

Systemy Bezpieczeństwa Narodowego
Zeszyt 26 (2022)
ISSN 2028-2677, s. 11-20
DOI: 10.37055/sbn/152883

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

National Security Studies
Volume 26 (2022)
ISSN 2028-2677, pp. 11-20
DOI: 10.37055/sbn/152883

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

RUSSIA-UKRAINE. WAR? NEW WAR? OLD WAR?

ROSJA-UKRAINA. WOJNA? NOWA WOJNA? STARA WOJNA?

Łukasz Kominek

Military University of Technology

Urszula Staśkiewicz

University of Justice

Mateusz Maciąg

The War Studies University

Abstract. The aim of this study is a polemological analysis of the conflict between the Russian Federation and Ukraine. The main research problem of the article was defined in the form of a question: can the analyzed conflict be classified as old or new wars? The secondary goal, however, was to indicate the characteristic elements of this analysis. The following research methods were used in the work: definition, which allowed to define the uniqueness of terms, analysis and synthesis, which allowed for appropriate interpretation of the existing data, induction and deduction, which allowed for finding answers to the research question considered in the work. The work also uses the method of comparative analysis in terms of definitions relating to the discussed scope. The analysis of sources, monographs and scientific articles dealing with the research topic was also used.

Keywords: Russia, Ukraine, war, Kaldor, polemology

Abstrakt. Celem artykułu jest analiza polemologiczna konfliktu między Federacją Rosyjską, a Ukrainą. Główny problem badawczy określono w formie pytania: Czy analizowany konflikt można zaliczyć do starych czy nowych wojen? Celem pobocznym było wskazanie elementów charakterystycznych w zakresie tej analizy. Postawiono hipotezę, iż: Działania obecnie trwającego konfliktu ukraińsko-rosyjskiego noszą znamiona typowe dla nowych wojen na płaszczyźnie wpływu konfliktu na porządek międzynarodowy. W pracy zastosowano następujące metody badawcze: definiowanie, które pozwoliło na określenie jednoznaczności

terminów; analizę i syntezę, które pozwoliły na odpowiednią interpretację zastanych danych; indukcję i dedukcję, które pozwoliły na znalezienie odpowiedzi na rozważne w pracy pytanie badawcze. W pracy posłużono się także metodą analizy porównawczej w zakresie definicji dotyczących omawianego zakresu. Zastosowano również analizę źródeł, monografii, artykułów naukowych traktujących o badanej tematyce. **Słowa kluczowe:** Rosja, Ukraina, wojna, Kaldor, polemologia

Introduction

Changes in the manner of conducting conflicts, which has led to the theory of „RMA”, „new wars” and introduced such terms as hybrid wars (Hoffman 2011), privatized wars (Keen 1995), informal war (Marriage 2016), cyberwar (Ashraf 2021), began to shape the belief in Western society that war, which we learn about during history lessons, is now a thing of the past. When studying security science or legal science, we learn that the use of Weapons of Mass Destruction (WMD), cluster munitions and TBX is forbidden. Armed forces are also prohibited from destroying hospitals or attacking humanitarian corridors (The Geneva Conventions of 1949 and their Additional Protocol).

Since 2007, after the DDoS attacks on Estonian servers, Western countries began to value the threat of cyberwar and focused closely on cyber defense. For this purpose, strategic documents were updated e.g. in Estonia, considerable attention was paid not only to cyber defense but also to the issue of disinformation and psychological defense of citizens (National Security Concept of Estonia 2017). These activities also concerned international organizations such as NATO and the European Union.

The West was convinced that mass murder during armed conflicts was only perpetrated in remote, desert regions e.g. by ISIS in Afghanistan or Arabs in Syria, and in Europe the only threat to civilians are random terrorist attacks (Madrid 2004, London 2005). NATO member states spend less and less on defense, which was criticized by Donald Trump (*NATO criticism*, <https://www.cnn.com/2018/07/11/trumps-nato-criticism-is-valid-europe-isnt-spending-enough-on-def.html>) and instigated discussions about the legitimacy of such close cooperation within NATO.

