Polish Political Science Yearbook, **vol. 51(4) (2022), pp. 95–107**
DOI: https://doi.org/10.15804/ppsy202254 PL ISSN 0208-7375
www.czasopisma.marszalek.com.pl/10-15804/ppsy

Wojciech Wróblewski
The Main School of Fire Service in Warsaw (Poland)
ORCID: 0000-0003-3415-9485
e-mail: wwroblewski@sgsp.edu.pl

Terrorism and the Hybrid Warfare in Aspect of War in Ukraine

Abstract: Contemporary terrorism is characterised by a complex and networked model of operation. While the main objectives of terrorist acts remain the same, the attack environment, tactics and tools are changing. The international community is taking steps to strengthen counter-terrorism systems, but these are peaceful solutions. These models do not consider the conditions of hybrid armed conflicts in which terrorism is an element of combat tactics. It is a relatively new phenomenon and particularly dangerous for the civilian population. The acts of terror in hybrid warfare are not mechanisms with a simple scheme of action, and, as we try to show in this article, they represent a deliberate and broad spectrum of action. Therefore, there is an urgent need to understand terrorism in the context of the threat of hybrid war (especially when terrorist acts complement hybrid tactics or significantly replace conventional tactics). This type of threat must be recognised before achieving its strategic goals. From the substantive point of view, the article studies the problem of terrorism as one of the threats of an armed conflict in Ukraine, commonly known as hybrid war.

Keywords: *civil protection, hybrid war, war in Ukraine, terrorism*

Abbreviations:
NATO – North Atlantic Treaty Organization
SBU – Security Service of Ukraine
FSB – Federal Security Service of the Russian Federation

Introduction

Terrorism is one of the most complex and interdisciplinary threats at the local and global levels. The majority of international communities intensify efforts to effectively mitigate the terrorism threat. However, they are not sufficient, and in addition, the anti-terrorist security environment has been violated by the new threats. During the pandemic time, acts of terrorism may have been minimised, but they did appear. These acts focused on

and have been diverted into medical infrastructure. Escalation of terrorism in cyberspace occurred and significantly increased the level of indoctrination and radicalisation. Once the pandemic situation stabilised, a full-scale armed conflict in Ukraine appeared. This threat is particularly dangerous from the perspective of crossing the threshold of war and due to the hybrid nature of actions, including acts of terrorism used in conventional tactics. Therefore, there is an urgent need to understand terrorism in the context of the threat of hybrid war (especially when terrorist acts complement hybrid tactics or significantly replace conventional tactics). This type of threat must be recognised before achieving its strategic goals. From the substantive point of view, the article deals with the problem of terrorism as one of the threats of hybrid war. Research can stimulate further efforts to better understand and combat terrorism and its specific manifestations in civil defence systems in hybrid armed conflicts. The views presented in this study constitute the author's personal opinion only and may not be treated as the official positions of any institution, organisation or state. Any mistake that may appear in the elaboration is the author's sole responsibility.

Methodology

The scientific databases (Google Scholar, Science Direct, ResearchGate) were analysed to identify the problem. When the sequence 'terrorism hybrid warfare Ukraine' was typed into academic databases, the results were as follows: Google Scholar showed 1910 studies, the vast majority of which did not relate to the use of terrorism in the conflict in Ukraine. In Science Direct, 127 studies were found, while 100 studies were indexed in ResearchGate. However, only a small number were directly related to the research area. The analysis of the studies in the scientific databases suggested that the role of terrorism as part of hybrid warfare was only marginally developed. All available scientific research data regarding the topic were analysed, and all information from open and government sources were collected. It showed that the use of terrorist tactics in hybrid military operations was a greater threat than in peacetime conditions. The acts of terrorism during the conflict in Ukraine in 2022 were analysed based on an open-source database. In order to carry out the analysis in open sources, typical web browsers were used, in which the results after entering the adopted sequence (in Polish and English) were as follows: Google showed 70100 results in Polish and 76100 results in English. There were 3780 results in Polish and 26300 in English in Microsoft Bing. Yandex found 5 thousand results in Polish and 2 million results in English. Most of them were not related to terrorism. The classification of events was based on the NATO definition of terrorism. Only those events, which were defined as terrorism in open sources, were accepted. Based on the events, a scheme of using terrorism in the activities carried out so far in Ukraine was developed. The most important elements that may serve as a guideline for an anti-terrorist strategy in hybrid wars were identified. Two types of analysis were carried out: content and thematic.

