M. Orzechowski, J. Jartyś, *Annexation of Crimea and federalization of Donbas as the exemplification of hybrid warfare in Ukraine. Implications for Poland*, „Rocznik Instytutu Europy Środkowo-Wschodniej" 18(2020), z. 1, s. 61-78, DOI: https://doi.org/10.36874/RIESW.2020.1.4.

Marcin Orzechowski[*]
Janusz Jartyś[**]

Annexation of Crimea and federalization of Donbas as the exemplification of hybrid warfare in Ukraine. Implications for Poland

Aneksja Krymu i federalizacja Donbasu jako egzemplifikacja wojny hybrydowej na Ukrainie. Implikacje dla Polski

Abstract: In the article, the authors attempted to analyze the actions of the Russian Federation towards Ukraine. The research goal was to justify the hypothesis that in the case of Ukraine, the neo-imperial expansionist strategy in the post-Soviet area is implemented through the deconstruction of statehood as a result of a hybrid war. The authors try to answer the following questions: what consequences can such actions have for Poland and is there a real threat from Russia for the countries of Central Europe?
As a result of the analysis, the authors managed to obtain affirmative answers to the above questions.

Keywords: foreign policy, hybrid warfare, political strategy, international security

Streszczenie: W artykule autorzy podjęli próbę analizy działań Federacji Rosyjskiej wobec Ukrainy. Celem badawczym było uzasadnienie hipotezy mówiącej, iż w przypadku Ukrainy neoimperialna strategia ekspansjonizmu na obszarze poradzieckim realizowana jest poprzez dekonstrukcję państwowości w wyniku wojny hybrydowej. Autorzy starają się odpowiedzieć na pytania: jakie konsekwencje mogą mieć tego rodzaju działania dla Polski i czy istnieje realne zagrożenie ze strony Rosji dla krajów Europy Środkowej?
W wyniku przeprowadzonej analizy autorom udało się uzyskać twierdzące odpowiedzi na postawione wyżej pytania.

Słowa kluczowe: polityka zagraniczna, wojna hybrydowa, strategia polityczna bezpieczeństwo międzynarodowe

[*] Marcin Paweł Orzechowski, PhD, University of Szczecin, Poland, ORCID ID: https://orcid.org/0000-0001-7272-6589, e-mail: orzechowski.martin@gmail.com.

[**] Janusz Jartyś, PhD, University of Szczecin, Poland, ORCID ID: https://orcid.org/0000-0001-5662-7433, e-mail: janujar.eu@gmail.com.

Introduction

This article reflects upon measures taken by Russia against Ukraine as part of a broader political strategy towards the entire post-Soviet area. The Russian foreign policy implemented on the former USSR territory has been dominated by neo-imperial expansionism, which has grown in intensity over the last few years in Ukraine. A tool used to pursue the said strategy is the hybrid war, not by accident referred to as one of the greatest modern-world threats to international security. In their analysis, the authors have attempted to systematize theories reflecting on the notion of hybrid warfare as an approach to international relations with a particular focus on Russia's actions towards its neighboring country falling under this strategic concept. The key hypothesis, which the authors verify in this publication, is the fact that the Russian Federation's strategy against Ukraine is multidimensional and involves the destruction of the enemy on various levels – military, economic, political, information and identity. The conflict in Ukraine is a war that has not been officially declared while the operations in the country are a characteristic mesh-up of classic military methods – mostly irregular armed actions (guerrilla force, sabotage, diversion, terrorist acts), but also the elements of information (propaganda, deception), and economic as well as cyber warfare. However, it is clear that the Russian Federation will not stop after Ukraine's deconstruction as these operations are part of a wider-ranging action against the entire post-Soviet area, without precluding confrontation with the Western states. Therefore, the authors considered it justified to present the implications of the hybrid war for Poland, which, as a country located in the immediate vicinity of these operations, is particularly vulnerable to the Russian Federation's hybrid retaliatory measures.

1. Specific features of the Russian hybrid warfare in Ukraine

At the beginning of the 21st century, the Russian Federation faced many challenges that have impacted its strategic thinking. The search for new concepts as the answer to a growing dissonance between ideas and actions carried out during the early Post-Cold War era and the overcoming of internal crises, typical for the 1990s, has led Russia to re-evaluate its strategic concepts towards the entire post-Soviet area.

Russia was criticized for inciting various conflicts accompanying the process of dissolution of the USSR already in the 1990s. Creating and resolving these conflicts has become, primarily for Russia, a form of a fight for influence and control outside the Russian Federation, which was increasingly often referred to as a "low-intensity conflict".

The specificity of the "low-intensity conflicts" in the post-Soviet area consisted in their "location" within the state and the existence of the so-called transnational links, expressed through different kinds of mediators, mercenaries, advisors, and experts, actively engaged in this type of conflicts, which, in consequence, blurs the distinction between the local and the global in such "low-intensity conflicts."[1] One must remember that the term "low-intensity conflict" was coined in military science in the United States in the late 1970s. It was used to define the actions taken by the USA and revolved around the search for an efficient mechanism to enable military operations in the Third World. It is, therefore, clear that the then definition of low-intensity conflicts had very little to do with the current understanding of the concept and was primarily based on the specificity of the bipolar system in international relations.[2]

For the considerations presented in this article, however, it is justified to refer to the notion of "hybrid warfare", also derived from American terminology describing the ways of conducting military operations.[3] It is believed that the conceptual approach to the specific features of hybrid warfare constitutes a kind of contestation of theories regarding conflicts between subjects of international relations such as the theory of guerrilla counterattacks, "fourth-generation war", "post-industrial war", "global insurrection", "strategic paralysis" or the concept of asymmetrical conflicts.[4] The key here seems to be the assumption that the potential military success does not guarantee the

[1] Z. Brzeziński, *Wielka szachownica. Główne cele polityki amerykańskiej*, Warszawa: Politeja, 1997, pp. 33-34.