More and more often the question begins to appear - Are new varieties of wars, still wars in the classically Clausewitz's sense? How to conduct defense preparation to arrange the state, armed forces and society for war? What will a possible future war look like? Is war in the classical sense in Europe still possible?

The aforementioned information seems rational until February 24th, 2022 when Putin announced a so-called “special military operation” which in the World media was rightly shown, to be more similar to warfare during World War II - equipment (tanks, armored personnel carriers), bombing of churches, shooting at humanitarian convoys but also rapes, looting, targeting civilians (degenerate warfare). It is also worth adding that the Russian Ministry of Defense has confirmed the use

of the TOS-1A system, which utilizes thermobaric rockets that produce incendiary and explosive effects.

As a result of the Russian actions (referred to by the Russian president as demilitarization and denazification of Ukraine) many Ukrainian cities have been destroyed, and millions of Ukrainian citizens have been forced to flee from their homes. How, then, should we understand this breakthrough in the conduct of wars? Are we returning to the middle of the 20th century?

The above prompted the authors to analyze the situation in Eastern Europe and compare it with scientific, contemporary and historical literature. According to the authors' thesis, contrary to appearances, the war in Ukraine is a modern war, a real war of the 21st century, in which not only military technology plays a significant role, however there was a factor that Putin did not foresee - social media. This publication aims to highlight this variable.

However, it should be noted that military operations are still ongoing and the situation is developing dynamically. Nevertheless, even at this stage, certain peculiarities of the conflict can be observed, which indicate that the wars of the 21st century are considerably different from those of previous centuries. The framework of this publication does not allow for a full analysis of the activities of the parties, therefore it was decided to focus on only a small fraction.

War as understood by polemologists

War, as defined by Clausewitz, „is an act of violence intended to compel our opponent to fulfil our will. [...] The aim of all action in War is to disarm the enemy”. In accordance with the dictionary definition, war is:

- a conflict carried on by force of arms, as between nations or between parties within a nation; warfare, as by land, sea, or air;
- a state or period of armed hostility or active military operations;
- a contest carried on by force of arms, as in a series of battles or campaigns (*War*, <https://www.dictionary.com/browse/war>).

How then should one call the conflict in Eastern Ukraine in 2014 or the annexation of Crimea (admission of the Republic of Crimea to the Russian Federation)? Or the fight against ISIS (*Договор между Российской Федерацией и Республикой Крым о принятии в Российскую Федерацию Республики Крым и образовании в составе Российской Федерации новых субъектов*, <http://kremlin.ru/events/president/news/20605>)? In her analysis of this problem, M. Kaldor has reached the conclusion that these wars differ from the classical understanding and created the new wars concept (Kaldor 2012).

According to Kaldor's concept, “old wars” were primarily conducted by regular armed forces of the conflicting countries. “New wars” involve paramilitary groups

gathered around charismatic, self-imposed leaders controlling certain areas, terrorist groups, fanatic volunteers (such as mujahedeens), organized crime groups, regular army units, security forces, as well as mercenaries and private armies (Münkler 2004). The new wars involve a blurring of the distinctions between:

- war (usually defined as violence between states or organized political groups for political motives),
- organized crime (violence undertaken by privately organized groups for private purposes, usually financial gain),
- large-scale violations of human rights (violence undertaken by states or politically organized groups against individuals).

Other authors use term 'post-modern' (Duffield 1998). „However, the term is also used to refer to virtual wars and wars in cyberspace (Gray 1997); moreover, the new wars involve elements of pre-modernity and modernity as well. A more recent term used by Frank Hoffman, which has gained widespread currency, particularly in the military, is 'hybrid wars' – the term nicely captures the blurring of public and private, state or non-state, formal and informal that is characteristic of new wars; it is also used to refer to a mixture of different types of war (conventional warfare, counter-insurgency, civil war, for example) and, as such, may miss the specific logic of new wars.