Literature Review

Russia's recent aggression against Ukraine in 2022 has given a broader context to the concept of hybrid (non-linear) war, which as a concept, goes beyond framed cause-and-effect patterns of conflict with attributes of interrelationships, dynamics, and processes. The authors of the publication are divided on the criteria for assessing conflicts in terms of hybridity. It is because hybrid actions are usually covert and attributed to actions below the threshold of war, although nowadays, hybrid actions are increasingly becoming a tactic in open armed conflicts (war in Ukraine).

According to Mumford, hybrid war is a multi-causal form of conflict that takes place in a multi-threat environment in which states and non-state actors interact (overtly or covertly) using a mix of regular and irregular warfare tactics to expand influence and interests, and in some cases territory (Mumford, n.d.). Solmaz (2022), on the other hand, when searching for the aetiology of hybrid warfare, draws attention to Thomas Mockaitis's study of British Counterinsurgency in the Post-imperial Era in 1995. However, the term is commonly attributed to a speech by General James Mattis at the Defence Forum supported by the Naval Institute and Marine Corps Association in September 2005 (Hoffman, n.d.). The term became particularly popular following the publication of Frank Hoffman (n.d.), *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies. Hoffman's team of researchers analysed contemporary theoretical models to propose a new scientific paradigm of future wars while juxtaposing their attributes with the course of historical conflicts to explain potential hybrid threats in their example. Three categories of theories – "fourth-generation wars", "complex wars", and "war without limits" – were examined. As Konieczny states: "In the case of the former, the claim is borrowed about the mixed character of future armed conflicts, i.e. (the simultaneous coexistence of a state of war and peace and the disappearance of the boundary between combatants and civilians) and the loss by the state of its monopoly on the use of violence - which is connected with the appearance of non-state actors as a fighting party. The concept of "complex wars" delivers the idea of the synergistic combination of conventional and irregular actions at strategic, operational, and tactical levels. The last theory Hoffman and his colleagues examined was "war without limits". This theory emphasised, among other things, the concept of omnidirectionality, which assumes that all spheres of the surrounding reality will constitute a single battlefield in future conflicts. Hoffman's team synthesised these elements and proposed a definition of hybrid warfare. According to it, hybrid warfare includes a set of different methods of warfare, including conventional actions, irregular tactics and armed groups, terrorist acts, including mass violence, and criminal actions" (Skoneczny, n.d.).

The concept of hybrid warfare became particularly discussed in the aftermath of the so-called Ukrainian crisis or "Russia's operation in Crimea" in 2014 (Solmaz, 2022) and as a result of the full-scale war in Ukraine in 2022. As a result, a special character was assigned to the so-called Gerasimov doctrine, delivered at a Russian military conference in 2013 and

later published in the article *The Value of Science in Prediction*. Gerasimov's concept, despite he does not once use the format "hybrid", indicates the direction of the evolution of armed conflicts, from which one can infer the identity of the proclaimed theory with the attributes characteristic of hybrid war. Gerasimov stated that there would be an increasing tendency to blur the boundary between the state of war and peace (no formal act of declaring war and a paradigm shift in the previously known patterns of war). An example is the so-called "Arab Spring", or events in North Africa and the Middle East. According to Gerasimov, the principles of warfare have also changed, with political, economic, psychological, and humanitarian instruments becoming important, supported by military means, especially in the form of information warfare and the actions of special units. The full-scale use of armed troops (often in the form of stabilisation, peacekeeping or humanitarian missions) is a stage to complete the victory. Gerasimov considered that the differences between the levels of action (strategic, operational, tactical) and between offensive and defensive have blurred (Skoneczny, n.d.; Valery, 2013).

