% of responses.

More than 80 per cent of respondents believe that terrorist activities will be used as part of hybrid threat scenarios undertaken on EU territory by a foreign state in the 3-year perspective.

In terms of the types of facilities that will have the highest level of terrorist threat within the EU in a three-year timeframe, respondents most frequently indicated: critical infrastructure in the energy sector (total of all indications: 70.91%), the public transport system (58.19%) and the seats of constitutional state bodies and places of worship (27.22% each).

Respondents indicated that the CI system that should be prioritised in the 3-year perspective for building resilience to hybrid threats is the energy system.

When asked what area of counter-terrorist activity the EU needs to prioritise today, experts' opinions were divided, with the three categories (detecting and blocking terrorist propaganda and instructional material published online; countering the financing of terrorism; and educational initiatives to build a culture of security for facilities vulnerable to terrorist attacks) receiving identical numbers of indications at 21.82% each.

The following were identified by respondents as the undertakings most likely to increase the level of resilience to terrorist attacks at protected facilities: standardisation

[4] Detailed survey data with commentary will be published in: Karolina Wojtasik, Results of a study on the perception of terrorist threats among EU PSA participants, Analizy PTBN, No. 1 (2023), Warsaw 2023.

of physical security (52.72% of all indications), development of counter-terrorism prevention initiatives as part of the facility's security culture (54.54%) and use of security control tests by external oversight bodies (47.28%). 45.45% of respondents believe that the perpetrators of current attacks on critical infrastructure systems are cyber criminals linked to a state actor.

Other aspects of terrorist threats in EU countries are presented in the unpublished results of research conducted by Jarosław Cymerski, PhD, on the directions of changes in the functioning of formations which protect persons and objects subject to statutory protection. In the face of a dynamically changing threat environment, a question was posed concerning the formation of the level of terrorist threat in Europe. The surveyed group of experts responding in the form of an expert interview drew attention to a number of aspects of the volatility of the environment in question, with an emphasis on the increase in the level of terrorist threats in the Member States. 77% of respondents considered that an increase in the level of terrorist threats should be expected and only 8% of respondents indicated a decrease in the level of terrorist threats in EU countries.

With regard to the source of terrorist attacks, the largest group, 54% of respondents, believes that the threats will be caused by uncontrolled immigration to the European Union, the ongoing process of political and economic destabilisation in EU countries and state conflicts (which appears to be in line with the reality of the current situation in European countries as a consequence, inter alia, of the Ukrainian-Russian war). 15% of respondents answered that the likelihood of attacks inspired by the Russian Federation should be taken into account. The same group pointed to the likelihood of attacks carried out by separatist organisations. 8% of respondents each said that the likelihood of attacks carried out by extreme left-wing organisations and supporters of "white supremacy" should be reckoned with.

Threats to critical infrastructure posed by cyber-attacks are also part of the nature of the war being waged – 23% of respondents said that the likelihood of threats caused by cyber-attacks on critical infrastructure systems in EU countries should be expected. In turn, 15% foresee the possibility of threats caused by weapons of mass destruction. It can therefore be assumed that the perception of terrorist threats has been confirmed in a number of studies conducted by both security institutions and individual researchers.

b. Perception of terrorist threat in Poland – participants in the AT system

In 2022, the scientific periodical "Terrorism – studies, analyses, prevention", published by the ABW, published the results of the first survey in Poland on the perception of the phenomenon of terrorism and the predicted, most likely directions of development of this type of threat in the Republic of Poland. The respondents were representatives of services and institutions belonging to the anti-terrorist community of the Republic of Poland (76%) and representatives of the academic community, as well as analysts involved in terrorism studies. Here are the most relevant issues from the point of view of assessing the terrorist threat in Poland:

- According to 53.19% of respondents, ISIS (Daesh) is the organisation that poses the greatest threat to the security of the Republic of Poland, the special services of the Russian Federation came second with a score of 17.02%, followed by the Atomwaffen network in third place with a score of 14.89%.
- Respondents identified the following types of facilities as the most likely target for terrorist attacks in the EU: critical infrastructure – 39.36%, public open spaces 32.98%, – tourism infrastructure and sports facilities 14.89%.
- According to 47.87% of respondents, between 2022 and 2025 Poland will be an attractive country for international terrorists planning their activities in the EU, while 19.15% of respondents held the opposite view.
- In the opinion of 90.43% of respondents, terrorist activity carried out as part of hybrid actions by third countries in Poland should be expected between 2022 and 2025.
- Among the facilities located in the Republic of Poland, whose level of threat of a terrorist attack in 2022-2025 was rated as the highest by respondents, respondents indicated, among others, critical energy infrastructure facilities – 36.17%, the public transport system – 34.04%, military bases used as part of NATO's eastern flank – 19.15%.

1.10. Prospects for the development of terrorist threats on Polish territory

The socio-political situation has become unpredictable in recent years, so any attempt at forecasting is fraught with risk. The likelihood of "black swans" – unexpected events that change the dynamics of processes – is increasing. Assuming, however, that such events do not occur in the near future, it is possible to attempt to delineate risk trends on the basis of long-term trends.

For threats of internal origin, one can rely on the theory that political violence (including terrorist violence) is the result of a radicalisation process. While individual radicalisation is difficult to diagnose and detect, mass radicalisation takes the form of social phenomena such as protest movements. In the case of Poland, this can include:

- deepening political and ideological polarisation,
- increased aversion to immigrants,
- social tensions (if the economic situation worsens),
- radicalisation of the environmental movement,
- radicalisation of supporters of conspiracy theories (e.g. the Great Reset).

Most likely are individual, largely spontaneous acts of over-power, targeting primarily symbols and property (e.g. buildings), less likely people (either recognisable figures or random individuals belonging to a 'hostile' group). Acts of sabotage against economic infrastructure are also possible – especially in the case of radical environmentalists or supporters of conspiracy theories. As protest movements become more radicalised, groups preparing for violence (physical training, especially martial arts) and using violence in an organised manner (although rather limited to street clashes) will develop. It cannot be ruled out that on the margins of these movements independently radicalised individuals will attempt to carry out deadly terrorist attacks.

Threats of external origin may come from two sources. The first is immigration, which has intensified in recent years and which may potentially give rise to a resurgence of jihadist terrorism, but also to an intensification of Polish-Ukrainian historical resentments (backlash); the transfer of foreign national antagonisms (e.g. Turkish-Kurdish) to Poland is also possible. The second source is the interference of state actors (basically the Russian Federation); due to the weak social base, it is likely to take the form of camouflaged inspiration of other (above-mentioned) movements.