However, these are not the only changes to undertaking warfare on the turn of 20th and 21st centuries, as one must remember the massive technological leap that had revolutionized armed conflicts. This problem is connected with another hypothesis in military theory about the future of warfare - *revolution in military affairs* (RMA).

The original theorizing was done by Marshal Nikolai Ogarkov (Marshal 1984) however it was popularized by the USA, specifically by Andrew Marshall. The basis of RMA is the assumption that the use of large ground forces will be minimized. In place of some ground forces, new technologies will be implemented in order to establish dominance on the battlefield.

At the turn of the 20th and 21st centuries, the RMA theory began to prove itself- technological development enables more and more precise strikes, which in the near future may lead to paralyze the adversary's massed military capability (Gouré 2020). Also, many scientific publications dealing with this issue began to be published (Young 2003).

However, technological advancement involves much more than increased precision in combat. It also means the development of a new kind of warfare – without the use of land, air or naval forces – that is, the cyberwarfare. The example of Estonia in 2007 proves that a state can be paralyzed without the need of a military action. This occurrence has caused further changes to the perception and definition of war. Questions arose of whether cyberwarfare even really counts as warfare? Is a cyberattack even an attack in the classical sense?

Against the backdrop of these polemological considerations, Russian troops began maneuvers and were massing close to Ukraine in a military buildup (*Russia moves troops*, <https://abcnews.go.com/International/russia-moves-troops-ukraine-analysts-explain-buildup/story?id=77165952>). The day has come, which forced us to verify the existing views and theories.

Analysis of the Russo-Ukrainian War

On the eve of Russian invasion on Ukraine, neither the public opinion nor leading analysts have predicted the country could be attacked on such a massive scale. It was difficult to disagree with the notion that such a move, strategically speaking, would be completely illogical. Despite that, Ukraine appears to have been well prepared for such an occurrence.

The authors have attempted to analyze this conflict and find the answer to the questions of why is Putin losing the war (at least as of writing) and why it is unfolding so differently to the events of 2014.

In our opinion, while not dismissing the years of Ukraine's military preparation, this has been made possible in large part to the impact of social media.

Even just a couple years ago it would be hard to imagine that geolocation of video uploads on social media would prove legitimately important to field operations of the military. Even before the invasion was launched, the online community has been trawling through videos showing vehicles being moved towards the Russian border and their kind has given us our first hints that we might not be looking at simple military exercises.

OSINT (open-source intelligence, that is collection and analysis of data gathered from open sources, primarily the Internet) has been present for years, but the sheer scale to which the social media have been used for its purposes is unprecedented (Khera V., *An Introduction to Open Source Intelligence (OSINT)*, <https://cybersecurity-magazine.com/an-introduction-to-open-source-intelligenceosint>). Prior to the invasion, numerous social media platforms have been flooded with audiovisual materials showing Russian military's transportation. For many - especially on TikTok, where such videos dominated - this proved a chance to gain many "likes".

In terms of information warfare surrounding this conflict, we are witnessing for the first time ways in which the social media can be used. Russia's attempts to frame the conflict according to its needs and to spread disinformation have completely failed. The information coming from the battlefield is quickly verified and used by Ukrainian and Western media with a singular purpose - to completely upend Russia's "special operation" and "denazification of Ukraine" narratives, effectively presenting the country as an aggressor committing war crimes.

There is also another dimension of the social media use. Never before has a nation's president use these portals in such a context. It is a rather unique aspect of the ongoing conflict. A key role has been played by the US-backed team that has prepared Volodymyr Zelensky for his role in this conflict, effectively utilizing his acting skills to both support and motivate the nation and create a worldwide image of a statesman defending the democratic thought from Russian barbarism. All of these elements have completely changed how the information system around him has been organized.

Currently, thanks to social media, all disinformation attempts are debunked within an hour by the online community. It is very important and poses a question of how these experiences will impact future wartime information and disinformation campaigns. Russia has been put at disadvantage due to these open source communities.

