Studia Bezpieczeństwa Narodowego
Zeszyt 35 (2025)
ISSN 2028-2677, s. 11-26
DOI: 10.37055/sbn/196886

Instytut Bezpieczeństwa i Obronności
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

National Security Studies
Volume 35 (2025)
ISSN 2028-2677, pp. 11-26
DOI: 10.37055/sbn/196886

Institute of Security and Defense
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

THE CONCEPT OF WARFARE IN CYBERSPACE AS AN EXAMPLE OF HYBRID WARFARE OF THE RUSSIAN FEDERATION

KONCEPCJA WALKI W CYBEPRZESTRZENI JAKO PRZYKŁAD DZIAŁAŃ HYBRYDOWYCH FEDERACJI ROSYJSKIEJ

Dawid DUDA
Military University of Technology in Warsaw
ORCID: 0000-0001-6548-9562

Joanna KOWALSKA
War Studies University in Warsaw
ORCID: 0009-0002-7748-1861

Abstract. The contemporary international security environment faces many challenges and threats resulting from the various goals of the entities that create it. The aim of the article is to indicate the ways in which the Russian Federation has influenced the cyberspace of Ukraine, starting from the annexation of Crimea in 2014. The main research problem is an attempt to answer the question: what value is attributed to the sphere of cyberspace in the area of conducting hybrid activities? The article hypothesises that cyber warfare has grown in importance in recent years and is one of the essential elements of hybrid warfare. The research methodology is based on a critical analysis of literature, definitions, induction and deduction. The conclusions from the research indicate the need to educate the security community, which is a key issue in formulating methods of counteracting practices conducted by the Russian Federation.

Abstrakt: Współczesne międzynarodowe środowisko bezpieczeństwa napotyka wiele wyzwań i zagrożeń wynikających z różnych celów podmiotów je tworzących. Celem artykułu jest wskazanie sposobów oddziaływania w cyberprzestrzeni Ukrainy przez Federację Rosyjską, począwszy od aneksji Krymu w 2014 roku. Główny problem badawczy stanowi próba odpowiedzi na pytanie: jaką wartość przypisuje się sferze cyberprzestrzeni w obszarze prowadzenia działań hybrydowych? W artykule przyjęto hipotezę, iż walka w cyberprzestrzeni nabrała w ostatnich latach na znaczeniu i stanowi jeden z zasadniczych elementów wojny hybrydowej. Metodyka badań oparta została o krytyczną analizę literatury, definiowanie, indukcję i dedukcję. Wnioski z badań wskazują potrzebę edukacji środowisk bezpieczeństwa, co jest kluczową kwestią w formułowaniu metod przeciwdziałania praktykom prowadzonym przez Federację Rosyjską.

Keywords: security, threats, cyber-security, cyberspace, hybrid operations.

Słowa kluczowe: bezpieczeństwo, zagrożenia, cyberbezpieczeństwo, cyberprzestrzeń, działania hybrydowe.

Introduction

The 2014 Olympic Games in Sochi were considered a Public Relation success for Russia. A modern Russia, open to the world and cooperation, was portrayed through the Olympics. Three days after the competition ended, a group of Russian supporters in unmarked uniforms seized the Crimean parliament. Subsequently, the airport in Sevastopol and Simferopol were occupied. The result of the aforementioned events was the declaration of independence of the Crimean parliament and the holding of a referendum on the question of Crimea's annexation to Russia (Roslan 2015, p. 73). The Russians will not give up their predestination to become a superpower again. Through propaganda, information and diplomatic activities, Cold War rhetoric representing the myth of an overwhelmed Russia as a result of the West's expansion to the East and the determinants of the international order negating the hegemony of any of the powers are exposed (Zalewski 2016, p. 207).

On February 24, 2022, Russia launched an invasion of Ukraine, shattering stability in Europe. The Russian army created a threat to European countries by attacking civilian housing, infrastructure, hospitals, industrial center or cultural resources in Ukraine.

To date, Russia has not succeeded in Ukraine by cyber means, but this does not mean that it is impossible. Attempts to nullify military defenses and disrupt civilian life indicate the limited usefulness and effectiveness of cyberoperations (as part of strategic coercion tools), although one should be aware that countering Russian cyber operations will require significant resources (Stevens, Burton 2023, p. 1).

Current state of knowledge

The topics of cyberspace and hybrid warfare have been gaining prominence in recent years. Despite the rapid development and evolution, there are still many doubts about, for example, the terminological or material scope of the areas indicated.

A starting point for indicating the methodological scope of the study is, among others, the publication of J. Apanowicz (Apanowicz 2002).

There are studies addressing the issues of cyber warfare or hybrid warfare (Meissner, 2022, p. 136). The issues of Russian cybersecurity policy are most of ten found in sorter studies, there is still a shortage of compact positions on the described topic.

