Europejski Przegląd Prawa i Stosunków Międzynarodowych
Europejska Wyższa Szkoła Prawa i Administracji w Warszawie

nr 3/2024/71

Ewa Jakubiak*

Legal Implications of the Hybrid Warfare on the Polish-Belarusian Border

> *We rarely use weapons to kill people to take their country.*
> *The cleanest way is blackmail, demoralisation, bribery,*
> *lies and intimidation of politicians and the media,*
> *and they will destabilise and break up their country for us.*
> *Then all that remains to be done*
> *is to arm pro-communist or simply criminal factions,*
> *and we have another coup d'état and another "liberated" country. How clean it is.*[1]

[Konsekwencje prawne wojny hybrydowej na granicy polsko-białoruskiej]

Abstrakt

Termin wojna hybrydowa nie ma spójnej definicji, ale ogólnie odnosi się do dających się zaprzeczyć i tajnych działań, wspieranych przez groźbę lub użycie sił konwencjonalnych lub nuklearnych, w celu wywarcia wpływu na politykę wewnętrzną krajów docelowych. Niektórzy autorzy używają tego terminu, aby odnieść się tylko do nieregularnych taktyk, inni używają hybrydy, aby opisać szereg nieregularnych i konwencjonalnych taktyk stosowanych na tym samym polu bitwy, a inni używają tego terminu do opisania doktryny wojny nowej generacji sformułowanej przez najwyższe kierownictwo rosyjskiego sztabu generalnego. Wielu autorów krytykuje ten termin jako pozbawione znaczenia, modne lub chwytliwe hasło, które w niewielkim stopniu pomaga nam zrozumieć specyfikę zagrożenia ze strony Rosji. Ocena teorii i praktyki działań prowadzonych przez Białoruś wskazuje, że pojawiła się nowa generacja wojny. Niektóre przykłady obejmują: cyberataki, ingerencje w wybory, a także kampanie dezinformacyjne, w tym prowadzone w mediach społecznościowych.

Przedstawiono podstawowe cechy wojny hybrydowej, odnosząc się do przypadku Rosji i Białorusi. Dla Rosji i Białorusi wojna hybrydowa to okazja do wywierania politycznego wpływu, a dla grup przestępczych – łatwy zarobek.

Celem artykułu jest ukazanie następstw wojny hybrydowej na granicy polsko- białoruskiej.

Słowa kluczowe: wojna, hybryda, dezinformacja, propaganda, granica.

* **Ewa Jakubiak** – PhD, University of Lomza (affiliation), Vice-dean of the Faculty of Law and Administration, mediator / dr nauk społecznych, Akademia Łomżyńska (afiliacja), prodziekan Wydziału Prawa i Administracji, mediatorka, https://orcid.org/0000-0002-7849-2880; ejakubiak@al.edu.pl.

[1] Y. Bezmenow, Love Letter to America, Los Angeles 1984, p. 36.

Introduction

War is, therefore, an act of violence;
violence is armed with inventions of Science and Technology.
It is accompanied by limitations, weak and little noticeable,
called the provisions of International Law, which violence imposes on itself,
But it is worth talking about them because they pose little threat to its capabilities.[2]
Carl von Clausewitz

The term "hybrid warfare" became the term that dominated the current forms of armed conflict. Russia's way of annexing Crimea and its involvement in the armed conflict in eastern Ukraine contributed to its significant popularisation. When it turned out that neither Ukraine nor the Russian Federation declared participation in the war and did not formally declare a state of war, the world began to wonder about the type of conflict conducted there. In recent years, hybrid warfare has become a new but controversial term in academic and political book positions to suggest a kind of combination of different military and non-military means and methods. Warfare is increasingly based on irregular and unconventional elements, which, on average, represent lower quality, ethical standards, and morale. This makes waging war less professional and more unpredictable.