The US intelligence service has also used such analyses when warning Ukraine. We have seen the speed at which various fake news have been debunked. The use of social media by Ukraine has been masterful in terms of waging information warfare - we all know about the 40 kilometer-long death convoy in which the conscripts freeze to death. We have seen videos and photos of incalculable supply trucks destroyed by Ukrainian forces. All of this gives us a more detailed understanding of what's going on out in the field, which is very rare for modern armed conflicts.

Importantly, in some contexts the Russian information security is very limited - we have seen unencrypted communication streamed online and satellite photos revealing precise data on their location and intents. There are dedicated groups on social media gathering visual confirmations of all vehicle losses, allowing for a much more precise tally than the information provided by the sides of the conflict - and reflects poorly on Russia's advances so far.

In terms of social media information flow in this ongoing conflict, Twitter is dominant, with Telegram following shortly afterwards. These sources account for much of the information sources important to collecting data (along with the aforementioned TikTok).

Telegram in particular might be key to the use of social media in the conflict, as the service retains metadata of the uploaded files, which is not necessarily true for the majority of other platforms to which the videos and photos are being uploaded. Metadata such as coordinates of the phone that has recorded a given photo/video provides many key pieces of information for purposes of conducting military operations. This has already been utilized by both US intelligence services and the Ukrainians to prove Russia is manufacturing disinformation and even false flag attack videos.

Having said that, the Russian public opinion needs to be seen with a certain understanding. The actions of the president of the Russian Federation are proving

that he has understood the impact social media had on his campaign. Putin has closed practically all independent media outlets and intimidated the journalists with a new law forbidding accurate reporting on the invasion, or even calling it so - instead of the much more neutrally sounding “special military operation”. His regime has raised a digital “iron curtain”.

As a result, according to common reports, most Russians are only able to see a sanitized picture of the war in Ukraine that Putin wants them to see. The state-controlled media dispense solely Kremlin’s lies on supposed persecution of Russian-speaking citizens by the Ukrainian government. They have no reason to suspect the Russian authorities are taking such actions to keep them from knowing about the perpetrated acts of cruelty.

After only a handful days of conflict, Russian government has blocked the Apple App Store in order to make it impossible to download software enabling creation of private virtual networks able to circumvent the state censorship. People watching television and visiting the approved websites - which most probably accounts for most of Russia’s citizens - are receiving a completely false retelling of the war, framing Russia’s actions as admirable, rather than regrettable. From that perspective, the paralyzing economic sanctions imposed by the western countries can appear unjustified and unfair. On the midnight of March 14th, Instagram has been shut down on Russia’s territory, further confirming the theory stated above (*Kyiv Independent*, <https://twitter.com/KyivIndependent/status/150308059055545548-9?s=20&t=nAvvVHzYcbUiUHJDBvwXOQ>).

One thing can be said for sure - the ways in which the social media are being utilized, whether as means of gathering data on military movements (videos uploaded to the social media, particularly Telegram) or building narratives (Ukraine President’s pleas on Twitter) will usher the information warfare into a new era, even after this war in Ukraine ends.

Information superiority leads to a decision-making advantage in regular military operations, thus granting a dominant position. Both Sun Tzu (Sun Tzu 2021) and more modern authors would agree that information has always been and will remain an incredibly important resource - and given the advancements in communication technology, has currently become a strategic asset. In truth, in recent years the analysis of data has proven to be the real challenge, rather than its acquisition (Liederman 2012).

The militaries have always been observing their opponents to gather information - whether in terms of available technology, troop movements or prepared plans. This is not unlike the natural world, in which the predator observes its prey before striking.

However, the social media have never been used at quite this scale in the known history of modern warfare and asymmetrical combat. Yet they have proven

a key element of the current situation - a game Vladimir Putin did not expect to play and therefore also expect to lose.

We live in an age when almost everyone publishes everything in social media - especially their power users. In the context of Russian actions towards Ukraine it is that phenomenon of uploading everything to “the socials” that has changed the outcome of this brutal and inhuman game.