In the literature one can find assumption that Russia's conflict with Ukraine is a classic example of hybrid warfare (Hajduk, Stępniewski 2000, pp. 135-137). It is

also worth referring to the War Doctrine of the Russian Federation, which *"sanctions"* hybrid warfare, which means the need to take into account the possibility of subliminal aggression in terms of the strategy of Russia's neighbours (BBN 2015).

The issue of social media is also extremely important in the area described. Russian service providers seem to lead the market in social media manipulation. Almost all identified infrastructure and software providers were of Russian origin (Singularex 2019).

From the Russian point of view, information confrontation is a continuous process, and the tools used to achieve it are all possible means at Russia's possession. The Kremlin uses information-technological as well as information-psychological weapons to achieve strategic victory without the need for conventional force and, at the same time, without triggering escalation in the target state. Securing the national information space and cyber sphere can not only protect the cohesion of society but also protect national technological and scientific development (Hakala, Melnychuk 2021).

Cyber attacks conducted at the tactical level provide benefits when combined with conventional weapons. To use an example, a cyber attack can confuse or disable command networks, making kinetic attacks more effective. The coordination of cyber and kinetic operations must be preceded by a proper degree of planning. The timing of some cyber operations conducted by the Russian Federation indicates that they were intended to support conventional operations (Lewis 2022).

The cyber domain has allowed information operations based on disinformation and propaganda to be implemented with unprecedented scale and speed. Attacks in cyberspace often focus on spreading false information and are also used for propaganda. Threat actors attempt to influence the information space and restrict access to reliable, official information (OECD 2022).

One of the more notorious activities of Russian cyber experts was the 2016 US presidential election. At the time, Russian hackers attacked the Democratic National Committee and made sensitive information public within the WikiLeaks. The world has entered another new era of conflict, characterised by blurred boundaries, constant uncertainty and strongly evolving threats (Luberisse 2023).

The subject of hybrid warfare is also addressed by authors posting studies on the websites of NATO, PISM, Warsaw Institute, Bellona Quarterly.

Research methodology

A search of the available literature identified a need to supplement and structure the knowledge on hybrid actions conducted by the Russian Federation in cyberspace. Despite the existing literature on hybrid issues, publications on the theoretical assumptions of the Russian Federation in terms of conceptual action, there is still

a lack of studies treating examples of applications of the aforementioned. Thus, the indicated arguments confirm that the specified issues are particularly important and cognitively interesting.

The purpose of the described research and assumption advised in this publication became the analysis of the theoretical scope of the indicated issues.

The following question was identified as the main research problem: what value is placed on the cyber sphere in the area of hybrid operations? A main hypothesis was specified: cyber warfare has grown in importance in recent years and is one of the essential elements of hybrid warfare.

The research process was framed by the following stages: defining the research problem, data collection, data processing and data analysis.

With reference to the formulated research problems and taking into account the assumptions made to solve the indicated fundamental research problem and the specific ones, mainly theoretical research methods were used, among which the following stand out: literature review, individual sources related to cyberspace, comparative analysis in the definitional area, induction, deduction were used.

A literature review is a systematic and comprehensive survey of existing books, reports, articles in a specific field of research or topic. It is a fundamental element of the research methodology as it provides direction, context and justification for the study. This study used mainly qualitative methods, document and content analysis. The content analysis indicated the extraction of key narratives in the media discourse on cyber activities. This made it possible to identify certain trends and propaganda used by the Russian side. The comparative analysis adopted several comparison criteria, such as, scope of definition, institutional perspective and context.

In addition, an attempt was made to use primarily two methods of comparison, i.e. the vertical method and the horizontal method. In the area of source selection, search criteria played an important role, among which the thematic scope, the time of publication (most recent sources), the type of sources and the language of the sources, both national and international, in order to make the research more holistic. Research techniques are defined as the methods and tools used to collect and analyse data and obtain answers to the research questions identified. This article was developed according to quantitative research techniques: secondary data analysis, so-called desk research, so existing data such as reports or statistics were used. Qualitative research techniques were also used, i.e. content analysis (qualitative study of documents, texts, attempting to find patterns, motives). The article uses both induction and deduction to attempt to achieve a comprehensive analysis of the issue. Induction allowed general conclusions to be drawn from the analysis of identified cases of cyber-attacks as elements of hybrid warfare. Deduction, on the other hand, enabled the application of existing theories of hybrid warfare within the framework of case-specific analysis.

An outline of terminology

The discussion should begin with an introduction to the term cyberspace as first used in science-fiction literature by W. Gibson in 1982, who defined cyberspace as: "A consensual hallucination experienced every day by billions of cultivated users in all countries. [...] A graphical representation of data downloaded from the banks of all the world's computers. Unimaginable complexity... Luminous lines ran through the mind's spacelessness, clusters and constellations of data" (Gibson 2001, p. 13).