2. Elements of the anti-terrorist system of the Republic of Poland

2.1. The cybersecurity system of the Republic of Poland and the threats of a terrorist nature

a. EU and national legal conditions on cyber-terrorism

There is no uniform definition of cyber-terrorism in Polish or European legislation. It can generally be assumed that cyber-terrorist attacks fall into two categories. The first encompasses actions aimed at destroying a selected target or destabilising a system resulting in the physical destruction of e.g. a country's critical infrastructure facilities. The second encompasses the use of information and communication technologies, e.g. for DoS and DDoS or virus attacks, as well as unauthorised access to government or corporate systems (important information, ICT and telecommunications nodes), aimed at causing a specific effect or response. It is thus an unlawful attack or threat of attack on computers, networks or information systems, resulting from the actions of non-state actors or foreign secret services, with the aim of intimidating or coercing a concession from the government or creating uncertainty and fear in the public.

Another issue is the qualification of acts involving the use of virtual space for activities leading to radicalisation (spreading terrorist propaganda), recruitment into organisations or communication of supporters and members of a terrorist group. Legislative work is underway in this area both at the level of the EU and at the level of individual Member States with a view to constantly updating regulations in the face of increasingly sophisticated methods of terrorist activity.

EU documents on cyber-terrorism

The EU is developing policy guidelines and recommendations in the field of cyberspace, such as:

- *Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cyber incidents and crises*. It sets out the objectives and modalities for cooperation between Member States and EU institutions in responding to large-scale cross-border cyber incidents or crises. It explains how existing crisis management mechanisms can be fully utilised by existing cyber-security actors at EU level.
- *Commission Recommendation (EU) 2021/1086 of 23 June 2021 on the creation of a Joint Cyber Unit*. The document is an important step towards the completion of the European Cyber Crisis Management Framework. It is a concrete outcome of the EU Cyber Security Strategy and the EU Security Union Strategy, contributing to a secure digital economy and society. The Joint Cyber Unit will act as a platform to ensure a coordinated EU response to large-scale cyber incidents and cyber crises, as well as offering assistance in dealing with the consequences of these attacks. To achieve this, the Recommendation also defines the procedure, milestones and timeline that Member States and relevant EU institutions, bodies and agencies should follow with a view to setting up and developing the platform.

On 16 December 2020, the European Commission unveiled a new cyber security package, which included, among others, an EU Cyber Security Strategy focused on building common capabilities to respond to major cyber attacks and to work with partners to ensure international security and stability in cyberspace and to strengthen Europe's resilience to cybercrime. The strategy consists of initiatives in the areas of (1) resilience, technological sovereignty and leadership, (2) building operational capabilities to prevent, deter and respond to cyber incidents, (3) developing a global and open cyberspace by enhancing international cooperation.

In addition, the Commission has put forward legislative proposals on both cyber resilience and physical resilience of critical entities and critical networks:

A *Directive on the security of network and information systems* (NIS 2 Directive) and a *Directive of the European Parliament and of the Council on the resilience of critical entities*. The proposed regulations aim to increase the level of security of critical infrastructure entities of the European Union Member States and their resilience from cyber

attacks and cyber terrorism to crime or natural disasters. The regulatory proposal takes the form of a directive to allow for national specificities, sectoral interdependencies and cross-border interdependencies. The new EU framework for the resilience of critical infrastructure includes, inter alia, a description of the obligations of competent authorities, including the identification of critical entities.

In addition, on 22 March 2021, the Council of the EU adopted conclusions on a cyber security strategy, emphasising that cyber security is central to building a resilient, green and digital Europe, and that a key objective of EU action in this area is to strive for strategic autonomy while maintaining an open economy by enhancing the ability to make autonomous choices in the area of cyber security. Until 18 May 2022, the Council extended the sanctions framework for cyber attacks that threaten the EU or its Member States. This allows the EU to continue to impose targeted sanctions on individuals or entities involved in cyber attacks that cause significant damage and are an external threat to the EU or its Member States. Sanctions can also be used in response to cyber attacks against third countries or international organisations when deemed necessary to achieve common foreign and security policy objectives.

Another aspect of cyber security is addressed by Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online. The primary objective of the provisions included in the indicated regulation is to reduce the use of networks for radicalisation, recruitment, incitement to violence and to enable the rapid removal of terrorist content, as well as to create a common legal framework for all Member States by introducing a mechanism for issuing and reviewing orders to remove or prevent access to terrorist content. The provisions apply to hosting providers offering services in the EU, regardless of where the entity's headquarters are located. Competent authorities in Member States will have the power to order service providers to remove terrorist content or block access to content within one hour. Full implementation of the provisions of the indicated regulation took place in Poland on 7 June 2022.

National documents and regulations relating to cyber-terrorism

At the strategic level in the Republic of Poland, cyber security is addressed in the following documents:

- The *Polish Cyber Security Strategy 2019-2024* was approved by the Council of Ministers on 22 October 2019 (with effect from 31 October 2019), replacing the National Cyber Security Policy Framework 2017-2022.

- The *Cyber Security Doctrine of the Republic of Poland,* which is only a conceptual document and has no legal force, was developed in 2015 at the National Security Bureau and approved by the National Security Council. It is an executive document in relation to the *National Security Strategy of the Republic of Poland* defining the objectives in the field of cyber security, as well as the recommendations that should be implemented in the construction of the state's cyber security system. It contains postulates such as: the introduction of specific formal and legal solutions, the creation of cooperation mechanisms between the public and private sectors, increased investment in national cyber security solutions and the use of civic potential for the protection of the state in cyberspace.
- *National Security Strategy*. The main objective identified in the NSS for the area of cyber security is to increase the level of resilience to threats and enhance the level of protection of information in the public, military and private sectors, and to promote knowledge and good practice to enable citizens to better protect their information assets.

In the Polish regulatory system, the primary area of counter-terrorism is criminal law and administrative law, in which legal mechanisms have been included to prevent cyber-terrorism, as well as to combat its effects. There is no single document that regulates the area of cyber attacks, and the provisions on cyber terrorism are regulated sectorally or fragmentarily, according to the tasks of different entities, as a result of which they remain scattered in many legal acts.

The *Act on anti-terrorist activities* does not directly refer to combating the phenomenon of cyber-terrorism and cyberspace protection, however, within the framework of the articles amending other laws, it included provisions on the ABW's responsibility to identify, prevent and combat threats in cyberspace. In addition, the Act amended the *Act on the ABW and the AW* by extending the tasks of the ABW with a provision indicating specific solutions for the protection of cyberspace within its statutory activities contained in Article 5(1) of the Act. The ABW became competent in the area of identification of threats threatening the security of information and communication systems of public administration bodies or information and communication network systems included in the uniform list of objects, installations, devices and services included in the critical infrastructure (referred to in art. 5b sec. 7 p. 1 of the *Act of 26 April 2007 on crisis management*), as well as information and communication systems of owners and holders of objects, installations or devices of critical infrastructure, which are significant from the point of view of continuity of the state's functioning. This provision indicated, for the first time in the Polish legal system, an entity responsible for a specific scope of the state's ICT security.