Both Hoffman's and Gerasimov's theories have some similarities. However, differences are also noticeable as similarities can be pointed out: the changes that are taking place in the tactics of modern warfare, including the decentralisation of command structures, the merging of strategic, operational and tactical spheres of action, and the significant increase in the importance of non-military means of warfare; the increasingly important role played by irregular forms of warfare (mainly the methods of guerrilla warfare and the use of small combat units) and the blurring in future armed conflicts of the clear division between the state of war and peace and between soldiers and civilians. In the fundamental differences, it should be pointed out that Hoffman, using the concept of "hybrid warfare", focuses primarily on the tactics of combat units and pays less attention to the non-military means of conducting hybrid conflict. In contrast, Gerasimov pays strategic attention to the non-military means of conducting war (e.g., the need to use propaganda activities – including modern information technologies - not only to disinform enemy troops or conduct intelligence operations but also to win the favour of the population living in the area of conflict or manipulate its mood) (Skoneczny, n.d.; Giles, 2020).

At the time of writing (despite at least a dozen definitions of hybrid warfare), the prevailing literature is the NATO and European Parliament (EP) definition. The definition adopted by NATO states that hybrid action combines military and non-military as well as covert and overt means, including disinformation, cyberattacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace and to sow doubt in the minds of target populations. Their goal is to destabilise and weaken societies (*NATO's response to hybrid threats*, n.d.; Bilal, 2021).

According to the Common Framework on Countering Hybrid Threats, the concept of hybrid threats aims to capture the mix of conventional and unconventional, military and non-military, and overt and covert activities that can be used in a coordinated manner by

state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared war (The European Commission, 2016).

Both NATO and EP definitions, in the presented approaches, do not mention terrorism in a literal (direct) way, but as shown by the Global Terrorism Index 2022 (Institute for Economics & Peace, 2022), it is a threat that should be included in any concepts of hybrid warfare (both for informal and formal actions).

Terrorism in a Hybrid Warfare

Seeking the place and forms of terrorism of the hybrid war, without the unique definition of terrorism, this analysis will build on the understanding of terrorism in NATO's Defense Against Terrorism Military Concept. The unlawful use or threats of force or violence, incitement to fear and terror against individuals or property to compel or intimidate governments or societies, or to take control of populations for political, religious or ideological purposes[1]. As noted by Varga et al. (2022), this approach is so broad that it allows for a comprehensive analysis of the indicated problem because it does not limit either the time of peace or the time of war. Moreover, the pursuit of military goals is not mentioned literally. The analysis focuses on the context of an equivalent conventional war (military goals should be counted among the political goals because, in the case of war, both goals are inseparable) and on the notion of "property", which was not more precise, its actions can be considered as directed against any private property, critical or civil infrastructure, housing, vehicles or other objects other than life and health purposes. It is also important that this definition covers terrorism committed by state and non-state actors.

There is no doubt that acts of terrorism are irregular activities that strike directly or indirectly at collective security. These acts, combined with war and rising geopolitical tensions, make terrorism an extremely effective weapon against state and non-state actors. As Mumford (2016) notes, "it is a particular threat in that civilians caught in the web of kinetic and non-kinetic actions must face attacks that are not determined by any humanitarian rules. Terrorism as an element of hybrid tactics is undoubtedly an advantage for the attacker, mainly due to drawing the greatest possible benefit from the existing conflict and avoiding the risks arising from conventional actions that are subject to international legal control". The irregular component, which is the act of terrorism, can significantly increase the operational opportunities and thus affect the strategic objectives. It must be agreed that counter-terrorism in hybrid warfare can no longer be seen as an isolated policy area, separate from other military or police operations. Under conditions of war, it must be recognised that, in a way, the civilian population itself must be the counter-terrorism component. In short, the tactical acts of terrorism seen today in hybrid war have the collective capacity to

[1] https://www.nato.int/cps/en/natohq/topics_69482.htm

have a strategic effect, given how it is used in conjunction with other conventional modes of conflict (Mumford, 2016).