[2] M. Pietraś, 'Istota i specyfika konfliktów niskiej intensywności', in: *Konflikt niskiej intensywności w Naddniestrzu*, eds. M. Celewicz, J. Kłoczowski, M. Pietraś, Lublin: Wydawnictwo Instytutu Europy Środkowo-Wschodniej, 2006, pp. 24-25.

[3] A. Palazzo, A. Trentini, 'Hybrid, Complex, Conventional, Fourth-Generation Counterinsurgency. It's Decision that Still Matters Most', *Australian Army Journal*, no. 1, 2010, p. 72.

[4] A. Gruszczak, 'Hybrydowość współczesnych wojen – analiza krytyczna' in: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, eds. W. Sokała, B. Zapała, http://www.bbn.gov.pl/download/1/8755/Hybrydowos___wspolczesnych_wojen_____analiza_krytyczna.pdf [2017-06-17].

achievement of intended goals and interests in the strategic, political, and social dimensions.[5] Sometimes, protracting a conflict, weakening the opponent by, for example, destabilizing the state's political system is of greater added value than ultimate victory. This is the kind of interpretation of hybrid warfare's specificity that prompted the authors to advance a thesis that the Russian Federation implemented a "hybrid warfare strategy" against Ukraine because it increased the chances of maintaining or even enhancing the influence in the country by destroying its territorial integrity and destabilizing its political system.[6] In this case, by adopting the elements of hybrid warfare, the dominant party in the conflict (the Russian Federation) seeks, first of all, to gain a relatively lasting advantage over its opponent to achieve the so-called structural transformation of the space of confrontation, which may manifest itself, among others, in increasing the scale of the conflict's impact on the local and international environment. Said increase may be used as a "bargaining chip", e.g., in mediation, and in the case of the Russian Federation, to underline the position of that country in the post-Soviet area. Hybridization may, therefore, concern both the fighting side (state, non-state actor, irregular armed grouping), and the conflict space, its genesis and nature, i.e., conflict ecosystem.[7]

The hybrid war strategy involves a number of different ways of conducting military activities, both with the use of standard weapons, tactics and irregular formations, and, in extreme cases, terrorist acts.[8] Hybrid wars may be waged by state or non-state actors. In such conflicts, the opponents (states, state-sponsored groups or self-funded actors) try to exploit access to modern military capabilities, including encrypted command systems, support protracted insurgencies (as is the case with pro-Russian separatists in Donbas) that

[5] D.T. Lasica, *Strategic Implications of Hybrid War: A Theory of Victory*, Fort Leavenworth: School of Advanced Military Studies, United Army Command and General Staff College Press, 2009, pp. 11-12.

[6] T.A. Marks, 'Counterinsurgency and operational art', *Low Intensity Conflicts & Law Enforcement*, no. 13, 2005, pp. 168-211.

[7] M. Orzechowski, 'Wojna hybrydowa jako przejaw neoimperialnego ekspansjonizmu w strategii politycznej Federacji Rosyjskiej wobec Ukrainy', *TEKA Komisji Politologii i Stosunków Międzynarodowych*, no. 11/3, 2016, pp. 165-180.

[8] J. Robb, *Brave New War. The Next Stage of Terrorism and the End of Globalization*, Hoboken: Wiley, 2007, pp. 152-164.

employ ambushes, improvised explosive devices and assassinations.[9] Other instruments that may be employed include the possibility of using technologically advanced capabilities, such as cyber financial warfare, which are operationally and tactically targeted and coordinated to achieve synergies in the physical and psychological dimensions of the conflict.[10]

In the case of the conflict in eastern Ukraine, we are dealing with a territorial platform of hybrid war – referring to the nation-state understood in the classic sense and traditional ethnic, clan, or tribal communities permanently living in a given territory. The main purpose of the territorial war is the expansion and maintenance of jurisdiction and administrative control in the area, protection of the borders delimiting the scope of the jurisdiction, enforcement of system founding rules and legal norms on the population domiciled in the area, ensuring public order, and managing natural resources and economic activity.[11]

It should also be noted that in such conflicts, we also deal with the so-called virtual dimension where the "quasi-states" may emerge, devoid of traditional elements of state power, international legal personality, and hierarchical organization. Nevertheless, they still hold effective tools and methods of shaping the international environment, influencing the population, multiplying financial resources, and conducting information campaigns.[12] In the case of the conflict in Ukraine, we are faced with a peculiar "hybrid dualism" for we may observe the occurrence of the elements that are characteristic to both the territorial and virtual dimension. On the one hand, the establishment of the Donetsk People's Republic and the Luhansk People's Republic is to be an embodiment of the abovementioned assurance of public order, and the adopted constitutions of both republics are to act as superior normative acts aimed at enforcing system-founding principles and legal norms

[9] M. Kaldor, *New* & *Old Wars: Organized Violence in a Global Era*, Stanford: University Press, 2001, pp. 5-10.