One of the most widespread definitions of cyberspace in the world is the one created by the US Department of Defense, which reads: "the global domain of the information environment consisting of interdependent networks of information technology infrastructure and the data contained therein, including the Internet, telecommunications networks, computer systems and embedded processes and controllers". It is worth adding that cyberspace is characterized by certain technical features, such as: the absence of its center with an open network architecture, and its most important component is the Internet, ageography – there are absolutely no territorial boundaries, immateriality and magnetic field (Zięba 2018, p. 56).

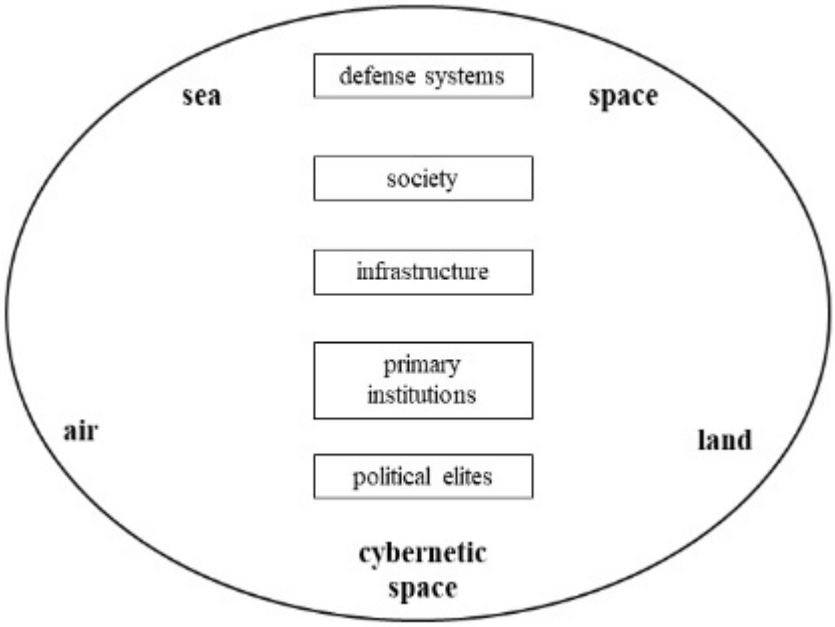
In the 2015 Doctrine of the Cyber Security of the Republic of Poland, cyberspace is defined as a place for the exchange and processing of information created by information and communications systems, i.e. sets of information devices working together and software responsible for storing them, the key is the links between these systems and the relationship between users. The cyberspace of the Republic of Poland is referred to as the cyberspace within the territory of the Polish state, as well as representative offices of the Republic of Poland, e.g. military contingents, diplomatic missions (BBN 2015). One of the greatest challenges for the state especially in recent years is to ensure the security of the RP precisely in cyberspace, as this is a process that consists of ensuring that the state as a whole, its individuals and entire structures are not threatened.

It should be remembered that the area of cyber threats is a new area of activity for every state, citizens and businesses. The new challenges and risks associated with cyberspace also on a global scale make one wonder how much effort states are facing to protect and safely use ICT systems. Constant change and innovation make it hard to prepare and adapt to new threats, especially when there were none before.

Cyberspace is often described as a new field of conflict, where battles can be fought not only with other states, but also with terrorist groups, hostile organizations or organized crime groups.

It is crucial to note cyberspace as a new dimension of warfare. So far, conflicts have taken place over land, sea, air and space. Cyberspace is referred to as the fifth dimension of combat (Bryjka 2015, p. 115). As can be seen, these dimensions are strongly interconnected, intermingle and interact with each other.

Image 1. Warden's *„five dimension"* model of struggle



Source: own study based on: Warden, J., 1995. The Enemy as System. Airpower Journal, 9 (1), p. 374-375

The Internet offers an incredible opportunity to be independent of geographical limitations. Modern times indicate that the operations carried out can be atterritorial and immaterial, with the help of cyberspace, action against a country are carried out from anywhere in the world, often guaranteeing a high degree of anonymity, this makes cyber threats so dangerous and difficult to detect. In this context, cyberspace can be seen as a negative environment, where terrorist organizations, criminal groups used in the strategy of the increasingly common hybrid warfare cooperate.

According to Marek Madej, the state can use the Internet in two ways: as an *"auxiliary"* tool to enhance the state's ability to act on reality, or as a kind of weapon to be used to launch IT attacks (Madej 2012, pp. 94-95). By cleverly using the virtual world, leaders exploit the capabilities of non-state actors to achieve national goals.