Accordingly, Article 32a of the *Act on the ABW and the AW* entrusts the ABW with conducting security assessments of designated ICT systems or ICT networks (so-called penetration tests) and with analysing events that breach the security of ICT systems resulting in issuing recommendations to the entities referred to in Article 32d(3) aimed at improving the security level of ICT systems. The issue in question is regulated in detail in the *Ordinance of the Council of Ministers of 19 July 2016 on conducting security assessments related to the prevention of terrorist incidents*. The quoted executive act, in addition to defining the conditions and procedure for conducting a security assessment, as well as the activities necessary for conducting a security assessment, sets out a model agreement containing the framework conditions for conducting the assessment.

In order to prevent, detect, counteract and prosecute terrorist offences, the possibility of applying the so-called "accessibility blockade" was introduced by virtue of Article 32c of the *Act on the ABW and the AW*. The District Court, upon a written application of the Head of the ABW submitted after obtaining a written consent of the Public Prosecutor General, by way of a ruling may order the blocking of accessibility in the ICT system by the service provider providing electronic services.

Another extremely important issue is the regulation at statutory level of the possibility of a terrorist event targeting ICT systems that are important for the functioning of the state. In this respect, the *Act on anti-terrorist activities* (Article 15) introduced a universally applicable, uniform and NATO-adapted four-level system of alert levels, including alert levels concerning the cyberspace of the Republic of Poland (CRP alert levels). In addition, a mechanism was introduced, based on Article 17 of the Act, for the Head of the ABW to appoint a coordination staff in the event of the introduction of an alert level concerning events on the territory of the Republic of Poland and a CRP alert level.

The *Act on the national cyber-security system* (hereinafter: KSC), fulfilling the obligation to implement Directive 2016/1148 into the Polish legal order, aims to comprehensively regulate the area of cyber-security by defining the organisation and functioning of the national cyber-security system, the manner of supervision and control with regard to the application of the provisions of the Act and the scope and procedure for the establishment of the Cyber-Security Strategy of the Republic of Poland.

b. The role and tasks of those responsible for countering cyber-terrorism

Ensuring the security of the cyberspace of the Republic of Poland, with particular emphasis on the threat of cyber-terrorism in the broadest sense, should take place

both through the development of defensive and offensive capabilities. Nevertheless, it is also important to cooperate and coordinate the activities of state institutions and services with private sector entities (e.g. telecommunications, energy, finance, transport). There is no doubt that identifying cyber-terrorism, as well as crimes committed in cyberspace, preventing them and prosecuting the perpetrators requires a systemic approach in legal, organisational and technical terms.

The main links in the system are the so-called CERTs (Computer Emergency Response Teams) set up by businesses and other network breach teams. These include:

- **CSIRT (Computer Security Incident Response Team) GOV**, which operates within the ICT Security Department of the ABW and has jurisdiction over incidents related to terrorist incidents as referred to in Article 2 p. 7 of the *Act on anti-terrorist activities* of 10 June 2016.
- **CSIRT NASK** run by the Research and Academic Computer Network – National Research Institute. CSIRT NASK together with CSIRT GOV operate the ARAKIS-GOV system, which is an early warning system for threats on the Internet.
- **CSIRT MON** run by the Ministry of Defence is competent for incidents related to events of a terrorist nature. CSIRT MON is obliged to coordinate incidents reported by entities subordinate to or supervised by the Minister of Defence.

Incidents (including incidents with the potential for cyber-terrorism) affecting the operations of key service operators (major incidents) and digital service providers (significant incidents), as well as incidents in public entities and, above all, critical incidents resulting in significant damage to public security or order, international interests, economic interests, the operation of public institutions, civil rights and freedoms or human life and health are reported to the above CSIRT teams.

Each of the CSIRT teams is responsible for the coordination of incidents reported by entities assigned under the Act. Under the KSC, in the event of a serious incident or cyber attack requiring cooperation at the national level, it is possible to coordinate the activities of all CSIRTs in Poland (also sectoral cyber security teams).

CSIRT teams have the ability to examine devices or software to identify vulnerabilities that may be used to threaten the integrity, confidentiality, accountability, authenticity or availability of processed data affecting public safety or a vital national security interest. Based on these examinations, CSIRTs can make recommendations to remediate vulnerabilities in devices or software used by national cyber security system entities.

The Critical Incidents Team is an auxiliary body in matters of handling critical incidents reported to CSIRT MON, CSIRT NASK or CSIRT GOV and coordinating activities undertaken by these teams and the Government Centre for Security (RCB) (Article 36 of the KSC Act). It is composed of representatives of CSIRT MON, CSIRT NASK, the Head of the ABW performing tasks within CSIRT GOV and the RCB.

The announced amendment to the KSC Act introduces new solutions concerning, among other things:

- the tasks of the SOC (Security Operations Centre) teams acting for the key service operators (the concept of operational SOC security centres has been introduced into the KSC, which will replace the previous structures responsible for the cyber security of the key service operator),
- the ISAC Cyber Security Information Sharing and Analysis Centre, a centre for the sharing and analysis of information on vulnerabilities, threats and incidents that operates to support KSC entities,
- the creation of sectoral CSIRT teams operating at sector or sub-sector level to support key service operators in handling incidents (**CSIRT Telco** – Computer Security Incident Response Team operating for electronic communications entrepreneurs).

A Government Plenipotentiary for Cyber Security and a Cyber Security College have been established in order to coordinate cooperation between the actors of the national cyber security system more effectively and to respond more efficiently to emerging new threats.

The Government Plenipotentiary for Cyber Security is responsible for coordinating at the national level the implementation of cyber security tasks in the Republic of Poland. His remit also includes analysing and evaluating the performance of the KSC on the basis of aggregated data and indicators developed with the participation of state administration bodies, competent authorities and CSIRT teams, as well as supervising the KSC risk management process using aggregated data and indicators developed with the participation of competent authorities and CSIRT teams.

The Cyber Security College is a consultative and advisory body for planning, supervising and coordinating the activities of CSIRTs, sectoral cyber security teams and competent authorities. The College is headed by the Prime Minister. Upon receiving a recommendation from the College, the Prime Minister may issue binding guidelines to coordinate cyber security activities.

Other entities involved in preventing and combating various types of crimes and incidents in cyberspace that may be classified as cyber-terrorism and dealing with the protection of national cryptologic technologies include the KGP Cybercrime Bureau (on the basis of which the Central Cybercrime Bureau is being established from January 2022) and the National Cyber Security Centre.