According to F. G. Hoffman, hybrid warfare is characterised by physical. and psychological, kinetic and non-kinetic convergence of fighters and civilians, armed forces and communities, states and non-state actors, and the combat capabilities with which they are equipped.[3]

As noted by M. Piotrowski, the definition of hybrid warfare was included in the doctrinal documents of the largest countries, including the National Military Strategy of the United States in 2015.[4] There is no agreed definition of hybrid warfare in the literature. Such a war is conducted in the "grey zone" of the conflict, which means that operations must not clearly cross the threshold of war. This may be due to the ambiguity of international law, the ambiguity of actions and attribution, or the fact that the impact of actions does not justify a response. Hybrid warfare is associated with the chief of the Russian General Staff, Valery Gerasimov, the author of the so-called Gerasimov Doctrine - a government-wide concept that combines hard and soft power in many areas and crosses the boundaries between time and peace. The Gerasimov doctrine is not the driving force of Russian foreign policy. Still, it attempts to develop an

[2] C. von Clausewitz, O naturze wojny [About the Nature of War], Warsaw 2006, p. 16.

[3] B. Pacek, Wojna hybrydowa na Ukrainie [Hybrid Warfare in Ukraine], Warsaw 2018, p. 10.

[4] M. Piotrowski, Konflikt nie jest prosty: amerykańska teoria i doktryna wojen oraz przeciwników hybrydowych [Conflict is Never Simple: American theory and doctrine of wars and hybrid opponents], „Sprawy Międzynarodowe" [International Affairs] 2015, 2, p. 21.

operational concept of Russia's confrontation with the West, supporting the current doctrine that has guided Russian policy for more than two decades: the Primakov doctrine. The Gerasimov doctrine creates a framework for these new tools and declares that non-military tactics are not auxiliary to using force but are the preferred way to win.[5]

The Concept of Hybrid Warfare in Legal Acts and Literature on the Subject

In the literature on the subject, there are many discussions about the evolution of modern war. It has become possible to simultaneously use a variety of strategies that are both conventional and unconventional in nature. After all, the hallmark of hybrid warfare is that it is not limited to the traditional battlefield or the use of heavy weapons and military operations.

A characteristic feature of hybrid warfare is its multidimensional nature and the fact that it can take various forms in parallel. These may include media and commercial channels that are used to exploit the target country's internal and external weaknesses.[6]

Western countries are democratic in human rights and the international legal order. However, they have proved helpless in the face of Russia's readiness to appropriate these concepts in its service. Hybrid warfare makes defence planning difficult.[7] It requires a revision of military doctrines and a greater focus on non-military threats.

So far, there has not been a universal definition of hybrid warfare (in the international dimension) that would be acceptable to all theoreticians and practitioners. Each definition leads to a debate on whether the term is useful. It can be stated that hybrid warfare is a set of military and non-military activities of a non-standard, complicated nature. Its opponent is difficult to define precisely and is variable in nature. Hybrid activities use a combination of conventional and unconventional methods. The ability to apply ambiguity provides the attacker with a plausible denial and obfuscation of the fact that an attack is taking place.

The formula of the hybrid warfare in Ukraine and the Gerasimov doctrine launched a discussion on the military power of Russia, the state and impor-

[5] M. Pietraś, *Bezpieczeństwo państwa w późnowestfalskim środowisku międzynarodowym* [State Security in the Late Westphalian International Environment] (in:) Kryteria bezpieczeństwa międzynarodowego państwa [Criteria for the security of the international state], (ed.) S. Dębski, B. Górka-Winter, Warsaw 2003, p. 112.

[6] A. Bryc, Rosja w XXI wieku. Gracz światowy czy koniec gry? [Russia in the 21st Century. World player or game over?], Warsaw 2009, p. 98.

[7] M. Depczyński, Rosyjskie siły zbrojne [Russian Armed Forces], Warsaw 2015, p. 101.

tance of conventional forces, the ability to project power, the state and scope of non-military instruments that, as part of the synergy effect, can support military ones, with particular emphasis on the role of propaganda.

In recent years, NATO and the EU have taken on greater responsibility for countering hybrid threats. This group of threats includes a wide range of hostile methods used by states and non-state actors. As mentioned earlier, this includes both military and non-military activities, such as special forces operations and irregular warfare, as well as disinformation and cyber-attacks. NATO and the EU are committed to facilitating international cooperation in countering hybrid threats and protecting their structures and institutions. In this way, both organisations strengthen their efforts at the national level, as the fight against hybrid threats is primarily the task of the Member States. Nevertheless, NATO and EU activities in this area are limited by insufficient financing and the reluctance of the Member States to improve the exchange of intelligence and sensitive information, e.g. related to the protection of critical infrastructure or cybersecurity.