This thesis is somewhat confirmed by Hoffman, who stated that: "The likeliest opponents on future battlefields accept no rules. Their principal approach will be to avoid predictability and seek advantage in unexpected ways and ruthless modes of attack. Acts of terrorism will be a key way for them to achieve this" (Hoffman, n.d.).

According to the Global Terrorism Index in 2020, 97.6% of deaths from terrorism occurred in conflict-affected countries. 80% of all terrorist incidents have occurred within 50 kilometres of a zone where a conflict is taking place, and as the intensity of conflict increases, so does the lethality of terrorist actions. Terrorist attacks in conflict countries are more than six times deadlier than attacks in peaceful countries. In armed conflicts, the intensity of terrorist activity in a given year is proportional to the number of battle deaths. Terrorism appears to be contracting into conflict areas, with a higher percentage of attacks happening in conflict areas.

All of the ten countries most affected by terrorism in 2021 were involved in armed conflict in the previous year, according to the report. The link between conflict and terrorism is strong because as the intensity of conflict increases, violence against police and military becomes more acceptable, as does violence against civilians perceived to be associated with the enemy. Terrorism is typically used to achieve tactical or strategic goals, as seen in the conflicts in Iraq, Afghanistan, and Syria (currently also in Ukraine). Moreover, as the intensity of conflict increases, the psychological barriers that protect against large-scale violence decrease. Over the past three years, 95.8% of terrorism deaths have occurred in conflict-affected countries, rising to 97.6% by 2021. As the intensity of conflict increases, the death toll resulting from terrorist activities increases. Attacks in countries with conflict are six times more deadly than those in countries without conflict. There is a significant statistical relationship between the intensity of conflict and the frequency of terrorist attacks (Institute for Economics & Peace, 2022). However, a distinction must be made between the use of terrorism in war and insurgent struggle. Unfortunately, it still happens that these two areas are treated integrally, although they are not. This aspect is pointed out by the already cited Global Terrorism Report (Institute for Economics & Peace, 2022) and Mumford, who points to the blurring of the classical understanding between terrorism and insurgency. Mumford writes, "terrorism is primarily a symbolic tool of political violence, used tactically and often indiscriminately to ensure coercion through fear. Insurgency is a strategic effort to overthrow and then transform the existing status quo through a combination of political and violent means. Therefore, terrorist groups must be distinguished from insurgent groups not only because of their different emphasis on tactics and especially the level of discrimination in attacks (insurgent groups tend to be much more likely to bomb specific targets such as embassies or symbols of the occupying power and to attack primarily military and political targets rather than civilians), but we must also consider the difference in strategic end goals

that the two have". Hence, Mumford (2016) points to terrorism as one of the most important elements in hybrid war.

Terrorism in hybrid warfare has one more feature. It can lead to the arousal of terrorism on a global scale. An example of this is the ongoing conflict in Ukraine, which has provided an opportunity for the leaders of the Islamic State (IS) to call on their members and sympathisers to carry out attacks in Europe. According to open sources, a IS spokesman stated that the Ukraine war is a "great opportunity" to take revenge for the death of leader Abu Ibrahim al.-Hashemi al-Quraysh[2].