[10] T. Stępniewski, 'Determinanty wewnętrzne polityki zagranicznej Ukrainy pod rządami Wołodymyra Zełenskiego', *Rocznik Instytutu Europy Środkowo-Wschodniej*, vol. 17, no. 1, 2019, pp. 123-141.

[11] G. Gil, *Upadanie państwa w stosunkach międzynarodowych po zimnej wojnie*, Lublin: Wydawnictwo Naukowe UMCS, 2015, pp. 49-51.

[12] L. Bershidskyy, 'Unreformed Ukraine is in Danger of Becoming a Failed State', *Bloomberg*, 6 November 2015, https://www.bloomberg.com/view/articles/2015-11-06/unreformed-ukraine-is-self-destructing [2018-09-29].

on the population living in this area.[13] On the other hand, it should be remembered that these entities are not recognized by the international community; therefore, it is justified to use the term "pseudo-state" or the above "quasi-state" when referring to both republics.[14]

In recent years, hackers have begun to engage in virtual subversion to demonstrate their abilities but also acting on behalf of some states against others.[15] Russian hackers very quickly made attempts to destabilize Ukraine's ICT systems. In June 2014, the "Snake" virus was found on the government administration servers, which was probably used to spy on and disrupt IT systems.[16] The Russian spy virus attacked 84 public administration websites, including Ukraine's Prime Minister's websites, the defense industry, and the diplomatic service.[17] A month earlier, on the day of the presidential election in May, the Russians carried out a hacker attack on the Central Election Commission's websites. The goal of the attack, claimed by the so-called CyberBerkut,[18] was to remove the election results and thus destabilize the country's situation on the day of the presidential election. The Russian cyber-gang Quedagh is responsible for a few cyberattacks of lesser degree, conducted using the Black Energy malware.[19]

[13] *Konstitucyja Donieckoj Narodnoj Riespubliki* [*Конституция Донецкой Народной Республики*], 30 August 2014, https://web.archive.org/web/20140830221524/http://dnr.today/wp-content/uploads/2014/08/aeAEl.pdf [2019-11-19]; see for example, *Konstitucyja Ługanskoj Narodnoj Riespubliki* [*Конституция Луганской Народной Республики*], 26 December 2014, https://archive.is/BbQdc [2019-11-23].

[14] S. Bachman, H. Gunneriusson, 'Terrorism and Cyber Attacks as Hybrid Threats: Defining a Comprehensive Approach for Countering 21st Century Threats to Global Peace and Security', in: *The Journal on Terrorism and Security Analysys*, 9th edition, Spring 2014, pp. 2-11, http://eprints.bournemouth.ac.uk/21206/1/Terrorism_and_Cyber_Attacks.pdf, pp. 2-11 [2018-05-20].

[15] G. Weimann, 'Cyberterrorism, How Real Is the Threat?', usip.org, December 2004, http://www.usip.org/sites/default/files/sr119.pdf [2017-06-27].

[16] D. Prokopowicz, S. Gwoździewicz, 'Analiza bezpieczeństwa ochrony systemów informatycznych w kontekście globalnego cyberataku ransomware przeprowadzonego 27 czerwca 2017 roku', in: *Prawne i społeczne aspekty cyberbezpieczeństwa*, eds. S. Gwoździewicz, K. Tomaszycki, Warszawa: Międzynarodowy Instytut Innowacji „Nauka – Edukacja – Rozwój", 2017, pp. 65-87.

[17] S. Jones, 'Ukraine PM's office hit by cyber-attack linked to Russia', ft.com, http://www.ft.com/cms/s/0/2352681e-1e55-11e4-9513-00144feabdc0.html#axzz3Sl3skQKn [2016-08-07].

[18] M. Baezner, P. Robin, 'Hotspot Analysis: Cyber and information warfare in the Ukrainian conflict', Center for Security Studies (CSS), ETH Zürich, October 2018, https://www.researchgate.net/publication/322364443_Cyber_and_Information_warfare_in_the_Ukrainian_conflict [2020-01-11].

[19] D. Gilbert, 'BlackEnergy Cyber Attacks Against Ukrainian Government Linked to Russia', ibtimes.co.uk, 26 September 2014, http://www.ibtimes.co.uk/blackenergy-cyber-attacks-against-ukrainian-government-linked-russia-1467401 [2019-10-18].