The existing **Bureau for Combating Cybercrime** performs tasks related to creating conditions for effective detection of perpetrators of crimes committed with the use of modern information and communication technologies. The tasks of the Bureau include, in particular, supervising, coordinating and supporting actions aimed at combating cybercrime carried out by voivodeship (and capital) police headquarters in the field of operational and exploratory activities and cooperating with the Central Bureau of Investigation of the Police in this respect. The newly-established Central Bureau for Combating Cybercrime (CBZC), in accordance with the Act of 17 December 2021, constitutes an organisational unit of the Police competent in matters of combating cybercrime, responsible for the implementation, throughout the country, of tasks in the field of recognition, prevention and combating of crimes committed with the use of information and communication technologies and supporting, to the necessary extent, other organisational units of the Police in the recognition, prevention and combating of crimes. Officers of the CBZC will be fully entitled to conduct operational-investigative and administrative activities resulting from the Act on the Police.

The National Cyber Security Centre was established on 1 June 2013 by the Ministry of Defence under Order No. 10/MON of 29 April 2013 as the National Cryptology Centre. As of 5 March 2019, it bears its current name. Its tasks include monitoring, analysis and proactive response to incidents that breach the security of the network and its users. To this end, among other things, it conducts research into methods of detecting cyber incidents (including for malware analysis) and protecting information (including cryptography).

2.2. Anti-terrorist security of the maritime areas of the Republic of Poland

The safety of Polish maritime areas is defined by the provisions of several legal acts. In particular, these are the following acts: *of 21 March 1991 on maritime areas of the Republic of Poland and maritime administration, of 18 August 2011 on maritime safety, of 4 September 2008 on the protection of shipping and sea ports, of 12 October 1990 on the*

protection of the state border, of 12 October 1990 on the Border Guard, of 10 June 2016 on anti-terrorist activities.

The provisions of these laws regulate the functioning and powers of a number of state bodies with both diverse competences and resources. The differentiation also relates to the possible areas of action of the individual services. While the provisions on maritime areas and the scope of action of the Border Guard allow for actions within the competences of these authorities on the area of internal waters, territorial waters and the exclusive economic zone, the *Act on anti-terrorist activities* narrows the scope of actions to the Polish SAR (Search and Rescue) zone of responsibility, which is not identical to the exclusive economic zone and includes other areas of the southern Baltic Sea.

In the case of civilian institutions, the authorisations of the government administration related to the use of the sea are held by **local maritime administrations**. Under the Maritime Security Act, the director of the competent maritime office has the right to issue binding orders to ships (e.g. to take a certain position or prohibit departure from a port) in order to prevent or limit a threat to maritime and port security. The **Maritime Search and Rescue Service**, on the other hand, is the service competent for the protection of human life at sea and has trained personnel and equipment in the form of rescue vessels and shore resources for this purpose. The **Border Guard** is authorised by law to supervise the operation of Polish maritime areas and the observance by ships of the regulations in force in these areas and has the authority to stop and control vessels within the limits set by the provisions of the Acts and to use coercive measures, including firearms, also against vessels. It has a specialised marine detachment (**Maritime Border Guard Regional Unit**) equipped with vessels of various types, including patrol vessels of the SKS-40 type, and it also includes a special subdivision prepared to operate on board vessels. This service also includes an aviation component equipped with helicopters and patrol aircraft. Finally, the **Police** and other services perform their statutory tasks on the coast and Polish maritime areas (especially internal waters and territorial sea), noting that their scope is dependent on equipment resources. The police have limited capabilities in this respect, having only motor boats with low maritime capacity at their disposal. In addition, it has a counter-terrorist service and some subdivisions are prepared to operate in the water environment (including the sea).

In turn, the capability of the Polish Armed Forces to operate in the maritime environment is concentrated primarily in two tactical compounds of the **Navy**: **3rd Flotilla of Ships** and **8th Flotilla of Coastal Defence.** These resources are complemented by the forces

of other components (including the **Special Forces**) and aviation (especially naval aviation: the **Naval Aviation Brigade**). The Armed Forces have capabilities in the area of reconnaissance and observation of the situation in Polish sea areas, missile defence against surface targets, anti-submarine warfare and mine threat reconnaissance and neutralisation. Detailed capabilities depend on the capabilities of naval, coastal and air forces. The Armed Forces also support rescue operations, especially with patrol aircraft and search and rescue helicopters.

Bearing in mind the determinants of anti-terrorist and counter-terrorist activities, it should be noted that the most important resources for countering and responding to terrorist threats are available to the Border Guard and the Armed Forces, primarily the Navy. It is these formations that have resources such as the Border Guard's Automated Radar Surveillance System and the Navy's observation posts.

Moreover, it is the military or the Border Guard that can take action in maritime areas using vessels and aircraft. In particular, vessels in the form of Border Guard vessels and Navy ships allow them to stay in maritime areas for long periods of time, potentially allowing them to obtain information on threats and prevent them through preventive actions – even by the mere fact of actively patrolling a given body of water. This capability is not provided by shore components. Indeed, a vessel is, by its very nature, a platform for reconnaissance equipment (sensors) and armament (effectors). At the same time, it should also be borne in mind that vessels allow for the use of forces of counter-terrorist units that need to be transported to the area of operations. Long-term transport using only special boats is difficult due to their design and parameters. Aircraft capabilities, on the other hand, allow for a rapid response to an incident, including the redeployment of people and equipment, but with a much shorter period of time during which a helicopter or aircraft can be in the ordered area. For aircraft, this is a period of a few hours at most, while for vessels it can be weeks. Finally, the land component in the form of a shore-based MW missile force can only be used if there is a need to destroy (sink) a vessel. The ongoing qualitative and quantitative limitations of the Navy's naval force capabilities over the years are of concern in this regard. This has a negative impact on the ability to respond to crisis situations in Polish maritime areas.

Another important problem is the fact that, in accordance with the *Act on anti-terrorist activities*, the person in charge of anti-terrorist activities is a Police officer (unless the incident would occur on a military area or facility – then the activities are directed by a soldier of the Military Police). While this is reasonable during operations on land, where it would be a representative of the formation providing the essential resources

necessary to resolve the crisis situation, in the case of maritime areas these resources will be provided by other services, having their own command systems and operating in a manner different from the land environment.

2.3. The Polish Anti-Money Laundering and Counter Financing of Terrorism system

a. Terrorism and financial crime nexus

The financing of terrorist organisations is carried out, inter alia, through crowdfunding or non-profit organisations, as well as by using the commercial system. Criminal groups and terrorist organisations use it to launder money and transfer monetary values derived from the commission of criminal acts using trade transactions – both fictitious and real, but carried out on the basis of false or misfiled shipping and customs documents.