According to NATO, hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, the deployment of irregular armed groups and the use of regular forces. They are designed to blur the lines between war and peace and sow doubt in the minds of the target populations. Therefore, hybrid threats should be treated as a collective concept encompassing various destabilising activities. On the one hand, this vague definition can impress the security debate. On the other hand, it may be conducive to discussion because individual states can bring their priorities to the security agenda. Taking into account hybrid threats includes not only kinetic operations, such as the use of troops without insignia, actions against critical infrastructure, and organising coups or assassinations ordered by foreign intelligence agencies, but also non-kinetic measures – for example, a wide range of disinformation and propaganda activities, sponsoring radical political movements, exerting economic pressure or clandestine activities aimed at destabilising other countries (including corruption of politicians). The main responsibility for countering hybrid threats lies with NATO and EU Member States. Only governments have adequate resources for this in the form of intelligence and counterintelligence agencies (civilian and military), uniformed services (ensuring public order and security), means of communication with citizens and the ability to respond to cyber incidents. In addition, national authorities are closer to potential threats than international organisations. This, combined with a shorter decision-making process, makes them more capable of dealing with hostile hybrid operations.

NATO and the EU intervened in the fight against hybrid threats mainly in response to the increased risk of terrorist attacks related to the emergence of the Islamic State, the development of information warfare, increasing foreign interference in elections (primarily from Russia) and always more harmful cyber-attacks.[8] Both organisations focus on protecting their structures, decision-making processes, and infrastructure in countering hybrid threats. In relation to NATO and EU Member States, they play supporting and coordinating roles (e.g. in ensuring common situational awareness), which means involvement in areas where national actions have proved ineffective or insufficient. NATO and the EU strive to develop international cooperation in counteracting hybrid threats (including NATO–EU cooperation), which is hindered by Member States' diverse perceptions of threats. This translates into their commitment to facilitating the exchange of experience, deepening knowledge about hybrid threats, and conducting international exercises covering hybrid scenarios. In addition, the organisation sets common standards and minimum requirements for its Member States regarding resilience against hybrid threats (to eliminate national weaknesses affecting European and transatlantic security). This applies to, among others, cybersecurity, prevention of money laundering and protection of critical energy infrastructure.[9]

To counter the military aspects of hybrid threats (such as irregular warfare), NATO has strengthened its intelligence capabilities and increased the readiness of NATO's Response Force (NRF) through the creation of the Very High Readiness Joint Task Force (VJTF). In the non-military dimension, NATO gives priority to cybersecurity. NATO's assistance to the Member States in responding to hybrid activities includes monitoring and analysing, sharing intelligence and experience, and providing common situational awareness. An important event in this field was the creation of a new branch of hybrid threat analysis (including cyber threats) in the structure of the Joint Intelligence and Security Division at NATO Headquarters, as well as strengthening cooperation between civilian and military intelligence. It was part of a broader reform of NATO intelligence carried out in 2017. The task of the hybrid branch was a comprehensive analysis of transatlantic security challenges, covering various military and non-military aspects of hybrid threats. However, this was only the first step towards increasing common situational awareness with regard to hybrid threats. NATO does not have its own intelligence services and, therefore, relies on intelligence provided by national agencies. In addition, the Member States are still reluctant to share intelligence within NATO. This is due to their lack of mutual trust and concerns about data security and classified information.

In 2018, NATO created anti-hybrid support teams consisting of experts specialised in assisting members struggling with hostile hybrid action. This

[8] A. Włodkowska-Bagan, Zaufanie w stosunkach międzynarodowych – *theoria et praxis* [Trust in International Relations: *theoria et praxis*], „Stosunki Międzynarodowe – International Relations" 2016, Vol. 52, 3, p. 19.