The Russians recruited the "new army of Internet trolls" who were to change the social perception of the invasion of Ukraine, among others, by posting the relevant content supporting the actions of Russia and smearing Ukraine and its allies on internet blogs and media pages of the Western world.[20]

In order to legitimize Russian activities in Ukraine among the widest possible international public opinion, an extensive information campaign was conducted, the common denominator of which was the "Sputnik" media platform. The website, administered by the Russian agency "Rossija Siegodnia" already operates in 14 countries, including Poland.[21]According to the Sputnik project's website, "it depicts a multipolar world in which each country has its national interests, culture, history, and tradition."[22] The narrative presented by the Sputnik platform portrays Russia as a liberator and a refuge of democracy, a victim of a Western conspiracy to bring Russian citizens to the brink of poverty - while smearing the European Union, Ukraine, and the United States. The titles of articles presented by the said platform illustrate, in an extremely suggestive way, the extent of propaganda and distortions in how the current events in international relations, especially those related to the Russian-Ukrainian conflict, are presented.[23] European politicians are presented as incompetent and corrupt technocrats, and the articles depict their weaknesses and take their statements out of context. At the same time, military-wise, the activity of the "little green men" in Crimea meets the criteria of hybrid warfare. They are soldiers in army uniforms, carrying standard military weapons, albeit without any markings that could identify their affiliation. For a long time, Russia had categorically denied that it had anything to do with them and only after the official annexation of the

[20] 'Russia and Ukraine: Information warfare', 17 June 2014, http://resources.infosecinstitute.com/russia-ukraine-information-warfare/ [2018-04-26].

[21] M. Kowalczyk, 'Sputnik ruszył z rosyjską propagandą po polsku', press.pl, 23 February 2015, http://www.press.pl/newsy/internet/pokaz/48006,Sputnik-ruszyl-z-rosyjska-propaganda-po-polsku [2018-05-22].

[22] 'Sputnik, o projekcie', *Sputnik News*, http://pl.sputniknews.com///docs/about/index.html#ixzz3SrQTLf50 [2017-11-13].

[23] J. Romanienko, 'Pierwaja gibridnaja. Kogda Rossija naczała wojnu protiw Ukrainy?' ['Первая гибридная. Когда Россия начала войну против Украины?'], hvylya.net, 10 March 2015, http://hvylya.net/analytics/politics/pervaya-gibridnaya-kogda-rossiya-nachala-voynu-protiv-ukrainyi.html [2016-12-21].

peninsula did President Vladimir Putin admit that they were Russian soldiers. According to IHS analytics, between 2014 and 2015 alone, 14,000 Russian soldiers were stationed in Ukraine, who offered support to illegal separatist formations in eastern Ukraine. Additionally, 29,400 Russian soldiers controlled the ground in Crimea, and about 55,800 were deployed along the Russian-Ukrainian border.[24]

2. The Gerasimov doctrine – a long-term strategy for the deconstruction of Ukraine's statehood?

As already stressed, both the annexation of Crimea and the conflict in Donbas bear the hallmarks of what specialists define as "hybrid war". Almost everyone appears to agree on its characteristic features. In the early stages of the events, the question arose whether Russia's operations were impulsive, hasty and not well thought-through, or, to the contrary, all the decisions and operations were well-planned. The authors, backed by knowledge based not only on theoretical aspects but, primarily, on the analysis of both events unfolding in Ukraine's territory, lean towards the latter.

The analysis of the statement made by the Chief of the General Staff of the Armed Forces of Russia Valeriy Gerasimov during the meeting of members of the Academy of Military Sciences on January 26, 2013, helped resolve the dilemma.[25] The Russian General, de facto, laid out a new theory of modern warfare, also unofficially referred to as the "Gerasimov doctrine". He referred to a specific type of conflict, in which the differences between war and peace in the classic sense of the terms as well as between a uniformed army and covert activities disappear. According to V. Gerasimov, the said type of conflict has the potential to change "a completely stable country into the arena of

[24] R.F. Johnson, 'Russia's hybrid war in Ukraine is working', janes.com, http://www.janes.com/article/49469/update-russia-s-hybrid-war-in-ukraine-is-working [2016-08-29].

[25] 'Rol Gienieralnogo sztaba w organizacyi oborony strany w sootwietstwii s nowym Położenijem o Gienieralnom sztabie, utwierżdionnym Priezidientom Rossijskoj Fiedieracyi' ['Роль Генерального штаба в организации обороны страны в соответствии с новым Положением о Генеральном штабе, утверждённым Президентом Российской Федерации'], avnrf.ru, http://www.avnrf.ru/index.php/vse-novosti-sajta/620-rol-generalnogo-shtaba-v-organizatsii-oborony-strany-v-sootvetstvii-s-novym-polozheniem-o-generalnom-shtabe-utverzhdjonnym-prezidentom-rossijskoj-federatsii [2019-12-03].

the most intense armed conflict over a few months or even days."[26] The Russian General made no secret of the fact that Russian politics, especially concerning the post-Soviet area in recent years, display an upward trend in the use of non-military means of achieving political and strategic goals, which may prove to be "significantly more effective than the classic military methods." The Chief of the General Staff has also mentioned the asymmetrical military means, such as the limited use of special forces, and the recruitment and mobilization of opposition groups in enemy territory. It is difficult not to notice an analogy to actions taken on the territory of Ukraine. And while the subversive and espionage actions of commando groups may be considered typical of many other conflicts around the world, the said "recruitment and mobilization of opposition groups" is nothing more than the creation of self-proclaimed armed units of the Donetsk and Luhansk People's Republics.

The Gerasimov Doctrine justifies referring to these kinds of instruments and claims that non-military operations are not merely a form aimed to support military actions but a primary method to gain victory. According to the Russian General: chaos is the strategy pursued by the Kremlin and aimed at creating an environment of permanent unrest and conflict within an enemy state.