The most common technique of money laundering through commercial transactions involves misrepresenting the value of the traded goods or their volume by:

- under- or over-invoicing of the actual value of the goods – in the first case, this mechanism allows the transfer of financial values from the exporter to the importer, who will pay for the goods at a lower price than their commercial value on the free market (the importer gains the opportunity to resell the goods at a higher profit), and in the second case, the transfer of financial values from the importer to the exporter, by paying above the actual value of the goods;
- multiple invoicing for the same goods;
- overstating or understating the volume of goods dispatched in relation to the volume of goods shown on the transport documents;
- providing an incorrect description of the goods with regard to their nature or quality on VAT invoices and transport or customs documents;
- in extreme cases, only dealing with freight or customs documentation without actually trading in the goods.

b. Protection of the State's financial interests

The authorities for the protection of the State's financial interests are an important element of the anti-terrorist system of the Republic of Poland, primarily in the area

of counteracting the illegal use of trade in goods and financial flows intended to support the activities of terrorist organisations. The tracking and analysis of commercial and financial transactions is indispensable in order to detect possible links between terrorist organisations, criminal groups and private individuals acting on their behalf. However, detecting the sourcing of funds by terrorist organisations, e.g. under the cover of legitimate economic entities or non-governmental organisations, poses a particular challenge to the competent authorities and services.

The financial information authorities in the Polish legal system are: the minister competent for public finance and the **General Inspector of Financial Information** (hereinafter: General Inspector, GIFI). The Inspector General in counteracting terrorist financing cooperates with the Head of the Internal Security Agency (ISA). The GIFI, in cooperation with the Counter-Terrorism Centre of the ISA, analyses links with persons or entities from countries with a higher terrorist risk and identifies links of these persons with terrorist organisations. A six-year term of office for the GIFI, which may be held for a maximum of two terms, and a ban on the General Inspector's affiliation with a political party were introduced in 2021.

The interministerial **Committee on Financial Security**, which had an advisory and consultative role in the application of specific restrictive measures against individuals, groups and entities, was replaced by the Financial Security Committee with an advisory and consultative role in the area of combating money laundering and terrorist financing. Thus, the position of the General Inspector was strengthened by extending the Committee's substantive responsibilities, expanding its composition and making it the lead body responsible for the area of financial security in the field of AML and CFT.

According to the *National Risk Assessment on Money Laundering and Terrorist Financing* published in mid-2019 by the GIFI, the threat of terrorist financing on the territory of Poland, like the terrorist threat itself, is currently low. However, there is a caveat that Poland may be considered an attractive country for terrorist organisations to build logistical and financial facilities. The highest level of probability in terms of terrorist financing was attributed to the physical transportation of assets across borders using natural persons. A relatively high estimate of this level was also given for the use of courier and postal services to transport illicit money across borders. In addition to this, risks were identified for areas such as virtual currencies, telecommunication services linked to mobile payments, crowdfunding, payment services (offered by entities other than banks), activities of *non-profit* organisations, insurance and banking.

c. AML and CFT strategy

On 19 April 2021, the Council of Ministers adopted the *Anti-Money Laundering and Countering Financing of Terrorism Strategy*. The document contains three sections: (1) Development of the national anti-money laundering and counter-terrorist financing system, (2) Action Plan and (3) Monitoring of the implementation of the Action Plan.

Increasing the effectiveness of the Polish anti-money laundering and counter-terrorist financing system requires action in four areas, i.e.: (1) supplementation of legal regulations, (2) development of training (both of employees of the Financial Intelligence Unit (FIU), as well as of cooperating units and obliged institutions), (3) exchange of information using electronic documents and ICT systems, and (4) generation of statistical data enabling objective assessment of the effectiveness of the national AML/CFT system.

The Strategy outlines the following priorities for the development of the national AML/CFT system:

1. **Improving the effectiveness** of the FIU and collaborating units in **analysing information** through the use of a risk-based approach.

2. **Adapting of the catalogue of obliged institutions and their obligations** to emerging risks and information needs.

3. **Harmonising and streamlining of the rules for supervision and control** of the institutions involved.

4. **Optimising** the modalities, scope and quality of **information exchange** and access to information.

5. Organising an **effective system of training** and exchange of knowledge and experience.

6. Defining **uniform rules for the generation of information**, in particular statistical data needed to carry out an assessment of the effectiveness of the national anti-money laundering and counter-terrorist financing regime and its components.

The implementation of the actions envisaged in the Strategy is staggered over the period 2021-2023 in order to be linked to the *National Money Laundering and Terrorist Financing Risk Assessment*, which should be updated at least once every 2 years.

d. Council of Europe MONEYVAL Report

The assumptions of the *Strategy* coincide with the key conclusions being the result of the fifth evaluation round on the compliance of the Polish anti-money laundering and counter-terrorist financing system with the recommendations of the FATF (Financial Action Task Force) conducted by the MONEYVAL Committee of the Council of Europe. The report was adopted during the 62nd plenary session of the MONEYVAL Committee on 16 December 2021. On the basis of the evaluation, it was concluded that Poland needs to improve the regulatory framework and increase measures against money laundering and terrorist financing, and among the elements that need to be improved were identified:

- the need to make greater use of the GIFI's analyses during prosecutions;
- strengthening cash control mechanisms at the border by providing a legal basis for the detention, restraint or seizure of suspected property;
- taking action to define terrorist financing as a separate offence and not as a derivative offence of terrorism;
- supporting terrorist financing investigations with additional guidelines and procedures;
- conducting financial investigations not only into terrorist financing cases, but also into cases of suspicion regarding the legality or destination of funds;
- considering the vulnerability of non-profit organisations to the risk of terrorist financing;
- using confiscation of the proceeds of money laundering and terrorist financing as a law enforcement policy objective;
- the need for competent authorities to develop a uniform practice to improve asset tracing.

In view of the shortcomings, Poland has been subject to extended monitoring by the MONEYVAL Committee of the implementation of the evaluation recommendations.

2.4. Selected organisational and legal developments of the AT community in Poland

a. Interdepartmental Team for Terrorist Threats (MZdsZT)

On 8 April 2021, the *Ordinance No. 37 of the Prime Minister amending the Ordinance on the establishment of the Interministerial Team for Terrorist Threats* entered into force, which introduced the following changes:

1) **§ 2 shall be replaced by the following:**

„**§** 2. 1. The team shall ensure the cooperation of the government administration in preparing to prevent, take control of, and respond to terrorist incidents by means of planned activities.

2. The main tasks of the Team are:

1) monitoring, analysing and evaluating terrorist threats and presenting opinions and conclusions to the Council of Ministers;

2) drafting standards and procedures for responding to incidents of a terrorist nature;

3) initiating, coordinating and monitoring actions taken by the relevant governmental authorities in preparation for preventing, taking control of and responding to terrorist incidents through planned undertakings;

4) drawing up proposals aimed at improving the methods and forms of preventing, preparing for and responding to terrorist incidents and requesting the competent authorities to undertake legislative work in this regard.";

2) in § 4:

a) the following paragraph 2a shall be inserted after paragraph 2:

„2a. The Team shall consider matters at meetings or by correspondence, including by means of electronic communication.",

b) paragraph 3 shall be replaced by the following:

„3. Meetings of the Team shall be convened by the Chairperson on his/her own initiative or at the request of one of the Team members".