It is worth mentioning at this point the concept of hybrid warfare itself, a component of which is the cyber warfare described earlier. The concept of hybrid warfare is not entirely new, but in view of the development of technology and technics, it has gained strongly in importance. States somehow *"tethered"* by international agreements and treaties do not want to openly declare war or allow direct armed conflict, which is why the possibility of using networks in hybrid warfare is so attractive. Thanks to information technology, it is possible to defect opponents

without declaring direct armed conflict, thus international agreements are not violated (Bilal 2021). It should be noted that states are always embroiled in political games, economic and military rivalries, but nowadays skirmishes are no longer conducted in such a radical way by means of lethal force, they are more often fought in the arena of innovation and investment in new technologies, which will then serve in an efficient and silent hybrid war.

The hallmark of hybrid war fare is its multidimensionality, a combination of conventional and unconventional tools of force and diversion. The instruments combine and synchronize to achieve the desired effect, to exploit the enemy's weaknesses. Using kinetic tools and non-kinetic tactics together in hybrid warfare, the synergy of these elements is ought to achieve a decent optimal effect in combat. Efficiently used instruments in hybrid warfare make it possible to inflict significant damage on the state involved in the conflict. At the same time, they often do not require the declaration of open war. Therefore, the defining characteristic of hybrid war is the unclear boundary between war and peace. The blurring of these boundaries makes the concept of war elusive, and it is difficult to identify the boundaries and thresholds of enemy action.

Another important feature of hybrid warfare is its implementation below the zone of hostilities, as it does not manifest direct, overt aggression. Despite these features, hybrid war has great benefits, while being cheaper and less risky than kinetic operations (Bilal 2021). An important factor why hybrid warfare has gained in „popularity" is also a social factor, by its less visible nature of operation, the public does not express such notorious opposition to actions of this type. There is less public response to sponsoring and spreading disinformation than to using tanks or fighters on the territory of another state. Hybrid warfare is a cheaper and more feasible course of action for conflicting states, and it does real damage on the enemy's side. It is now a way to defeat the enemy without fighting, which is the highest level of the art of war. What is convenient for states using the instruments of hybrid warfare is that it is often difficult to attribute responsibility to a state for hostile actions, the ambiguity and lack of territorial boundaries as in cyber warfare, for example, means that these actions often remain anonymous and the perpetrators difficult to catch. The difficulty in attributing these actions means that they often go unpunished, the targeted state is unable to detect the source of these actions, the ambiguity makes it very difficult and challenging to attribute hostile actions to a given state.

Hybrid warfare uses a combination of actions by multiple entities, so hybrid defense should take the form of a synergy of multiple actions and actors. NATO and the European Union are aware of the threat, having already identified combating hybrid threats as one of their priorities for cooperation since 2016 (Hagelstam 2018). The European Center of Excellence for Combating Hybrid Threats (Hybrid CoE), with its capital in Finland, plays a major role in this cooperation, expanding

knowledge in this area is crucial, as the level of improvement and technological innovation is increasing all the time and the risks involved will continue to evolve, arming hybrid warfare with new tools. It goes without saying that combating new forms of hybrid warfare should be done in a dynamic manner using international cooperation.

The modern world operates in a global system of interconnectedness, consisting of common transportation, energy, financial systems, so the weakness of one state to hybrid attacks has a huge impact on the others. Sovereign action by states, joint planning and response to manifestations of hybrid attacks is therefore required. A special priority for these actions was given by NATO after the painful experience in Crimea in 2014, following the events a strategy to combat hybrid threats based on a horizontal and NATO-wide approach was put in place (Hagelstam 2018). NATO as well as the European Union created an infrastructure for analyzing and monitoring hybrid threats based on intelligence activities, working together interstate.

An example of cooperation is the signing of a joint declaration in 2016 by NATO Secretary General Jens Stoltenberg and the Presidents of the European Commission and the EU Council Jean-Claude Juncker and Donald Tusk, which enshrined a "common set of proposals" and 74 concrete actions to build defense against hybrid threats and in the field of cybersecurity.

The rise of non-military methods of warfare is undeniable. A particular variety of it is disinformation, essentially influencing young citizens, aimed at undermining the historical, patriotic and spiritual traditions of a country. Provoking social tensions, ethnic hatred, extremism or reinforced religious hostility is part of hybrid warfare, in which the instrument is precisely the informational impact on the population (Darczewska 2015, p. 20).

An interesting thesis is to look at social media as a new battlefield in hybrid warfare (Wierucka, 2022). Information warfare can be defined as negative cooperation in information acquisition, deliberate transformation of information, information disruption, and each of these domains will influence each other triggering a feedback loop of further domains. Information hybrid warfare is thus constituted by manipulative actions to discredit the state under attack, leading to the disorganisation of the adversary.

