DOI: 10.4467/27204383TER.22.026.16346

ORCID: 0000-0003-1514-7657

MICHAŁ PIEKARSKI

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

Abstract

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

Keywords:

terrorism, terrorist attack, hybrid warfare

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

---

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[16] Ibid., p. 173.

[17] Ibid., p. 174.

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

Hybrid operations in Poland's security environment

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

Possible attack scenarios

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

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

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

Scenario 1. Terrorist attack against military infrastructure and equipment

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

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

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

[23] Ibid.

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

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

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

Scenario 1a. Terrorist attack against military personnel

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

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

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

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

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

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

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

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

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

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

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

Scenario 2. Attack on a critical infrastructure facility

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

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

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

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

Scenario 2a. Attack on electricity infrastructure

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

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

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

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

Scenario 2b. Attack on fuel infrastructure

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

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

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

Scenario 2c. Attack on transport infrastructure

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

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

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

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

Scenario 3. Attack on a symbolic target

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

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

Scenario 3a. Assassination of a well-known person

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

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

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

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

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

Scenario 3c. Assault on a symbolic site

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

Scenario 4. An attack demonstrating ineffective performance of services

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

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

Conclusion

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

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

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

Bibliography

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

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

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

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

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

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

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

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

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

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

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

Internet sources

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

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

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

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

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

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

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

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

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

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

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

Legal acts

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

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