Subsequently, on 13 October 2021, the Prime Minister signed the *Guidelines for the Coordination of the Exchange of Information on Terrorist Threats*, a draft of which was developed under the MZdsZT. In 2022, the Team also updated *Decision No. 41 of the Chairman of the MZdsZT of 2 November 2020 on the establishment of the Task Force – Standing Group of Experts* (clarifying the role of the Group and allowing for

the correspondence agreement of positions, outside the mode of permanent meetings). In addition, in the same year, Resolution No. 1/2022 of the MZdsZT removed the secrecy clauses from *Resolution No. 2/2019 of 27 August 2019 on cooperation on the assessment of the reliability of information on the setting of an explosive device*, as well as updated the organisational units of the Police cooperating in this area, inter alia, by adding the Central Bureau for Combating Cybercrime.

b. Anti-terrorism legislation

In 2021, a marginal amendment was made to the *Act on anti-terrorist activities* of 2016 as a result of the entry into force of the *Act of 30 March 2021 amending the Act on counteracting money laundering and terrorist financing and some other acts* (in Article 5.1, the composition of institutions participating in the coordination of analytical and information activities carried out by the Head of the ABW was updated).

In 2022, section 13a. was added to the *Act on anti-terrorist activities*, which reads:

> "Article 13a. 1. The Prime Minister, having regard to the possibility of a terrorist incident or a threat to public safety and order, may, by order, restrict public access to lists, registers, databases and ICT systems containing location data of technical infrastructure.
>
> 2. The order referred to in paragraph 1 shall indicate the lists, registers, databases and information and communication systems to which public access shall be limited and the period of such limitation.
>
> 3. The keepers of the lists, registers, databases and information and communication systems designated in the order referred to in paragraph 1 shall restrict public access to them in accordance with that order without delay".

In 2023, it is planned to amend the *Act on anti-terrorist activities* and the *Act on the Internal Security Agency and the Foreign Intelligence Agency*, constituting the implementation into the Polish legal order of the mechanism for blocking content promoting terrorism on the Internet under *Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on the prevention of the dissemination of terrorist content on the Internet*.

Conclusions (#ZaleceniaAT)

In the PTBN Report, Volume I (2020): "Terrorist Threats and the Anti-Terrorist System in the Republic of Poland", issued in March 2021, we defined seven challenges facing Poland in the context of building societal resilience to terrorist threats and improving the anti-terrorist system in the Republic of Poland. In this report, we also proposed possible options for solutions. The #ZaleceniaAT of 2021 addressed issues such as:

1. supporting research on political extremism and radicalisation of religious minorities and building bridges between the institutions responsible for coordinating the strategic level of the AT system in the Republic of Poland (MZdsZT) and those carrying out such research projects;

2. criminalisation of the possession of material/content needed to commit a terrorist offence (excluding scientific and educational activities) and education and information activities pointing out the negative consequences of such behaviour;

3. adopting a National Counter-Terrorism Education Programme to raise awareness and develop appropriate mechanisms for responding to terrorist threats, which would be coordinated within the whole of the AT system in the Republic of Poland by an existing state institution with responsibility for terrorism prevention;

4. developing an anti-terrorist security audit methodology (vulnerability to physical incidents of a terrorist nature) for the seats of constitutional state bodies, facilities of strategic importance for the country's security and defence and selected critical infrastructure facilities of the Republic of Poland, which would be implemented by a state institution competent in the field of personal and property protection;

5. flattening the procedures related to the use of counter-terrorist forces by simplifying statutory procedures (among other things, moving decisions from the departmental level to the tactical level) and standardising in this respect the procedures for carrying out official activities for all formations used to support specialised police units;

6. linking the staffing levels of provincial counter-terrorist forces and the level of capability and readiness to act to possible threats, in particular the size of urban centres, the volume of critical infrastructure and other contemporary attack targets, while increasing their mobility;

7. establishing teams which can support system entities of medical rescue, such as Rescue Task Force (Medical Rapid/Special Response Teams – MZSR) and undertaking works on solutions incorporating MZSR into the Polish system of medical rescue, as well as standardising their scope of competence and responsibility in the area of medical security of terrorist or extraordinary events.

Two years later, all the calls and #ZaleceniaAT described in the previous report remain relevant and need to be implemented.

In addition, they are supplemented by the anti-terrorist security deficits that have been defined in the current version of the PTBN Report. In 2023, we propose the following #ZaleceniaAT:

- Implementing the provisions of EU Directive 2017/541 of 15 March 2017 on combating terrorism with regard to the establishment of a single point of contact for victims of terrorism, in order to ensure that Polish citizens have equal rights when pursuing claims arising from a terrorist attack in which they have suffered.
- Improving the capacity to prevent terrorist incidents in Polish maritime and coastal areas by:
  - » recognizing the Exclusive Economic Zone as an area where anti-terrorist activities may be carried out – this will allow activities to be carried out in the event of a threat to the security of shipping or infrastructure in the entire maritime area of the Republic of Poland;
  - » indicating that anti-terrorist activities in maritime areas (or more broadly: in the area of local jurisdiction of the Border Guard) may be directed by an officer of this formation or directly by an officer of the Navy;

  - » ensuring that port facilities, those located in offshore areas (oil rigs, wind farms) and those located on the coast (including the proposed nuclear power plant) are protected from terrorist activities, including those carried out using unmanned underwater vehicles and unmanned aerial vehicles;
  - » developing the capacity of the maritime components of the armed forces and police formations to provide anti-terrorist and anti-sabotage security in maritime areas, including for the protection of their oil rigs;
  - » striving to have ships that are as versatile as possible, designed to perform tasks equally in times of peace, crisis and war. The backbone of this force should be multi-purpose frigates, submarines and naval aviation aircraft and helicopters, supported by mine countermeasures forces. When defining the future of the patrol component, consideration should be given to the performance of these units also in times of crisis and war. This is because the capabilities needed in wartime also allow tasks to be performed effectively in times of peace and crisis, especially in support of counter-terrorism operations and critical infrastructure protection;
  - » assessing counter-terrorism capabilities in the maritime environment, including identifying the most likely counter-terrorism scenarios. In particular, care should be taken to avoid duplication of competencies and tasks between different formations. One or two services and their components should be identified as the lead and personnel, equipment and training resources should be concentrated in them.

- Systematic (using statistical tools) monitoring of indicators of the growth of the potential terrorist threat: (a) non-political violent crime (especially heavy and technically advanced), (b) hate speech, praise of violence and incitement to violence in public spaces (referring not to selected groups but to all participants in the conflict).
- Transfer of norms for combating cybercrime and cyberterrorism from criminal law to administrative law.
- Update of the National Money Laundering and Terrorist Financing Risk Assessment (has not been updated since 2019).