A state weakened by effectively waged information warfare may lose its ability to make strategic decisions, actions and may even be deprived of combat capability. Therefore, it is particularly important to convince public opinion of the rightness of one's actions or to raise the morale of soldiers. A case in point is the current Ukrainian conflict, where the Ukrainian president in his numerous media appearances has sought to debunk the Russian narrative of the war and to reinforce and support the attitude of his soldiers.

Many times, the success of a battle victory depends on convincing the public of one's cause. In the age of the information society, it is the efficient and attractive transmission of information to influence the mentality and mindset of the recipient that determines the course of war.

The problem of information warfare continues to grow, with fake news and a flood of information capable of effectively destabilising society and, consequently, the entire state.

War is defined as „aimed at forcing the opponent to do our will – an act of violence" (Clausewitz 2010, p. 15), and can also be carried out precisely in cyberspace or information space (Daniluk 2019, p. 150).

The role of cyberspace in Russian operations

The range of threats posed by the development of cyberspace is wide and manifold, which is why the protection of this area has become one of the most significant priorities of the Polish strategy. Recently, another alarming phenomenon of violation of cyberspace can be observed, which is the increased activity of the Russian Federation in the virtual world. Russia is increasingly using online networks as a weapon in hybrid conflicts. At present, it is alarming to note the gradual evolution of the area of hostilities, which are no longer visible to the naked eye at first but play out over the Internet in the hands of skilful hackers and programmers.

In front of the world's eyes, in the volatile situation related to the war in Ukraine, it is becoming common place to identify examples of the Kremlin's use of cyberspace to initiate attacks, as well as its active participation in the information war using manipulation and propaganda. In its cyber security policy, Russia wants to take the lead, realising on which plane, i.e. the virtual one, the key movements within the conflict will be played out in the coming years. With this knowledge, Russia has created the Runet network project, an internal space independent of the global Internet. It is safe to say that Russia, with its own internet network, would become a forerunner of new attacks in cyberspace.

The Russian authorities initially used the internet as a surveillance tool to gather intelligence, the web is also great for monitoring others, including independent media or activists. Currently, we can observe Russia's use of cyberspace not only in the dimension of active attacks, e.g. probable attacks on the infrastructure of Estonia, Georgia, but, above all, activity in the sphere of covert manipulation, e.g. during presidential and parliamentary elections (Gardocki, Worona 2020).

In its attacks, the Kremlin uses so-called „troll farms", which carry out commissioned cyberattacks from fictitious profiles, criminal groups disseminate false information so-called *„fake news"*. The ongoing conflict in Ukraine has shown what

a huge role disinformation and well-organised propaganda can play. Our times show that the key to achieving the goals of hybrid warfare is to capture the mind of the enemy.

Misinformation is designed to ridicule, depreciate the opposition and praise the actions of the Kremlin authorities. Trolls can publish hundreds of posts a day spreading disinformation, the consequences of aggressive cyber tactics can be very serious. At the same time, Russia consistently denies and dements that it uses cyber attacks in its political game.

When considering new forms of war, it is worth going back to texts which gave an alternative account of battles and conflicts two hundred years ago, such an author being Carl Phillip Gottlieb von Clausewitz. This participant in the war campaigns against France, directly observed the Napoleonic style of battlefields, rose to the rank of general in his military career, and has been called „the misunderstood genius of war" (Clausewitz 2010). In order to understand the universal nature of war and, further, the directions of current actions, it is useful to draw on the historical insights of this Prussian general who, in the 19th century, in his life's work „On War", included the following observations. „On War" contained insights and conclusions on the basic principles of warfare. Considered a genius of the „art of war" on the basis of his own experience, Clausewitz placed emphasis in his work on the morale of soldiers and the ultimate goals of war, which he defined as follows: „War is merely the continuation of politics by other means", „War is an act of violence aimed at bending the enemy to our will". „Disarming or defeating the enemy, no matter what we call the thing, must always be the goal of warfare" (Zera 2015).

These two sentences above also fit into the picture of hybrid warfare at the time completing its pattern, politics is continually part of the course of wars, it directly influences them, and if unskill fully conducted it is dangerous and results in open conflict also armed. The general pointed out a very interesting aspect of war „If two sides have armed themselves to fight, a feeling of hostility must have pushed them to do so, and as long as they are armed, that is, they do not talk about peace, this feeling must persist" (Zera 2015). Its intangible nature, the aforementioned „feeling" about the conflict playing as important a role as the number of troops and strategy. This can be transferred within the framework of the contemporary eastern conflict, did not this „feeling" of Russia for war result in the annexation of Crimea or the incursion into Ukrainian territory? This situation can be written into the very nature of war flowing from political teachings and actions. It is precisely in its feeling that an area belongs to it that Russia uses all methods to achieve its goal in our time, including by means of cyberspace.