[9] A. Podraza, Promocja demokracji a bezpieczeństwo europejskie: skuteczność i dylematy polityki wschodniej Unii Europejskiej w XXI wieku [Promotion of Democracy and European Security: Effectiveness and dilemmas of Eastern European Union Policy in the 21st century], 2016, 2, p. 5.

mechanism was launched for the first time in 2019 by Montenegro. These extraordinary measures were motivated by Russia's efforts to destabilise Montenegro, including the 2016 coup attempt. The team's mission focused on the necessary changes in legislation and cybersecurity.

Perhaps other Member States have not experienced large-scale hybrid activities that would require the help of NATO experts. An alternative explanation, however, may be a reluctance to reveal the weaknesses of their defence systems or doubts about the prospects of receiving timely and well-suited assistance. NATO plays a triple role in cyberspace. It motivates allies to invest more in cybersecurity, serves as a platform for information exchange and training, protects its networks, and supports the security of Member States' networks. In 2016, NATO committed to cyber defence to strengthen the capabilities necessary for cyber defence of national infrastructures and networks. They also mentioned the need to allocate adequate resources to cyber defence without setting a NATO target level for cyber spending as a share of the defence budget.

Hybrid threat perspectives combine conventional and unconventional military and non-military activities that can be used and coordinated by state or non-state actors to achieve specific policy objectives.[10]

The EU emphasises the multidimensional nature of hybrid threats, which range from "cyber-attacks on critical information systems, through disruption of critical services such as energy supply or financial services, to undermining public trust in government institutions or deepening divisions."[11] They are directed against "critical weaknesses" and use "coercive and subversive means", are "difficult to detect or attribute" and are designed "to create confusion to hinder quick and effective decision making."[12]

The EU is increasingly concerned about hybrid threats. Since 2014, it has adopted more than 20 different documents in this field (on counteracting weapons of mass destruction, ensuring the security of energy supply, controlling direct foreign investments, maritime security, data protection, border protection, space security and others). In addition, the EU is developing its Critical Infrastructure Protection Programme embedded in the 2008 European Critical Infrastructure Directive. However, in recent years, the EU has decided to put situational awareness, cybersecurity and disinformation at the heart of its efforts to counter hybrid threats.

[10] https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2020-04-24/nato-i-unia-europejska-wobec-zagrozen-hybrydowych [accessed: 4.12.2023].

[11] https://repozytorium.amu.edu.pl/bitstream/10593/24833/1/Cyberterroryzm%20w%20policy%20safety%C5%84stw%20pa%C5%84stw.%20Problems%20ochrony%20infrastruktury%20krytycznej%20-%20Robert%20Maciejewski.pdf [accessed: 20.12.2023].

[12] https://repozytorium.amu.edu.pl/bitstream/10593/24833/1/Cyberterroryzm%20w%20policy%20safety%C5%84stw%20pa%C5%84stw.%20Problems%20ochrony%20infrastruktury%20krytycznej%20-%20Robert%20Maciejewski.pdf [accessed: 20.12.2023].

Hybrid threats refer to a wide range of methods or actions used by a hostile state or non-state actors in a coordinated manner to combat the weaknesses of democratic states and institutions while remaining below the threshold of a formally declared war. Some examples include cyber-attacks, election interference, and disinformation campaigns, including those on social media. The conclusions call for a comprehensive approach to security to counter hybrid threats, operating in all relevant policy sectors more strategically, coordinated and coherently. To ensure the coherence of this work, the EU and NATO call for strengthening resilience to hybrid threats across different policy areas, for example, when developing and exploiting new and emerging technologies, including artificial intelligence and data collection techniques, as well as when assessing the impact of foreign direct investment or future legislative proposals.

The scope of the EU's and NATO's fight against hybrid threats covers a fairly wide area, from the fight against disinformation campaigns to the identification and prevention of crises or conflicts (including those of an armed nature). Finally, in 2018, The EU Council and the North Atlantic Council endorsed a joint set of 74 concrete security actions, 20 focusing on combating hybrid threats.[13]

The security of the EU and NATO are intertwined, which means that Member States cooperate and effectively use the wide range of tools and resources available to meet the challenges and increase the security of their citizens. EU–NATO cooperation is an integral pillar of the EU's efforts to strengthen Europe's security and defence capabilities. The partnership between the two organisations strengthens the transatlantic bond, and EU defence initiatives contribute to equal military involvement in Europe with the help of NATO forces. In other words, a stronger EU and a stronger NATO strengthen each other.