This Report contains only the private views of the authors and cannot be associated with the institutions in which the authors are employed.

Selected bibliography

Books:

Bolechów B., *Słowa w cieniu mieczy – Dabiq i narracja państwa islamskiego* (Eng. Words in the shadow of swords – Dabiq and the Islamic State narrative), Wrocław: Wydawnictwo Uniwersytetu Wrocławskiego, 2020.

Burczaniuk P., *Legal aspects of the European inteligence services' activities,* Warsaw: Wydawnictwo ABW, 2022.

Cymerski J., Zubrzycki W., *Terroryzm i sposoby jego finansowania* (Eng. Terrorism and its financing), Szczytno: Wydawnictwo WSPol, 2022.

Cymerski J., Zubrzycki W., *Terroryzm/Antyterroryzm dwie dekady po zamachach z 11/9* (Eng. Terrorism/Anti-terrorism two decades after the 11/9 attacks), Szczytno: Wydawnictwo WSPol, 2023.

Encyklopedia Bezpieczeństwa Wewnętrznego (Eng. Encyclopedia of Internal Security), Warszawa: INP UW – ELIPSA, 2021.

Izak K., *Leksykon organizacji i ruchów islamistycznych* (Eng. Lexicon of Islamist organisations and movements), Warszawa: Dialog, 2014.

Hołub A., *Ekstremizm i radykalizm wobec państwa* (Eng. Extremism and radicalism against the state), Szczytno: Wydawnictwo WSPol, 2020.

Olech A., *French and Polish fight against terrorism*, Poznań: Kontekst Publishing House, 2022.

Olech A., *Walka z terroryzmem polskie rozwiązania a francuskie doświadczenia* (Eng. Fight against terrorism Polish solutions vs. the French experience), Warszawa: Difin, 2021.

Olender D., *Przeciwdziałanie i zwalczanie piractwa morskiego* (Eng. Preventing and combating maritime piracy), Warszawa: Difin, 2017.

Olejnik Ł., Kurasiński A., *Filozofia cyberbezpieczeństwa* (Eng. The philosophy of cybersecurity), Warszawa: PWN, 2022.

Piasecka P., Maniszewska K., Borkowski R. (eds.), *Dwie dekady walki z terroryzmem* (Eng. Two decades of fighting terrorism), Warszawa: Difin, 2022.

Piekarski M., *Ewolucja Sił Zbrojnych RP w latach 1990-2020 w kontekście kultury strategicznej* (Eng. Evolution of the Polish Armed Forces 1990-2020 in the context of strategic culture), Toruń: Wydawnictwo Adam Marszalek, 2022.

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

Piekarski M., *Ochrona infrastruktury krytycznej na polskich obszarach morskich w kontekście zagrożeń hybrydowych* (Eng. Protection of critical infrastructure in Polish maritime areas in the context of hybrid threats), Ekspertyzy PTBN, nr 1 (2023), Warszawa 2023.

Terrorism Prevention Brochure, Warszawa: Centrum Prewencji Terrorystycznej ABW, 2022.

Rękawek K., *Foreign Fighters in Ukraine – The Brown–Red Cocktail*, Abingdon-on-Thames: Routledge 2022.

Wiśniewska-Paź B., Szlachter D. (eds.), *XX- lecie Wojny z terroryzmem – bilans i konsekwencje* (Eng. The 20th anniversary of the War on Terror – assessment and perspectives), (Vol. I: *Współczesne zagrożenia, strategie reagowania, edukacja*) (Eng. Contemporary threats, response strategies, education), Toruń: Wydawnictwo Adam Marszalek, 2022.

Wiśniewska-Paź B., Szlachter D. (eds.), *XX-lecie Wojny z terroryzmem – bilans i konsekwencje (Eng. Contemporary threats, response strategies, education),* (*Vol. II: Infrastruktura krytyczna, analizy, case study*) (Eng. Critical infrastructure, analysis, case study), Toruń: Wydawnictwo Adam Marszalek, 2022.

Wojtasik K., Ścieżki radykalizacji i działalności *dżihadystycznych organizacji terrorystycznych* (Eng. Pathways of radicalisation and activities of jihadist terrorist organisations), Toruń: Wydawnictwo Adam Marszalek, 2021.

Wojtasik K., *Anatomia zamachu (Eng. Anatomy of an attack),* Warszawa, Medium, 2019.

Wojtasik K., *Wyniki badania na temat percepcji zagrożeń o charakterze terrorystycznym wśród uczestników EU PSA* (Eng. Results of the survey on the perception of terrorist threats among EU PSA participants), Analizy PTBN, nr 1 (2023), Warszawa 2023.

Articles/chapters:

Gasztold A., Szlachter D., *The Role of Anti-Terrorist Coordination Centers in the Security Systems of Germany and Poland. A Comparative Analysis,* „Studia Politologiczne" 2022, vol. 63.

Piekarski M., *Zamachy z użyciem urządzeń wybuchowych w możliwych scenariuszach wojny hybrydowej w Polsce* (Eng. Attacks with explosive devices in possible hybrid war scenarios in Poland), [in]: Wilk-Woś Z., Stawicki R. (eds.). *Wokół bezpieczeństwa wewnętrznego i zewnętrznego: wyzwania, metody i narzędzia*, Łódź: Wydawnictwo Społecznej Akademii Nauk, 2019.

Piekarski M., *Broń strzelecka jako narzędzie ataków terrorystycznych: dotychczasowe trendy i kierunki ewolucji* (Eng. Small arms as a tool of terrorist attacks: past trends and directions of evolution), [in]: Wiśniewska-Paź B., Stelmach J. (eds.) *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej*. (T. I) Warszawa: Difin, 2021.

Szlachter D., *Dwie dekady budowy systemu AT w warunkach RP* (Eng. Two decades of building an AT system under Polish conditions), [in:] Piasecka P., Maniszewska K., Borkowski R. (eds.), *Dwie dekady walki z terroryzmem*, Warszawa: Difin, 2022.

Szlachter D., *Dwie dekady walki z terroryzmem w warunkach RP* (Eng. Two decades of building an AT system under Polish conditions), [in:] Stelmach J. (ed.), *Terroryzm i antyterroryzmu w opiniach ekspertów w XX rocznicę zamachów na WTC i Pentagon*, Warszawa: Difin, 2022.

Szlachter D., *Rozpoznanie i sabotowanie potencjału infrastruktury krytycznej krajów Europy Środkowowschodniej i Północnej jako przykład strategicznych celów aktywności rosyjskich służb specjalnych* (Eng. Recognition and sabotage of the critical infrastructure potential of Central and Eastern and Northern European countries as an example of strategic targets of Russian special services activity), "Biuletyn Biura Analiz i Reagowania" (Rządowe Centrum Bezpieczeństwa) 2021, no. 32.