Conclusions

Summing up the considerations presented in this article, one should agree with the thesis that the war started by Russia is a modern war, a real war of the 21st century. It is a hybrid war, conducted both on land, in the air and in cyberspace, and it uses various means of influence - information warfare, disinformation, disavowing selected people, attack on critical infrastructure, attack on civilians, but also what Ukraine has used, OSINT.

In the future, researchers of information warfare will have to take into account this new factor - the functioning of social networking sites. As Z. Śliwa noted - the effectiveness of the methods is directly related to the specificity of threats, therefore the methods must be adapted adequately to the needs and based on the available possibilities - independently and in coordination with allies (<https://ine.org.pl/rozmowa-z-dr-hab-zdzislawem-sliwa-baltic-defen--ce--c---ollege>).

BIBLIOGRAPHY

- [1] Ashraf, C., 2021. *Defining cyberwar: towards a definitional framework*, Defense & Security Analysis, 274-294.
- [2] Duffield, M., 1998. 'Post-modern conflict: warlords, postadjustment states and private protection', Michael Ignatieff, *The Warrior's Honor: Ethnic War and the Modern Conscience*, London: Chatto & Windus, 1998.
- [3] Gouré, D., 2020. *Army's Newest Long-Range Fires System Isn't New, But It Will Be Effective*.
- [4] Gray, C., 1997. *Post-Modern War: The New Politics of Conflicts*, London and New York: Routledge.
- [5] Hoffman, F., 2011. *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies.
- [6] Kaldor, M., 2012. *New and Old Wars. Organised violence in a global era*, 3rd Edition, Polity.
- [7] Keen, D., 1995. 'When war itself is privatized', Times Literary Supplement.
- [8] Khera, V., *An Introduction to Open Source Intelligence (OSINT)*, <https://cybersecurity-magazine.com/an-introduction-to-open-source-intelligenceosint> [accessed: 17.08.2022 r.].
- [9] *Kyiv Independent*, <https://twitter.com/KyivIndependent/status/150308059055545548-9?s=20&t=nAvvVHzYcbUiUHJDBvwXOQ> [accessed: 17.08.2022 r.].
- [10] Liederman, K., 2012. *Bezpieczeństwo informacyjne*, Warszawa.
- [11] Marriage, Z., 2016, *Formal Peace and Informal War*. Security and Development in Congo, Routledge.

- [12] Marshal, N. V., 1984, "The Defense of Socialism: Experience of History and the Present Day," Красная Звезда [Red Star], May 9, 1984; trans. Foreign Broadcast Information Service, Daily Report: Soviet Union, Vol. III, No. 091, Annex No. 054.
- [13] Münkler, H., 2004. *Wojny naszych czasów*, Kraków.
- [14] *National Security Concept of Estonia 2017*.
- [15] *NATO criticism*, <https://www.cnn.com/2018/07/11/trumps-nato-criticism-is-valid-europe-isnt-spending-enough-on-def.html> [accessed: 17.08.2022 r.].
- [16] *Rozmowa*, <https://ine.org.pl/rozmowa-z-dr-hab-zdzislawem-sliwa-baltic-defence-college> [accessed: 17.08.2022 r.].
- [17] *Russia moves troops*, <https://abcnews.go.com/International/russia-moves-troops-ukraine-analysts-explain-buildup/story?id=77165952> [accessed: 17.08.2022 r.].
- [18] Sun Tzu, 2021. *The Art of War*, Penguin Books.
- [19] *The Geneva Conventions of 1949 and their Additional Protocols*.
- [20] *War*, <https://www.dictionary.com/browse/war> [accessed: 17.08.2022 r.].
- [21] Young, T., 2003. *The Revolution in Military Affairs and Coalition Operations: Problem Areas and Solutions*, Defense & Security Analysis Vol. 9, No. 2.
- [22] *Договор между Российской Федерацией и Республикой Крым о принятии в Российскую Федерацию Республики Крым и образовании в составе Российской Федерации новых субъектов*, <http://kremlin.ru/events/president/news/20605> [accessed: 17.08.2022 r.].