The Russian authorities make skilful use of cyberspace in their domestic and international politics. One of the first recorded cyber attacks carried out by Russia was that of 10 September 1986, an espionage attack involving the hacking of the then Soviet services into the computer system controlling Ronald Reagan's strategic

defence missile system called Star Wars (Gardocki, Worona 2020). In recent years, one can observe the increased negative activity of Russia in the virtual network, especially in the area of propaganda and information activities. It is in Moscow's interest to develop a strategy for conducting information warfare in order to efficiently manipulate attitudes and views in the international community. The weakening of the community of NATO member states and the European Union is one of the main objectives of disinformation. The distortion of facts, the concealment of information is intended to build a positive image of Russia and to instil a sense of fear among citizens. In contrast to Western countries, freedom of speech is significantly restricted in Russia, independent media, opposition activists are harassed and intimidated, targeted and discredited by false information about them online. Newspapers, television and radio stations are subordinated to the Kremlin's interests and only present the actions of President Putin's government in a positive manner.

There is no doubt that the Kremlin in its policy uses cyber attacks not only conducted by state authorities but also sponsors hacking organisations or informal criminal groups for this purpose, very difficult to unmask. An example of a massive attack of false information in cyberspace was the time after the assassination of Boris Nemtsov, the opposition leader, in February 2015 (Gardocki, Worona 2020). At that time, false information was disseminated from hundreds of fictitious angles to cast doubt on the link between the assassination and the authorities, and attempts were made to distort reality by reversing the facts by spreading the position that it was the opposition that would gain from the assassination of their leader, not the Kremlin authorities. Using fictitious accounts, private profiles, hackers published content on forums that were made to look like discussions of ordinary citizens. Thanks to these actions, discord was „sown" in cyberspace, the inability to verify fiction from falsehood, reality was modelled for their political goal, and Russian society is relatively easily subject to propaganda.

Russian actions targeting the east make it possible to infer a new generation of warfare taking place in the virtual world. Russia's aggression against Ukraine in 2022 is an example of full-scale action using asymmetric operations saturated with attacks in cyberspace. A holistic and sophisticated approach to the ongoing conflict can thus be observed here. In Russia, the Gerasimov Doctrine, the named erived from the Chief of the General Staff of the Armed Forces of the Russian Federation, as the interpretation of the current perception of war (Meissner 2022, p. 136). The doctrine incorporates an approach to warfare as a means of combining what are termed hybrid measures, among others: psychological, informational, political actions that affect the enemy in lieu of or in parallel with military action. Often, hybrid actions can also be the beginning of an armed conflict, beforehand the adversary is weakened in cyberspace, among others.

Cyber-attacks must be seen as the first level of aggression that can lead to full--blown, intense military conflicts, a prelude to weakening the opponent's defence

capabilities. Although Russia has long combined military and non-military means against Western states, these actions are now being enriched with new technologies, so these games are becoming more dangerous. The aforementioned Gerasimov doctrine is part of Russia's concept of new-generation warfare using hybrid means, taking full advantage of current scientific and technological advances (Meissner 2022, p. 136).

Russia's attitude was very well outlined by the former Chief of General Staff of the Polish Army, saying: "one can see the cultural difference, the attitude of the Russian elite and the brutality in the use of the tool of power that is the Russian army. High tempo, manoeuvre, aggressive action, and disregard for losses have always been the hallmark of Russian operations. [...] Observations of contemporary armed conflicts and civilisational, social, technological changes made by the Russians result in a kind of paradigm shift in warfare. [...] The inclusion [...] of such a broad spectrum of means (including non-kinetic, economic, informational) and the insertion of them into a coherent theoretical basis of operational art makes it an extremely effective and dangerous tool for world order. Reflexive management or information, special operations are nowadays as effective an element of operational art as armoured strikes and operational maneuver groups and give character to modern Russian operational art" (Depczyński, Elak 2020, pp. 7-9). The Russian government's activity geared towards confrontation with the West is likely to continue, which will require the international community to increase its efforts towards cyber security and the levelling of hybrid attacks.

Given the above into considerations, the negative role of cyberspace in Russian operations is illegal information gathering, in the international arena the use of the virtual network to interfere with the political and security foundations of other states, while in domestic politics virtual space is used to fight the opposition and build a good image for the Kremlin. Cyber attacks in hybrid warfare used by Russia lead to the effective achievement of their goals at a lower image and economic cost and often guarantee anonymity. In the light of recent events in Ukraine, one can be sure that Russia is prepared to make many sacrifices to maintain its superpower status, it will undoubtedly develop its „negative" potential in cyberspace for this purpose, affecting the instability of the international situation.

Conclusions

The West has been taken aback by the effectiveness and efficiency of Russian propaganda, above all by its reach, which manifests itself, among other things, in creating the image of the need to rebuild the Russian empire. Identification and analysis of photos, videos and comments indicate the aims of Russian aggression: to crush Ukrainian democracy by force of arms and define new European borders,

to stop the penetration of European values in the context of civil society, to give up Novorossiya would entail loss of face and defeat, as well as loss of strategic influence in the „post-Soviet" area (Zalewski 2016, p. 218).