Tomasiewicz J., *Ideologia przemocy w „wieku końca ideologii": idee i ideologie w terroryzmie XXI w.* (Eng. The ideology of violence in the "age of the end of ideologies": Ideas and ideologies in 21st century terrorism.), [in:] Piasecka P., Maniszewska K., Borkowski R. (eds.), *Dwie dekady walki z terroryzmem*, Warszawa: Difin, 2022.

Tomasiewicz J., *The Ideological Component in 21st Century Terrorism*, "Studia Poli-to-logiczne" 2002, vol. 63.

Tomasiewicz J., *Zagrożenia z przyszłości: próba ekstrapolacji* (Eng. Threats from the future: an attempt at extrapolation), [in:] Wiśniewska-Paź B., Szlachter D. (eds.), *XX-lecie Wojny z terroryzmem – bilans i konsekwencje* (Vol. I), Toruń: Wydawnictwo Adam Marszalek, 2022.

Wojtasik, K. *Implementacja tzw. załącznika AT w zakładach produkcyjnych. Doświadczenia, wnioski i rekomendacje* (Eng. Implementation of the so-called AT Annex in production facilities. Experiences, conclusions and recommendations), [in]: Wiśniewska-Paź B., Szlachter D. (eds.), *XX-lecie Wojny z terroryzmem – bilans i konsekwencje* (Vol. II), Toruń: Wydawnictwo Adam Marszalek, 2022.

Reports:

Applied Cybersecurity and Internet Governance (2022).

Country Report on Terrorism (2021-2022).

Cross-national level report on digital sociability and drivers of self-radicalisation in Europe (DARE: Dialogue about Radicalisation and Equality), bmw 2020.

EU Terrorism Situation & Trend Report (TE-SAT) (2021-2022).

Global Terrorism Index (2021-2023).

Systematic Review of Quantitative Studies on Inequality and Radicalisation (DARE: Dialogue about Radicalisation and Equality), bmw 2018.

Periodicals:

“Biuletyn Biura Analiz i Reagowania RCB” (2021-2021).
“Frag-Out” 2020-2023.
“Internal Security” (2020-2023).
“Polska Zbrojna” (2020-2023).
“Przegląd Bezpieczeństwa Wewnętrznego” (2020-2023).
“Przegląd Policyjny” (2020-2023).
“Przegląd Strategiczny” (2020-2023).
“Securo – badania nad terroryzmem” (2022).
“Special-Ops” (2020-2023).
“Studia Politologiczne” (2021-2022).
“Terroryzm. Studia, analizy, prewencja” (2022-2023).

Events/Media projects/ Audio-visual recordings

#20latWTC

The Centre for Security Studies and Education at the University of Wrocław and the Polish Association for National Security organised a conference on 10 September 2021, entitled "The 20th Anniversary of the War on Terror – Assessment and Perspectives", which aimed to summarise two decades of the fight against terrorism at the national and international level, as well as to commemorate the victims of those events with a special focus on Polish citizens.

The event was held under the honorary patronage of, among others, the National Security Bureau, the Ministry of Internal Affairs and Administration, the Government Centre for Security, the Civil Aviation Authority and the Zygmunt Wojciechowski Western Institute.

The aim of the conference was to analyse the consequences of the 9/11 attacks from the widest possible perspective, from the geopolitical effects through the evolution of protection systems, methods and forms of identifying and combating terrorist threats, to the development of unmanned platforms and ways of providing medical assistance to victims of terrorist attacks. The issues were discussed during panel discussions, fostering an exchange of views between professionals representing different professional groups and perspectives.

The conference was attended by more than 50 speakers representing key, civilian and uniformed, academic centres, recognised think tanks, the largest Polish news por-tal

dedicated to security, a number of state institutions (i.e. RCB, BBN, ABW, Police, ULC, SOP) and foreign partners representing, among others, the US diplomatic mission in Poland, the European Commission (DG HOME) and FRONTEX. The #20latWTC online broadcasts were watched by several hundred viewers in total.

The following list of recordings from the #20latWTC conference, which are available on the YT channel, at: **https://www.youtube.com/@20latwtc27**

- Opening of the conference and Panel No. 1: Geopolitical implications of the terrorist attacks of 11 September 2001
- Panel No. 2: Security of public spaces and critical infrastructure
- Panel No. 3: Anti-terrorism education
- Panel No. 4: The evolution of terrorist groups' ideologies, organisations, strategies and tactics and the direction of counter-terrorism efforts
- Panel No. 5: Reform of the security systems of EU and NATO member states
- Panel No. 6: Modern technologies as a tool of terrorism in the second decade of the of the 21st century
- Panel No. 7: Methods of analysis and assessment of terrorist threats

Polish Association for National Security is an interdisciplinary scientific society bringing together researchers involved in various fields of security.

The aim of the Association is to develop and disseminate knowledge on building state resilience against threats to national security and the international position of the Republic of Poland.

PTBN is a member of the EU-HYBNET pan-European network for countering hybrid threats. PTBN's specialisation within EU-HYBNET includes the protection of critical infrastructure. PTBN representatives also participate in the European Commission's DG MOVE working group on drone systems and take part in initiatives and meetings dedicated to building resilience to terrorist attacks in public spaces implemented by the European Commission's DG HOME.

Members of the Association develop and publish the "PTBN Report" series, which analyses contemporary threats to the security of the Republic of Poland and the Polish raison d'état (terrorism, information warfare in cyberspace, modern technologies vs. critical infrastructure protection, hybrid threats to the energy sector on land and at sea).

Each PTBN Report contains recommendations for state bodies and institutions, as well as key economic players from the point of view of ensuring the continuity of the functioning of the economy and the state.

Published to date:

- PTBN Report, Volume I (2020): "Threats of a terrorist nature and the anti-terrorism system in the Republic of Poland",
- PTBN Report, Volume II (2021): "Security of critical infrastructure against threats from unmanned platforms",
- PTBN Report, Volume III (2022): "5G technology and information threats to critical infrastructure".

In 2023, PTBN introduced two new specialist series: "PTBN Expertises" and "PTBN Analyses" under which the following publications have been published so far:

- Piekarski M., Ochrona infrastruktury krytycznej na polskich obszarach morskich w kontekście zagrożeń hybrydowych (Eng. Protection of critical infrastructure on Polish maritime areas in the context of hybrid threats), Ekspertyzy PTBN, no. 1 (2023), Warszawa 2023.
- Wojtasik K., Wyniki badania na temat percepcji zagrożeń o charakterze terrorystycznym wśród uczestników EU PSA (Eng. Results of the survey on the perception of terrorist threats among EU PSA participants), Analizy PTBN, no. 1 (2023), Warszawa 2023.

SECURITY
BEYOND DIVISIONS

www.PTBN.online