To sum up the foregoing, it should be noted that the phenomenon of hybrid war in the second decade of the 21st century presents itself as an ideal strategic variant for the destabilization of another country by a state, which, for various reasons, does not want to engage in open armed conflict. In the long term, Russia's operations on Ukraine's territory move towards subordinating this country and preventing it from integrating into Western European military and political structures. As a pivotal state occupying a significant part of the Eastern European area, Ukraine may be considered, according to the concept of Halford Mackinder, as Europe's *Heartland,* theoretically enables it to gain dominion over the World Island. With that in mind, it will al-

[26] W. Gierasimow, 'Cennost' nauki w priedwidienii, Nowyje wyzowy triebujut pierieosmyslenija form i sposobow wiedienijabojewych diej' ['Ценность науки в предвидении, Новые вызовы требуют переосмысления форм и способов ведения боевых действий'], *Wojenno-promyszlennyj Kurjer* [*Военно-промышленный Курьер*], no. 8 (476), 2013, http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf [2017-06-24].

ways be on Russia's path to achieving an imperial position, and Russia will, therefore, strive to control this country in various ways. Owing to modern technologies, propaganda, destabilization of IT infrastructure, and the use of conventional military attacks, the Russian Federation is consciously and systematically implementing its strategic assumptions to intensify the process of deconstructing Ukraine's statehood.

3. Hybrid threats in Central and Eastern Europe – implications for Poland

All the arguments outlined in the previous parts of the article suggest that the hybrid war is a strategic category. It can be defined as a set of actions aimed at achieving political goals by triggering synchronized kinetic and behavioral effects through the multidimensional application of influence tools and capabilities at the attacking party's disposal. The above definition implies that this is a new type of conflict management, considered by some theorists to be a new generation war, in which, in addition to the old ones, the new tools, often non-military, are employed, e.g., interaction in cyberspace to achieve strategic effects. The hybrid nature of military operations, as well as the spectrum of non-military instruments used in the Russian-Ukrainian conflict, constitute a serious challenge for political decision-makers in Central European countries, including Poland.[27]

The armed conflict in Ukraine, the annexation of Crimea, the war in Syria, the presidential election in the United States, and a number of provocations and actions unfavorable towards NATO countries and the European Union are the exemplification of the offensive of the Special Services of the Russian Federation, reformed by President Vladimir Putin. This reform, apart from a cosmetic change involving the renaming of the Federal Security Service (FSB) to the Ministry of Public Security, was to serve the regaining of control by the President of the Russian Federation over the Foreign Intelligence Service (SWZ FR) and the Federal Protective Service (FSO). In intelligence circles and the press, it was said that Putin sought to merge all security in-

[27] G. Soroka, T. Stępniewski, 'The Three Seas Initiative: Geopolitical Determinants and Polish Interests', *Rocznik Instytutu Europy Środkowo-Wschodniej*, vol. 17, no. 3, 2019, pp. 15-29.

stitutions (FSB, GRU, SWZ FR). The goal was to rebuild the influence of the special services to model the KGB.[28]

The main task of the Foreign Intelligence Service of the Russian Federation includes, among others, providing political, economic, technical, scientific information to the president and the government of the Russian Federation, analysis of the above information on countries, organizations, people, and everything that is crucial for conducting an effective policy by the president, prime minister and government of the Russian Federation. Foreign Intelligence Service officers act as diplomats and officers without the diplomatic immunity (the so-called Illegals), conducting their activities claiming to be journalists, tourists, etc. For this purpose, they use Russian embassies, consulates scattered around the world, and various enterprises and organizations.

Supporting separatist movements in countries that sympathize with NATO or the EU is among the standard activities of the intelligence services. The services' effectiveness has been tested in practice during the armed annexation of Crimea. Former US Secretary of State John Kerry has repeatedly admitted in his media statements that pro-Russian demonstrations in some Ukrainian cities were part of a plan of Russian entry into Ukraine. Similar activities can be observed in the Baltic States, such as Latvia, Lithuania, and Estonia.

Undermining the international order through military intimidation tactics (military exercises, development of military infrastructure, etc.) is just one of many propaganda and intelligence operations of services and agents, which uses such events during the information war to produce a desirable image. The Russian-Belarusian Zapad-2017 exercise (WEST-2017), which took place on September 14-20, 2017, may serve as another example. The strategic "Zapad" exercises organized every four years (since 2009) are treated by Russia as part of the information war with the West.[29]

Although a risk of a real confrontation with NATO forces is unlikely, Russia's military actions indicate that its preparations for a possible

[28] M. Sankowski, 'Rosyjskie Służby Specjalne. Reforma Kremla wskrzesi KGB?', osluzbach.pl, 23 April 2018, https://osluzbach.pl/2018/04/23/rosyjskie-sluzby-specjalne-reforma-kremla-wskrzesi-kgb/ [2020-01-19].

[29] A. Wilk, 'Ćwiczenia Zapad-2017 – wojna (na razie) informacyjna', *Komentarze OSW*, 1 September 2017, https://www.osw.waw.pl/sites/default/files/komentarze_249.pdf [2020-01-18].

armed conflict in Europe are being carried out consistently and are of a lasting nature. The Armed Forces of the Russian Federation have reached the level of capability that enables the implementation of any military goals in the post-Soviet area. The open issue is not so much the ability to pursue Russia's military policy goals but Moscow's actual need to use a military factor. It should be assumed that if the *status quo* is maintained, i.e., the lack of greater NATO military support for Ukraine (which has a real impact on the growth of the Ukrainian army's potential), a significant military presence of the Alliance in the Baltic States, Russia should abandon the direct use of military force to implement its political purposes. However, neither the Russian Federation's resignation nor even the limitation of using the military factor as a tool of information war with the West should be expected.