The examples of the conflicts in Crimea and eastern Ukraine indicate that the West faced a formidable challenge from Russia. Russia is a strong player in the post-Soviet area and both the efforts of the United States and the European Union probably have not been sufficient to prevent conflict in 2022.

Russian cyber-attacks did not completely paralyse the Ukrainian state, critical infrastructure and the command and control system of the armed forces, so they ultimately failed (Orenstein, 2022). Based on available sources, it is not clear to what extent Russia failed to achieve its main objectives due to the effectiveness of Ukraine's cyber defence and support from the West or due to its limited defensive capabilities (The Economist, 2022). It is worth emphasising that Russia, having lost much of its military capability, will continue to use asymmetric methods, including actions in the cyber and information space.

Russian propaganda activities are conducted in cyberspace and are one of the essentials elements of hybrid actions. Their effectiveness is determined, among other things, by crucial human factor, within which Russian agitators create content that convinces audiences of the Alliance's provocative role. Russian propagandists present the defense policy of NATO's members in a false view of offensive or aggressive actions.

In conclusion, it is significant to be aware that mainly engagement and cooperation allows for the achievement of the intended objectives, particularly in the context of conducting cyber warfare (Szyłkowska 2021). It is also related to the conduct of an effective civil-military policy (Urych, Matysiak 2022).

Bibliography

1. Apanowicz, J., 2002. Metodologia ogólna. Gdynia: Dom organizatora.
2. BBN, 2015. Doktryna Cyberbezpieczeństwa Rzeczpospolitej Polskiej [online]. Available at: https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf [accessed: 11.10.2024].
3. BBN, 2015. Informacja na temat Doktryny wojennej Federacji Rosyjskiej [online]. Available at: https://www.bbn.gov.pl/ftp/dok/03/35_kbn_doktryna_rosji.pdf [accessed: 11.10.2024].
4. Bilal, A., 2021. Wojna hybrydowa - nowe zagrożenia, złożoność i „zaufanie" jako antidotum [online]. Available at: https://www.nato.int/docu/review/pl/articles/2021/11/30/wojna-hybrydowa-nowe-zagrozenia-zlozonosc-i-zaufanie-jako-antidotum/index.html [accessed: 27.10.2024].
5. Bryjka, F., 2015. Cyberprzestrzeń w strategii wojny hybrydowej Federacji Rosyjskiej. W: T. Grabińska, Z. Kuźniar, Bezpieczeństwo personalne a bezpieczeństwo strukturalne

III. Czynniki antropologiczne i społeczne bezpieczeństwa personalnego. Wrocław: WSO WL, 115-131.
6. Clausewitz, C., 1997. O wojnie. Wordsworth.
7. Daniluk, P., 2019. Wojna informacyjna - złożona przeszłość i niepewna przyszłość. Rocznik Bezpieczeństwa Międzynarodowego, 13(2), 149–168 [online]. Available at: https://doi.org/10.34862/rbm.2019.2.9 [accessed: 15.10.2024].
8. Darczewska, J., 2015. Diabeł tkwi w szczegółach wojna informacyjna, wojna informacyjna w świetle doktryny wojennej Rosji [online]. Ośrodek Studiów Wschodnich. Available at: http://katedrawiss.uwm.edu.pl/sites/default/files/download/202006/pw_50_pl_diabel_tkwi_net.pdf [accessed: 27.10.2024].
9. Depczyński, M., Elak, L., 2020. Rosyjska sztuka operacyjna w zarysie [online]. Available at: https://www.bing.com/ck/a?!&&p=c8deda7b5a9b30c6e821363734d70a41e6117a38883f52ed824a4d8c640055bfjmltdhm9mtczmdqxotiwma&ptn=3&ver=2&hsh=4&fclid=3db85f4f-edc1-6972-08f6-4a65ecce688d&psq=depczynski+elak+2020&u=a1ahr0cdovl2nlannolmljbs5lzhuucgwvy2vqc2gvzwxlbwvudc9id21ldgexlmvszw1lbnqub2pzlwlzc24tmju0my02otyxlxllyxitmjaymc1pc3n1zs05lwfydgljbgutztlkotixnmitmtfloc0zyzrmlwe3otgtzmnkndmyogq0yjvm&ntb=1 [accessed: 21.10.2024].
10. Gardocki, S., Worona, J., 2020. Wykorzystanie przez Rosję cyberprzestrzeni w konfliktach hybrydowych a rosyjska polityka cyberbezpiezpieczeństwa [online]. Colloquium, 12 (2). Available at: https://colloquium.amw.gdynia.pl/index.php/colloquium/article/view/174 [accessed: 26.10.2024].
11. Gibson, W., 2001. Neuromancer. Warszawa: Książnica.
12. Hagelstam, A., 2018. Współpraca przeciwko zagrożeniom hybrydowym [online]. Available at: https://www.nato.int/docu/review/pl/articles/2018/11/23/wspolpraca-przeciwko-zagrozeniom-hybrydowym/index.html [accessed: 27.10.2024].
13. Hajduk, J., Stępniewski, T., 2015. Wojna hybrydowa Rosji z Ukrainą: uwarunkowania i instrumenty. Studia Europejskie, 4 (76), 135-137.
14. Hakala, J., Melnychuk, J., 2021. Russia's Strategy in Cyberspace [online]. Available at: https://stratcomcoe.org/publications/russias-strategy-in-cyberspace/210 [accessed: 20.01.2025].
15. Lewis, J., A., 2022. Cyber War and Ukraine [online]. Available at: https://www.csis.org/analysis/cyber-war-and-ukraine [accessed: 20.01.2025].
16. Luberisse, J., 2023. Russia: Hybrid Warfare and the Weaponization of Cyberspace (Excerpt from Silent Wars: Espionage, Sabotage, and Covert Battles in Cyberspace) [online]. Available at: https://medium.com/fortis-novum-mundum/russia-hybrid-warfare-and-the-weaponization-of-cyberspace-excerpt-from-silent-wars-espionage-529274aa42ab [accessed: 20.01.2025].
17. Madej, M., 2012. Zagrożenia asymetryczne – „nowy" problem bezpieczeństwa międzynarodowego. W: A. Raciborska, Bezpieczeństwo międzynarodowe. Warszawa: Wydawnictwo Naukowe Scholar, 94-95.