Terrorism in Ukraine's Hybrid War – MODUS OPERANDI

The eastern doctrine of using terrorism in asymmetric (hybrid) war has already been described in detail by Yevgeny Eduardovich Messner, who, in his *study Miatezh - imia trietjej wsiemirnoj*, predicted the form and features of the Third World War, which will develop before the eyes of the unseen world (*Operation Crimea…*, n.d.). This concept was described in detail by Kazimierz Kraj, who stated that Messner, based on the observation of the development of events, concluded that between irregular fighting and underground strikes (terrorism) of secret or terrorist organisations, sabotage groups and individual fighters, there will be a synergism that will be difficult to classify and to identify their sources. Messner's concept of miatezh warfare forewarned the world of the advent of an era of non-classical wars, worldwide rebellion, insurgency (miatezh), and terror without any bounds. As it was argued, during two world wars and a host of local wars, a "worldwide revolution" was born. Wars became intermingled with rebellions, insurgencies (guerrillas, saboteurs, terrorists), rebellions with wars, and so a new form of armed conflict emerged, which he called "miatieżewojna". For Messner, the "miatieżewojna" has the characteristic of broad conflict and is not guided by specific norms or templates of behaviour. The tactics of war-rebellion are flexible: "avoid what is strong, strike at what is weak". When they expect you at the gates, enter through the window. The stages of "miatieżewojna" have such phases as demoralisation, disorder, terror, progressive recruitment to the cause of revolution, reconstruction of souls (creation of a new man), and construction of the system of the machine-human. Messner concluded that the time of Clausewitz's classical wars had passed. As Kraj goes on to write, despite the initial rejection of Messner's concept, the issue of miatezh warfare was in the public eye, already during the discussion of Russia's new military doctrine in 1999. The Chechen wars, the destabilised situation in the North Caucasus, the burning borders of Tajikistan, the war in Afghanistan, Iraq, Libya, Syria and currently in Ukraine show the timeliness of the problem of miatieżewojna (hybrid, irregular war) (*Operation Crimea…*, n.d.).

[2] https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8403507,panstwo-islamskie-wezwanie--do-atakow-w-europie.html

As noted by Varga et al. (2022), contemporary Russian military thinking pays the most attention to the role of asymmetric and indirect methods, including the use of terrorist formations both to defend the country against such actions and to utilise them for offensive purposes. Contemporary Russian military thought attaches great importance to the role of asymmetric and indirect methods, including the use of terrorist formations to defend the country against such actions and utilise them for offensive purposes. Russian military analysts have carefully tracked the asymmetric conflicts of recent decades conducted by insurgents and terrorists and have drawn conclusions that may be relevant to Russia. One such promise, repeated in many military publications, is that the United States and its western allies are more vulnerable to casualties and have many vulnerable facilities critical to their operations. Exploiting these vulnerabilities could become the basis of a Russian asymmetric strategy. Targeting infrastructure and civilians seems justifiable to Russian military thinkers in a situation of total war against an equal opponent. Using terrorists and other illegal formations can serve operational and strategic purposes, as it can force the leaders of an enemy state to conform to political will. The Russian authors note that nuclear weapons no longer ensure state sovereignty and integrity under cyber, network-centric, psychological, and biological warfare conditions. They note that information, economic and terrorist warfare is becoming natural (Varga et al., 2022; *Terrorism Threat…*, 2017). However, this is not a coherent approach because Russian language studies are dominated by the conviction that Russia does not wage hybrid war and does not commit terrorist acts, and attributing to it the attributes of such actions is just political rhetoric of the west, which justifies its hybrid conflicts and conducts anti-Russian agitation (Konyshev & Parfenov, 2019). Varga et al. (2022), in their *Defence Against Terrorism Review*, identified five main types of terrorist attacks that Russia can carry out using its own services or proxies:

"– Terrorist attacks with a strategic effect could either coerce the adversary into some political concessions, end the conflict in terms acceptable for Russia, or significantly undermine its political and/or operational capabilities. Such attacks could also be used to provoke the enemy to take actions that would actually serve Russia's interests.
– Attacks on the political/military leadership of the enemy could decapitate the adversary and slow down its reaction time in the beginning of the war. Disorganisation of enemy decision-making during the initial period of war is a key element of Russian operational thinking. Targeted killing against the political leadership can also serve a geopolitical goal directly.
– Targeted killings abroad. In the past decades numerous citizens of its own as well as of other states fell victim of Russian targeted killings. The Russian state has carried out such operations for a variety of reasons not only on its territory but beyond the borders too.
– Sabotage attacks against various properties including objects of critical infrastructure could seriously hamper the mobilisation of enemy forces, or undermine public

support for the war. As events of the recent years demonstrated, cyber-attacks are a convenient way to cause serious disruption in vital services such as electricity or water.