In the opinion of Polish political-military decision-makers and military experts, the crossing of the Alliance's border and the large-scale aggression of the Russian Federation are rather unlikely. The Russian strategic doctrine involves attacking the enemy throughout the entire depth of its territory, in all possible dimensions of influence. The consequence of such action would be a threat to Poland's allies. It is estimated that due to treaty obligations and their direct strategic interest, allied countries would be interested in suppressing aggression as far away from their territories as possible. It seems that the best way to suppress, restrain, and deter a potential opponent is to deploy the troops of other NATO countries on the territories of border states. However, due to response time, it would be most beneficial to deploy permanent bases with equipment. Then the potential aggressor should be prepared to find itself in direct conflict not only with the forces of the state attacked using subliminal methods but also with the forces of other allies.

An equally serious threat is posed by attempts to destabilize the political and economic situation by compiling measures aimed at the state's strategic goals, political diversion, and the activities of hostile propaganda centers. In Poland, the Russian services' activity grows in intensity while espionage is one of the most effective tools of the hybrid war.

The report of the Computer Emergency Response Team (CERT) presenting data from 2014 makes it clear that since the actions related to the annexation of Crimea and the intensification of the federalization of Donbas, Poland has become the target of one of the elements of the hybrid war, namely the information war. Significant growth in the number of attacks based on advanced tools is noticeable. Attacks on the President of the Republic of Poland's websites and the stock exchange, as well as on some websites of state administration institutions, have been reported. The group calling themselves "Cyber Berkut" claimed responsibility for these attacks, conducted on the grounds of Poland's alleged involvement in the conflict related to the situation in Ukraine. CERT emphasized that the Internet and social media – due to their availability and ease of use – are also becoming a tool used to support military and intelligence activities carried out by states by implementing widely understood propaganda and disinformation campaigns.[30]

Hybrid threats in Poland have been highlighted in both the *National Security Strategy* of the Republic of Poland and the *White Book on National Security* of the Republic of Poland. The Strategy says that in unfavorable conditions, the military threats to Poland's security may occur and take the form of *military conflicts of various scales – from military activities below the threshold of a classic war to a less probable large-scale conflict.*[31] The White Book emphasizes that there is a high probability of occurrence of a non-territorial conflict, where the opponent does not intend to take control over the attacked territory. Instead, the opponent employs measures deliberately limited in scale and reach, and implicit in the authorship, which are applied to "disarm" legal security mechanisms and thus force the attacked party to conduct independent military operations in the conditions of international isolation as a result of creating the so-called consensus-challenging situations.[32]

In the context of hybrid war, the important parts of the Strategy concern the strategic approach aimed at increasing the state's resilience to aggression. It involves military and non-military operations

[30] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014*, March 2015, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raporto-stanie-bezpieczenstwa cyberprzestrzeni-RP-w-2014-roku.html [2019-11-27].

[31] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, 2014, https://www.bbn.gov.pl/ftp/SBN%20RP.pdf [2020-01-12].

[32] *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, 2015, http://www.bialystok.ap.gov.pl/arch/teksty/biala_ksiega.pdf [2020-01-21].

strengthening the state's territorial inviolability, the comprehensive preparation of defense non-military structures, as well as the effectiveness of the support of the armed forces, including the possibility of organized resistance in areas occupied by the aggressor.[33]

Considering Poland's points of susceptibility to hybrid threats, reflected by political and military pressure implemented mainly in the information sphere, also in the cyberspace, it seems that the next priority should be building an effective information security system with a well-organized cybersecurity sector. The strategic goal in the area of information security is to ensure the safe functioning of the Republic of Poland in the information space, taking into consideration the information security of the state structures (especially public administration, security and public order services, special services, and armed forces), the private sector and civil society.[34] The information security units (including cybersecurity units) should be created and developed in the defense and protection (military and non-military) subsystems of the national security system.

In turn, the strategic goal in the area of cybersecurity of the Republic of Poland, formulated in the National Security Strategy of the Republic of Poland, is to ensure the safe functioning of the Republic of Poland in cyberspace, including an adequate level of security of national ICT systems – especially the critical ICT infrastructure of the state – as well as the private economic entities that are key to the functioning of society, in particular those in the financial, energy, and healthcare sectors.[35]

It is also particularly important to ensure independent operational and technical control over highly computerized combat and support systems, including control systems (holding control over their software source codes). An important task is the supra-ministerial coordination of these issues when building an integrated national security management system, assuming that one of the most challenging aspects of crisis management resulting from hybrid threats is the aspect

[33] S. Koziej, 'Strategiczna odporność kraju i rola w niej podmiotów niepaństwowych', *Krytyka Prawa*, no. 1, 2016, p. 84.

[34] *Projekt Doktryny bezpieczeństwa informacyjnego RP*, 2015, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf [2020-01-10].

[35] *Doktryna cyberbezpieczeństwa RP*, 2015, https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf [2020-01-15].

of communication and developing common situational awareness, the cyberspace and the information sphere are becoming the most sensitive fields of confrontation.