Currently, eight key areas require progress in EU–NATO cooperation:[14]

- counteracting hybrid threats,
- operational cooperation – especially at sea, in the face of increased migration,
- cybersecurity,
- defence capability,
- arms industry,
- scientific research in the field of security, technology and military,
- joint exercises and training,
- support for allied countries in the east and south of Europe as part of the partnership. Cooperation shall be based on established standards and good practices, guided by the principles of openness, transparency, communication and reciprocity while fully respecting the decision-making autonomy and procedures of both organisations and preserving the character of the security and defence policy of individual Member States.

[13] https://www.consilium.europa.eu/pl/policies/defence-security [accessed: 21.12.2023].

[14] https://www.consilium.europa.eu/pl/policies/defence-security [accessed: 21.12.2023].

Hybrid threats, i.e. hybrid activities carried out, are understood as a combination of regular and irregular activities (i.e. of varying intensity and frequency), both by the armed forces and by criminals, terrorists and even political organisations. Such a new form of threat, or rather its diverse nature, indicates the need to verify the ability of countries to respond to such threats. This is primarily related to the activities of governments, the efficiency of defence systems and international cooperation in the field of security.

It should be noted that the costs of conducting irregular attacks, referred to as hybrid actions, are much lower than in the case of traditional warfare. Moreover, the attacker is not, at least not entirely, exposed to a strong response from the international community.

Border Conflict Between Poland and Belarus

The hybrid conflict on the Polish-Belarusian border is part of the evolution that takes place in the post-Soviet countries (as is currently the case, for example, Azerbaijan and Armenia). It is a multidimensional crisis, consisting of the activities of national and supranational entities pursuing their political and economic interests using available methods, from the conventional use of armed forces to disseminating false news.

The current situation on the border between Poland and Belarus contains all the signs of a border conflict. This applies to foreigners who, through the Belarusian authorities, enter Poland’s eastern border, seeking to cross it illegally. Media reports indicate that the regime of Aleksandr Lukashenko artificially caused this whole situation. Therefore, the Polish government undertook several actions to seal the border between Poland and Belarus.

The activity of the Lukashenko regime on the eastern border of Poland fits into the catalogue of hybrid warfare activities. An example is the widespread use of civilians, including women and children, to achieve political objectives. Provocation by Belarusian services in which migrants are used are non-military activities and are aimed at destabilising the internal situation of Poland and the European Union.

The conflict began in mid-May 2021 when the Lithuanian Border Guard began noting the intensification of attempts by Belarus to illegally cross the border. The Belarusian authorities have engaged state-owned companies in transporting migrants to Belarus from countries such as Iran, Iraq, and Syria, their accommodation on the spot and transport to the border of the European Union. Belarusian services supported the migrants. Belarus aimed to present Poland, Lithuania and Latvia on the international arena as countries unwilling to accept refugees and migrants. In addition, forcing the three eastern flank states to increase the efforts of state services to protect the borders has an impact on public sentiment and partially diverts attention from Russian actions, e.g. in the vicinity of Ukraine and the South Caucasus.

One of the hybrid actions on the Polish-Belarusian border was an attempt by the Belarusian authorities to lower Poland's image and public trust in uniformed services protecting the border, including primarily the army. The aim of the disinformation war was also to influence the societies of other EU countries, which was aimed at weakening the image of Poland. The message focused mainly on the brutality of border services and victims among migrants. The Belarusian migration and border crisis is a hybrid warfare level conflict, which does not reach the level of an active armed conflict. Still, its trends consistently pose a threat to the security environment in Central Europe. Earlier, Lukashenko's government simplified visa regulations, thanks to which he could bring more people to Europe. Walls and barriers were created on the border. The research conducted by IBRIS for the Republic of Poland shows that 55.4% of respondents strongly agree with the statement that the crisis on the Polish-Belarusian border is an element of the hybrid warfare that Lukashenko is waging. In addition, 30.5% rather agree with this opinion.[15]