– Finally, attacks aimed to stir up social tensions can push the enemy state into a political crisis, lead to regime change and can distract attention and resources to maintain internal order".

This brief analysis may indicate that Russia has been preparing to use these doctrines in all possible and not entirely obvious fields for a long time. The concepts of Messner or Gerasimov, as well as many other lesser-known authors, show that terrorism in the Russian concept of warfare did not remain in the so-called grey zone of operations (below the threshold of war), but it was used in a full-scale war with Ukraine in 2022. Russia's hybrid actions in 2014 showed that among potential military and non-military threats, terrorist actions used during line-of-battle (conventional) warfare would play an important role. NATO has repeatedly stressed that Russia's aggressive actions threaten Euro-Atlantic security; terrorism in all its forms and manifestations remains a constant threat to all (Brussels Summit…, 2021)[3].

Results

The Russian annexation of Crimea and occupation of the Donbas region until the full-scale war in Ukraine was a model pattern of hybrid warfare, using activities below the threshold of war, such as subversion, cyber-attacks, conventional military interventions, and military exercises for deterrence and coercion, all done under cover. The situation has changed dramatically with the launch of a full-scale war on February 24, 2022, in which terrorism is used in combat operations. At this stage, it is still difficult to say unequivocally whether these actions are complementary or in line with the concepts of Gerasimov et al. and therefore preceding or fronting. There is no doubt that the Russian military's attacks on civilian objects and defenceless residents of Ukraine should be counted as acts of terror at any level, but for this study, open-source attacks officially designated as acts of terrorism (both planned and conducted) were analysed. Data was collected through May 28, 2022.

Discussion

As a result of the analysis, it can be concluded that three indicators characterise acts of terrorism used in the hybrid war in Ukraine. The first indicator is attacks planned and carried out by the occupying forces. Their purpose was to intimidate the civilian population and influence the Ukrainian authorities and the international community. As a result of these attacks, at least dozens of people were killed, and dozens more were wounded. Accord-

[3] https://www.nato.int/cps/en/natolive/topics_50090.htm

ing to the Global Terrorism Index 2022 (GTI), Ukraine was ranked 62nd, with an index of 2,304/10 (the algorithm assumes four indicators: incidents, fatalities, injuries and property damage), which means that terrorism in the country until the outbreak of the war did not have a significant impact. However, as the report points out in key trends, the conflict in Ukraine will increase traditional and cyber terrorism, reversing the previous situation in the region (Institute for Economics & Peace, 2022).

The second indicator is the trend indicating so-called false flag (in this case, Ukrainian) attacks. Such actions are most likely to gain public support for waging a full-scale armed conflict. According to an open source, before Russia attacked Ukraine, it and pro-Russian separatists carried out a series of provocations to provide a pretext for intervention. On Tuesday, February 22, 2022, the Donetsk People's Republic news agency reported that three people were killed in two car explosions. Separatists blamed the incident on Ukrainians who allegedly planned to bomb a military leader but blew up two civilian cars due to a mistake. The story thus created was published on Twitter by, among others, Dean O'Brien, an American who takes an active part in spreading Russian disinformation content. He called the event a "terrorist attack by Ukrainian armed forces" and presented it as an argument for Russian intervention in Ukraine: "People in the west must understand that this is why Russian peacekeepers are needed here". However, journalists from the BBC station and the independent blog glasnostgone.net have clarified what suggests that the whole event was crafted by the separatists and deliberately presented as a Ukrainian attack[4]. According to the Centre for Eastern Studies analysis, Russia's Secret Service has long since embarked on a disinformation operation to create the impression that Ukraine is planning terrorist acts on Russian territory. The Federal Security Service revealed a six-person "group of Ukrainian nationalists" that aimed to kill leading Russian propagandists (Vladimir Solovyov, Dmitry Kiselyov, Margarita Simonian, Olga Skabieeva). After the revelation of reports about the allegedly planned assassinations, Chairman of the State Duma of the Russian Federation Vyacheslav Volodin demanded that Ukraine be recognised as a terrorist state. According to the authors, this is intended by Russia to support the thesis of an aggressive policy of Kyiv, which allegedly does not seek to resolve the conflict. Attention is also drawn to the fact that on the territory of the regions bordering Ukraine, a state of high terrorist threat is maintained, and mysterious incidents involving the destruction of critical infrastructure have occurred there (including a fire at the fuel depot in Bryansk)[5].