18. Mazurek, A., Widzińska, M., 2023. Reakcja Unii Europejskiej i NATO na agresję rosyjską w Ukrainie [online]. Available at: http://refleksje.amu.edu.pl/wp-content/uploads/2023/12/13-Mazurek_Widzinska.pdf [accessed: 10.10.2024].
19. Meissner, J., 2022. Rosyjska Koncepcja Wojny Nowej Generacji w świetle pierwszych doświadczeń wojny na Ukrainie [online]. Available at: https://ojs.tnkul.pl/index.php/rns/article/view/17783/16761 [accessed: 10.10.2024].
20. OECD, 2022. Disinformation and Russia's war of aggression against Ukraine [online]. Available at: https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/ [accessed: 20.01.2025].
21. Orenstein, M., 2022. Russia's Use of Cyberattacks: Lessons from the Second Ukraine War, Foreign Policy Research Institute.
22. Rosłan, G., 2015. Rosyjski model konfliktu. Kwartalnik Bellona, 1 (680), 73.
23. Singularex NATO StratCom COE, 2019. The Black Market for Social Media Manipulation [online]. Available at: https://stratcomcoe.org/publications/the-black-market-for-social-media-manipulation/103 [accessed: 20.01.2025].
24. Stevens, T., Burton J., 2023. NATO i strategiczna rywalizacja w cyberprzestrzeni [online]. Available at: https://www.nato.int/docu/review/pl/articles/2023/06/06/nato-i-strategiczna-rywalizacja-w-cyberprzestrzeni/ [accessed: 19.10.2024].
25. Szyłkowska, M., 2021. Attributes of cyberconflict in the context of armed conflict – an outline of the problem. Przegląd nauk o obronności, 11, 134-154.
26. Urych, I., Matysiak, G., 2022. Preparing youth for defence: Socialisation, education, and training of young people in Europe for national security. Security and Defence Quarterly, 38 (2).
27. Warden, J., 1995. The Enemy as System. Airpower Journal, 9 (1), 374-375.
28. Wierucka, J., 2022. Social media as a tool of an information combat [online]. National Security Studies, 26, 51-62. Available at: https://sbn.wat.edu.pl/pdf-156476-92600?filename=social%20media%20as%20a%20tool%20of.pdf [accessed: 21.10.2024].
29. Zalewski, J. (2016). Intoksykacja psychologiczno-informacyjna głównym elementem wojny informacyjnej prowadzonej przez Federację Rosyjską. Studia Bezpieczeństwa Narodowego, 9(1), 201-220 [online]. Available at: https://doi.org/10.37055/sbn/129826 [accessed: 18.10.2024].
30. Zera, P., 2015. "O wojnie" Clausewitza - wojenny poradnik sprzed 200 lat [online]. Available at: https://historia.wprost.pl/501406/o-wojnie-clausewitza-wojenny-poradnik-sprzed-200-lat.html [accessed: 26.10.2024].
31. Zięba, R., 2018. Bezpieczeństwo międzynarodowe w XXI wieku. Warszawa: Poltext, 56.