Poland's border with the Republic of Belarus is 418.24 km. Currently, despite the wall on the border, there are still attacks on Polish patrols on the border with Belarus. When Border Guard officers and the army patrol the areas by the metal fence, the migrants attack the border guards. However, in cooperation with the army, the Border Guard keeps its finger on the pulse; only on 1–3 December 2023 did it thwart as many as 64 attempts to cross the Polish border illegally. According to data from the Border Guard, since the beginning of 2023, there have been more than 25,500 attempts to cross the Polish-Belarusian border illegally. The construction of a dam on the 186 km border with Belarus and the installation of an electronic barrier significantly reduced the migratory pressure artificially created in 2021 by the regime of Alexander Lukashenko. In August 2021, in the period preceding the peak of the migration crisis, more than 3,500 attempts to illegally cross the Polish-Belarusian border were recorded. In August of 2023, The Border Guard registered 2,800 of them.

The Polish barrier not only makes it difficult for migrants to cross the border illegally but also facilitates the guards' work. It is possible thanks to the electronic barrier consisting, among others, of motion sensors and cameras over a length of 206 km. Not only migrants but also smugglers and Belarusian services are gathering in the vicinity of the dam. Therefore, in this situation, the dam also increases the security of Polish patrol members, although attacks on guards and soldiers are becoming more frequent.

[15] https://wiadomosci.wp.pl/sondaz-solidny-mur-rozwiazaniem-kryzysu-na-granicy-6692921765182080a [accessed: 27.12.2023].

Conclusion

The European Union defined hybrid threats as a combination of forced and subversive actions, as well as conventional and unconventional methods (i.e. diplomatic, military, economic, technological) that can be used in a coordinated way by state or non-state actors to achieve specific goals, remaining below the threshold of a formally declared war.

NATO sees threats and hybrid warfare as a brutal conflict that is characterised by the simultaneous use of conventional and irregular tactics that can involve both states and non-state actors that are used seamlessly, disregarding the limitations of the physical battlefield or territory.

Each attack combines the two and aims at aspects of the state and society to achieve its goals. The nature and tools required to wage hybrid warfare make no distinction between state and non-state actors, with non-state actors (such as extremist groups) being as capable of waging such a war as a state actor and its armed forces can be.

Both the North Atlantic Treaty Organisation and the European Union carry out several activities in countries where their presence is essential for maintaining order and security. Thus, considering two types of military missions – those carried out by both NATO and the EU – threats can be counteracted simultaneously. The forces and resources of the two international organisations differ significantly and can, therefore, be used to complement each other and ultimately eliminate hybrid threats. These operations are also important from the point of view of communication. They play a key role in the fight against disinformation and in verifying the credibility of information in networks regarding the actual state of affairs in conflict regions. Due to the international nature of hybrid threats, including terrorism, it is important to emphasise the role of civilian and military missions. For this reason, joint missions are an inevitable element of further cooperation between NATO and the European Union. Only the cooperation of these two organisations will make it possible to fight threats more effectively and minimise the risk of their spread.

The term “hybrid threats” has questionable conceptual value. Various definitions have joined it, and other terms such as “non-linear warfare,” “asymmetric conflict,” and “subversion” also compete with it. In short, “hybrid threats” refer to the exploitation of state-sponsored but not officially affiliated (which can be denied) actors who do not resort to physical violence.

The purpose of hybrid threats is to force the threat object to meet the strategic interests of the aggressor. There is a hidden warning against the use of force behind such threats.[16]

[16] J. Kranz, Kilka uwag na tle aneksji Krymu przez Rosję [Some Remarks Against the Background of Russia’s Annexation of Crimea], Państwo i Prawo [The State and the Law] 2014, 8, p. 56.