The third indicator (so far, the only one formally indicated) is self-conducted terrorist attacks. Based on a single event, it is not easy to define whether this is a broader trend or just an episode of a Dnieper resident. Perhaps it is important to note the sequence of dates

[4] https://konkret24.tvn24.pl/swiat,109/falszywe-eksplozje-ataki-rakietowe-i-naruszenia-granic-jak--rosja-przygotowala-preteksty-do-ataku,1097385.html

[5] https://www.osw.waw.pl/pl/publikacje/analizy/2022-04-26/atak-rosji-na-ukraine-stan-po-61-dniach

from which it appears that on April 19, 2022, IS called, among others, the so-called "lone wolves" to fight and the planned attack was revealed by open sources on May 12, 2022.

Conclusion

The security environment, especially in Eastern Europe, was significantly affected already in 2014 but radically changed with the full-scale war in Ukraine in February 2022. Many authors have described Russia's actions in Ukraine as hybrid warfare. It is because the tactics use a wide range of unconventional combat methods, including terrorism. In the analysis, it has been shown that terrorism is an asymmetrical tactic integral to hybrid warfare. The consequences of this type of action are much more extensive and dynamic than acts of terrorism in peacetime conditions. Analysing international and regional counter-terrorism strategic documents, one must conclude that although they speak of hybrid threats and terrorism, they refer to conditions of peace rather than war. In many of these studies, counter-terrorism is identified in the context of peace-oriented integrated actions undertaken by local or global institutions responsible for counter-terrorism security. These actions aim to reduce the likelihood of a terrorist attack and minimise the consequences once it has occurred. The anti-terrorist security strategies created based on legislation and formal recommendations recommend protective tactics in conditions similar to the source documents. This state of affairs already seems inadequate. Taking the scale of potential attackers and operations in combat settings and relating it to the scale of attackers in civilian settings, the differences seem radical and disproportionate. In each of these settings, civilians are most often the targets of acts of terrorism. While there are many terrorism sensitisation programmes and campaigns in most countries, they are not more applicable in a hybrid war environment, where the sequence of threats is much more extensive and dynamic. To consider that civilians under conditions of disinformation, psychological warfare, cyber-attacks, lack of external communications, conventional attacks and terrorist attacks overlaid on top of all this will be able to apply a counter-terrorism algorithm prepared under conditions of peace seems at least a far-fetched illusion. Integrated such actions significantly degrade the ability to adequately respond to the terrorist threat. Therefore, there is an urgent need to analyse the war in Ukraine to draw conclusions for the entire international community at both strategic and operational levels.

References:

Bilal, A. (2021). Hybrid Warfare - New Threats, Complexity, and 'Trust' as the Antidote. *NATO Revue*. https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

Brussels Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels. (2021, June 14). https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en

Giles, A. (2020). Valery Gerasimov's doctrine from Soviet armor officer to strategic mastermind? DOI: 10.13140/RG.2.2.10944.35848

Hoffman, F. (n.d.). Conflict in the 21st Century: The Rise of Hybrid Wars. *Potomac Institute for Policy Studies*, 10–14. potomacinstitute.org

Institute for Economics & Peace. (2022). *GLOBAL TERRORISM INDEX. MEASURING THE IMPACT OF TERRORISM*. https://www.visionofhumanity.org/wp-content/uploads/2022/03/GTI-2022-web_110522-1.pdf

Mumford, A. (2016). *The Role of Counter Terrorism in Hybrid Warfare, A report prepared for NATOs Centre of Excellence for Defence Against Terrorism (COE DAT)*. https://www.tmmm.tsk.tr/publication/researches/04-TheRoleofCounterTerrorisminHybridWarfare.pdf

Mumford, A. (n.d.). *A report prepared for NATOs Centre of Excellence for Defence Against Terrorism*. tmmm.tsk.tr.