Conclusions

Summing up the considerations within this article, it should be noted that the annexation of the Crimean Peninsula, the support of pro-Russian separatists in Donbas, and the information war accompanying these events – being one of the key elements of hybrid war – is the result of the policy of strengthening the state and rebuilding the spheres of influence of the Russian Federation in the post-Soviet area implemented for many years. These actions were outlined in the Doctrine of Information Security of 2000, whose list of the most serious threats included, among others, "dissemination of disinformation about Russia and the activities of federal state authorities". The presidential programs implemented in recent years, such as: Creating a positive image of the Russian Federation, Strengthening Russia's information security, or Building a unified Russian information space, which President Putin subordinated to the goals of strengthening the civic identity of the multiethnic society of the Russian Federation, were supposed to neutralize information wars against the Russian Federation.

In its pursuit of hybrid confrontation with the Central and Western European states, the Russian Federation is trying to use many advantages such as its own controlled information space, extensive social engineering instruments, expert, journalistic and executive facilities, as well as many years of conducting information operations. These are large-scale actions that use digital platforms and disseminate content in line with Kremlin's policy. Their purpose is not only the desirable, i.e., compatible with the interests of the Russian Federation, modeling of internal and foreign public opinion. As the annexation of Crimea showed, their purpose is also to shape a new reality. These actions are based on the belief that Russia has the right to defend its own interests and *soft power* operations in the post-Soviet area. The Russian and Western versions of *soft power* in international relations, in reality, represent two different worlds. Representatives of the Russian *soft power* organized and falsified a referendum in Crimea, destabilized the eastern regions of Ukraine, and "delegitimize" the legally elected

Ukrainian authorities in propaganda campaigns. Therefore, it is hardly surprising that Poland and other Central European countries should closely follow the situation in the post-Soviet area and take a number of preventive actions to minimize the chance of occurrence of the hybrid threats presented in this paper.

Thus, in present-day conditions, the hybrid war is becoming one of the greatest threats to international security – as clearly demonstrated by the information coming from Ukraine. The West tried to watch this war for a while from a safe distance, but the vision of its effects expanding beyond the post-Soviet area somehow forces the Western states to take more and more specific actions to suppress the neo-imperial "inclinations" of the Russian Federation.

References

Bachman, S., Gunneriusson H., 'Terrorism and Cyber Attacks as Hybrid Threats: Defining a Comprehensive Approach for Countering 21st Century Threats to Global Peace and Security', *The Journal on Terrorism and Security Analysis*, 9th edition, Spring 2014, 2 April 2014, http://eprints.bournemouth.ac.uk/21206/1/Terrorism_and_Cyber_Attacks.pdf.

Baezner, M., Robin, P., 'Hotspot Analysis: Cyber and information warfare in the Ukrainian conflict', Center for Security Studies (CSS), ETH Zürich, October 2018, https://www.researchgate.net/publication/322364443_Cyber_and_Information_warfare_in_the_Ukrainian_conflict.

Bershidskyy, L., 'Unreformed Ukraine is in Danger of Becoming a Failed State', Bloomberg, 6 November 2015, https://www.bloomberg.com/view/articles/2015-11-06/unreformed-ukraine-is-self-destructing.

Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, 2015, http://www.bialystok.ap.gov.pl/arch/teksty/biala_ksiega.pdf.

Brzeziński, Z., *Wielka szachownica. Główne cele polityki amerykańskiej*, Warszawa: Politeja, 1997.

Doktryna cyberbezpieczeństwa RP, 2015, https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf.

Gierasimow, W., 'Cennost' nauki w priedwidienii, Nowyje wyzowy triebujut pierieosmyslenija form i sposobow wiedienijabojewych diej' ['Ценность науки в предвидении, Новые вызовы требуют переосмысления форм и способов ведения боевых действий'], *Wojenno-promyszlennyj Kurjer* [*Военно-промышленный Курьер*], no. 8 (476), 2013, http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf.

Gil, G., *Upadanie państwa w stosunkach międzynarodowych po zimnej wojnie*, Lublin: Wydawnictwo Naukowe UMCS, 2015.

Gilbert, D., 'BlackEnergy Cyber Attacks Against Ukrainian Government Linked to Russia', ibtimes.co.uk, 26 September 2014, http://www.ibtimes.co.uk/blackenergy-cyber-attacks-against-ukrainian-government-linked-russia-1467401.

Gruszczak, A., 'Hybrydowość współczesnych wojen – analiza krytyczna', in: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, eds. W. Sokała, B. Zapała, http://www.bbn.gov.pl/download/1/8755/Hybrydowos___wspolczesnych_wojen_____analiza_krytyczna.pdf.

Johnson, R.F., 'Russia's hybrid war in Ukraine is working', janes.com, http://www.janes.com/article/49469/update-russia-s-hybrid-war-in-ukraine-is-working.

Jones, S., 'Ukraine PM's office hit by cyber-attack linked to Russia', ft.com, http://www.ft.com/cms/s/0/2352681e-1e55-11e4-9513-00144feabdc0.html#axzz3Sl3skQKn.

Kaldor, M., *New* & *Old Wars: Organized Violence in a Global Era*, Stanford: University Press, 2001.