Hybrid tricks have been used throughout history, from the Trojan Horse invented by Odysseus to the Trojan malware written by today's hackers. Indeed, even periods of peace are "hybrid," punctuated by assassinations, corruption, espionage, disinformation, manipulation and economic pressure. Public debate on hybrid threats focuses on fake news, information warfare, and social media manipulation. This remark is understandable: fake news is the most visible element of a hybrid campaign. However, how states use undisclosed and unassigned assets to weaken adversaries goes far beyond these elements. Disinformation is rarely an end in itself but rather a preparatory stage for further subversion.[17] Combining NATO's military capabilities with the political and economic potential of the European Union is a project that can fully ensure Europe's security, as well as play a significant role in the Middle East and Africa. This is due to the different nature of the two organisations and the multinational commitments made by their individual members. As indicated earlier, the essence of hybrid threats requires an immediate and collective response, which can only be achieved with the significant involvement of many actors. Here, international military missions deserve special attention.[18]

Abstract

The term hybrid warfare does not have a consistent definition. Generally, it refers to deniable and secret activities supported by the threat or use of conventional or nuclear forces to influence the internal policies of the target countries. Some authors use the term to refer only to irregular tactics, others use the hybrid to describe several irregular and conventional tactics used on the same battlefield, and others use the term to describe the doctrine of next-generation warfare formulated by the top leadership of the Russian General Staff. Many authors criticise this term as meaningless, fashionable, or catchy, which does not help us understand the specificity of the threat from Russia. An assessment of Belarus's theory and practice of actions indicates that a new generation of war has emerged. Some examples include cyber-attacks, election interference, and disinformation campaigns, including those on social media.

The basic features of hybrid warfare are presented, referring to the case of Russia and Belarus. For Russia and Belarus, hybrid war is an opportunity to exert political influence, and for criminal groups – easy money.

The purpose of the article is to show the consequences of hybrid warfare on the Polish-Belarusian border.

Keywords: war, hybrid, disinformation, propaganda, border.

[17] J. Kranz, Kilka..., p. 57.

[18] *Ibid.*

BIBLIOGRAPHY

Bezmenow, Y., Love Letter to America, Los Angeles 1984.

Bryc, A., Rosja w XXI wieku, Gracz światowy czy koniec gry? [Russia in the 21st Century. World player or game over?], Warsaw 2009.

Clausewitz C. von, O naturze wojny [About the Nature of War], Warsaw 2006.

Depczyński, M., Rosyjskie siły zbrojne [Russian Armed Forces], Warsaw 2015.

Kranz, J., *Kilka uwag na tle aneksji Krymu przez Rosję* [Some Remarks Against the Background of Russia's Annexation of Crimea], „Państwo i Prawo" [The State and the Law] 2014, 8.

Pacek, B., Wojna hybrydowa na Ukrainie [Hybrid Warfare in Ukraine], Warsaw 2018.

Pietraś, M., Bezpieczeństwo państwa w późnowestfalskim środowisku międzynarodowym [State Security in the Late Westphalian International Environment] (in:) Kryteria bezpieczeństwa międzynarodowego państwa [Criteria for the Security of the International State], (ed.) S. Dębski, B. Górka-Winter, Warsaw 2003.

Piotrowski, M., Konflikt nie jest prosty: amerykańska teoria i doktryna wojen oraz przeciwników hybrydowych [Conflict is Never Simple: American theory and doctrine of wars and hybrid opponents], „Sprawy Międzynarodowe – International Affairs" 2015, 2.

Podraza, A., Promocja demokracji a bezpieczeństwo europejskie: skuteczność i dylematy polityki wschodniej Unii Europejskiej w XXI wieku [Promotion of Democracy and European Security: effectiveness and dilemmas of the Eastern European Union Policy in the 21st century], „Politeja" 2016, 2, 41.

Włodkowska-Bagan, A., Zaufanie w stoskach międzynarodowych – *theoria et praxis* [Trust in international relations: *theoria et praxis*], „Stosunki Międzynarodowe" [International Relations] 2016, Vol. 52, 3.

Online Publications

https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2020-04-24/nato-i-unia-europejska-wobec-zagrozen-hybrydowych [accessed: 4.12.2023].

https://repozytorium.amu.edu.pl/bitstream/10593/24833/1/Cyberterroryzm%20w%20policy%20safety%C5%84stw%20pa%C5%84stw.%20Problems%20ochrony%20infrastruktury%20krytycznej%20-% 20Robert%20Maciejewski.pdf [accessed: 20.12.2023].

https://www.consilium.europa.eu/pl/policies/defence-security [accessed: 21.12.2023].

https://wiadomosci.wp.pl/sondaz-solidny-mur-rozwiazaniem-kryzysu-na-granicy-6692921765182080a [accessed: 27.12.2023].