NATO's response to hybrid threats. (n.d.). https://www.nato.int/cps/en/natohq/topics_156338.htm

Operation Crimea Anno Domini 2014. (n.d.). ka.edu.pl

Skoneczny, Ł. (n.d.). Hybrid warfare - a challenge of the future? Selected issues. *Internal Security Review*, 39–45.

Solmaz, T. (2022, April 27). Conventional Warfare versus "Hybrid Threats". *Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/conventional-warfare-versus-hybrid-threats-example-either-or-fallacy

Terrorism Threat During Peer-to-Peer Conventional War - A Background Study. (n.d.). tmmm.tsk.tr

The European Commission. (2016). *Joint Communication to the European Parliament and the Council Joint Framework on countering hybrid threats a European Union response. FAQ: Joint Framework on Countering Hybrid Threats*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018;https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_1250

Varga, T. C., Jójárt, K., Rácz, A., & Tálas, P. (2022). Terrorism Threat During Peer-to-Peer Conventional War A Background Study. *Defence Against Terrorism Review, 14*. https://www.tmmm.tsk.tr/publication/datr/volumes/datr14.pdf

Валерий, Г. (2013). *Ценность науки в предвидении*. [Valery, G. (2013). *The value of science in foresight*]. https://vpk-news.ru/articles/14632

Конышев, В., & Парфенов, Р. (2019). Гибридные войны: между мифом и реальностью, Мировая экономика и международные отношения. [Konyshev, V., & Parfenov, R. (2019). Hybrid wars: between myth and reality]. *World economy and international relations, 63*(12), 56–66. https://www.imemo.ru/en/index.php?page_id=1248&file=https://www.imemo.ru/files/File/magazines/meimo/12_2019/08-KONYSHEV.pdf

Tables:

Table. 1. Planned attacks – officially designated as terrorist

City	Date	Purpose	Method	Injured	Victims	Source
Kharkov	22.02.2022	Orthodox Churches of the Moscow Patriarchate	n.a.	n.a.	n.a.	SBU [20]
Chernobyl	11.03.2022	Nuclear power plant	n.a.	n.a.	n.a.	Ukrainian Supreme Council [21]
Russian towns	12.04.2022	Homes, Schools, Hospitals,	gunfire	n.a.	n.a.	Head of the Main Intelligence Directorate of the Ministry of Defense of Ukraine [22]
n.a.	25.04.2022	Children returning from school	n.a.	n.a.	n.a.	SBU [23]
Territory of Russia or Belarus	01.05.2022	Passenger aircraft	Stinger launcher	n.a.	n.a.	SBU [24]
Zaporozhye	12.05.2022	City centre	Self-prepared load reinforced with a load of nails	n.a.	n.a.	SBU [25]

Source: own elaboration based on open sources.

Table 2. Realised attacks – officially defined as terrorist acts

City	Date	Purpose	Method	Injured	Victims	Source
Kharkov	01.03.2022	Freedom Square	Self-steering rocket	6	dozens	President of Ukraine [26]
Kramatorsk	08.04.2022	Railroad station-evacuation node	Missile attack/ cluster munitions	87	39	Governor of Donetsk Oblast [27]
Region Koreński	13.04.2022	Russian border guards	gunfire	n.a.	n.a.	Governor of Kursk Region [28]
Bryansk Region	14.04.2022	Border crossing point	gunfire	n.a.	n.a.	FSB [29]
Trans-Dnieste	25.04.2022	Building of the Ministry of Security	gunfire	n.a.	n.a.	Interfax [29]
Parkans	26.04.2022	Military unit	gunfire	n.a.	n.a.	Security Council of the separatist Transnistria [30]
Majac	26.04.2022	Radio Towers	Explosive charges	n.a.	n.a.	Administration of Dnieste [30]

Source: own elaboration based on open sources.