Konstitucyja Donieckoj Narodnoj Riespubliki [*Конституция Донецкой Народной Республики*], 30 August 2014, https://web.archive.org/web/20140830221524/http://dnr.today/wp-content/uploads/2014/08/aeAEI.pdf.

Konstitucyja Ługanskoj Narodnoj Riespubliki [*Конституция Луганской Народной Республики*], 26 December 2014, https://archive.is/BbQdc.

Kowalczyk, M., 'Sputnik ruszył z rosyjską propagandą po polsku', press.pl, 23 February 2015, http://www.press.pl/newsy/internet/pokaz/48006,Sputnik--ruszyl-z-rosyjska-propaganda-po-polsku.

Koziej, S., 'Strategiczna odporność kraju i rola w niej podmiotów niepaństwowych', *Krytyka Prawa*, no. 1/2016.

Lasica, D.T., *Strategic Implications of Hybrid War: A Theory of Victory,* Fort Leavenworth: School of Advanced Military Studies, United Army Command and General Staff College Press, 2009.

Marks, T.A., 'Counterinsurgency and operational art', *Low Intensity Conflicts & Law Enforcement*, no. 13, 2005.

Orzechowski, M., 'Wojna hybrydowa jako przejaw neoimperialnego ekspansjonizmu w strategii politycznej Federacji Rosyjskiej wobec Ukrainy', *TEKA Komisji Politologii i Stosunków Międzynarodowych*, no. 11/3, 2016.

Palazzo, A., Trentini, A., 'Hybrid, Complex, Conventional, Fourth-Generation Counterinsur-gency. It's Decision that Still Matters Most', *Australian Army Journal*, no. 1, 2010.

Pietraś, M., 'Istota i specyfika konfliktów niskiej intensywności', in: *Konflikt niskiej intensywności w Naddniestrzu*, eds. M. Celewicz, J. Kłoczowski, M. Pietraś, Lublin: Wydawnictwo Instytutu Europy Środkowo--Wschodniej, 2006.

Projekt Doktryny bezpieczeństwa informacyjnego RP, 2015, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf.

Prokopowicz, D., Gwoździewicz, S., 'Analiza bezpieczeństwa ochrony systemów informatycznych w kontekście globalnego cyberataku ransomware przeprowadzonego 27 czerwca 2017 roku', in: *Prawne i społeczne aspekty cyberbezpieczeństwa*, eds. S. Gwoździewicz, K. Tomaszycki, Warsaw: Międzynarodowy Instytut Innowacji „Nauka – Edukacja – Rozwój", 2017.

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014, March 2015, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738, Raporto-stanie-bezpieczenstwa cyberprzestrzeni-RP-w-2014-roku.html.

Robb, J., *Brave New War. The Next Stage of Terrorism and the End of Globalization*, Hoboken: Wiley, 2007.

'Rol Gienieralnogo sztaba w organizacyi oborony strany w sootwietstwii s nowym Położenijem o Gienieralnom sztabie, utwierżdionnym Priezidientom Rossijskoj Fiedieracyi' ['Роль Генерального штаба в организации обороны страны в соответствии с новым Положением о Генеральном штабе, утверждённым Президентом Российской Федерации'], avnrf.ru, http://www.avnrf.ru/index.php/vse-novosti-sajta/620-rol-generalnogo-shtaba-v-organizatsii-oborony-strany-v-sootvetstvii-s-novym-polozheniem-o-generalnom-shtabe-utverzhdjonnym-prezidentom-rossijskoj-federatsii.

Romanienko, J., 'Pierwaja gibridnaja. Kogda Rossija naczała wojnuprotiw Ukrainy?' ['Первая гибридная. Когда Россия начала войну против Украины?'], hvylya.net, 10 March 2015, http://hvylya.net/analytics/politics/pervaya-gibridnaya-kogda-rossiya-nachala-voynu-protiv-ukrainyi.html.

'Russia and Ukraine: Information warfare', 17 June 2014, http://resources.infosecinstitute.com/russia-ukraine-information-warfare/.

Sankowski, M., 'Rosyjskie Służby Specjalne. Reforma Kremla wskrzesi KGB?', osluzbach.pl, 23 April 2018, https://osluzbach.pl/2018/04/23/rosyjskie-sluzby-specjalne-reforma-kremla-wskrzesi-kgb/.

Soroka, G., Stępniewski T., 'The Three Seas Initiative: Geopolitical Determinants and Polish Interests', *Rocznik Instytutu Europy Środkowo-Wschodniej*, vol. 17, no. 3, 2019.

'Sputnik, o projekcie', *Sputnik News*, http://pl.sputniknews.com///docs/about/index.html#ixzz3SrQTLf50.

Stępniewski, T., 'Determinanty wewnętrzne polityki zagranicznej Ukrainy pod rządami Wołodymyra Zełenskiego', *Rocznik Instytutu Europy Środkowo-Wschodniej*, vol. 17, no. 1, 2019.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, 2014, https://www.bbn.gov.pl/ftp/SBN%20RP.pdf.

Weimann, G., 'Cyberterrorism, How Real Is the Threat?', usip.org, December 2004, http://www.usip.org/sites/default/files/sr119.pdf.

Wilk, A., 'Ćwiczenia Zapad-2017 – wojna (na razie) informacyjna', *Komentarze OSW*, 4 September 2017, https://www.osw.waw.pl/sites/default/files/komentarze_249.pdf.