

MIROSŁAW BANASIK*

Uniwersytet Jana Kochanowskiego, Kielce, Polska

ANDRZEJ SOBOŃ**



Akademia Sztuki Wojennej, Warszawa, Polska

INFORMATION WAR AS A MECHANISM OF CONDUCTING INTERNATIONAL COMPETITION BY THE RUSSIAN FEDERATION



ABSTRACT: The article focuses on information war used by the Russian Federation as part of its holistic approach to conducting international competition. Through a critical analysis of Russian literature and operational practice, the mechanisms of its application and challenges to the security of European states were identified. Through the research it was established that the Russian perception of contemporary international rivalry is based on the idea of playing out the struggle in people's minds, and its foundation is the concept of new generation war. The article justifies that information war is a holistic concept of influencing people's cognitive sphere and forming their behavioral attitudes in line with Russia's expectations. Moreover, it is suggested that in the strategic dimension, information war allows to achieve the goals of international rivalry or create conditions for achieving them, without the need for military force. In this context, conducting information campaigns integrated with psychological operations in cyberspace is a weapon of the Russian government, which is used to discredit legitimate authorities and weaken the political, economic and social systems of European states.

KEYWORDS: information war, international competition, cognitive sphere, information, disinformation, propaganda,

* **dr hab. Mirosław Banasik**, Jan Kochanowski University, Kielce, Poland

 <https://orcid.org/0000-0002-9358-1240>  miroslaw.banasik@interia.pl

** **plk dr hab. inż. Andrzej Sobon**, War Studies University, Warsaw, Poland

 <https://orcid.org/0000-0003-2540-2252>  andrzej.sobon@wp.pl

INTRODUCTION

Information war is a regular feature of the activity that the Russian Federation (RF) conducts internationally. According to Russian views, it encompasses a series of processes aimed at stealing, destroying, manipulating, distorting, and neutralizing information¹. It can be conducted overtly or covertly. It is usually used as part of a rivalry below the threshold of open armed conflict, which goes beyond the context of classic war² and is referred to the literature as a war in the gray zone³. Modern technologies, the Internet and social media constitute a new field of competition for information war, which is moving into the cognitive sphere and is aimed at shaping people's attitudes in line with Russia's expectations. Under these conditions, informational impact becomes the main factor influencing the paradigm shift in the conduct of modern wars, which is based on the idea of playing out the battle in the minds of the people, as pointed out by Yevgeny Messner⁴. Unlike other forms and methods of international influence, information war is a continuous process, independent of relations with strategic rivals. It is assumed that in the context of the Russian Federation's quest for supremacy over the West, the intense confrontation in the information domain towards European states began with Vladimir Putin's speech at the Munich Conference in 2007, in which the Russian leader demonstrated his dissatisfaction with the existing international order⁵. Since 2014, international relations have witnessed a phenomenon of information war reminiscent of the Soviet style of disinformation and propaganda. Previously dormant tools of informational international influence used as part of Russian foreign policy, have caused widespread surprise⁶, and this has contributed to the perception that their use in the 2014 conflict with Ukraine represents a radically new and different form of war. However, the steadily growing importance of information operations could be discerned in Russian strategic thinking long before the Ukrainian crisis began⁷. However, the new role of information in the strategy of conducting international competition cannot be overlooked. In the era of modern technologies,

¹ K. Giles and A. Seaboyer., *The Russian Information Warfare Construct*, Kingston 2019, p. 5.

² D. Pronk, *The Return of Political Warfare*, Strategic Monitor 2018-2019.

³ "The gray zone is an operational space between peace and war, involving coercive actions to change the status quo below a threshold that, in most cases, would prompt a conventional military response, often by blurring the line between military and nonmilitary actions and the attribution for events" (Morris et. al., 2019, p. 8).

⁴ Y. Messner, *Choczesz Mira, Pobiedi Miatieżewojnu!* [You want Peace, Defeat Rebellion!], Moscow 2005.

⁵ T. Shanker and M. Landler, *Putin Says U.S. is Undermining Global Stability*, The New York Times 2007, 11.02.2007.

⁶ S. Sukhankin, *The Western Alliance In The Face Of The Russian (Dis) Information Machine: Where Does Canada Stand?*, SPP Research Paper, Volume 12:26 September 2019, Calgary 2019, p. 1.

⁷ S. Blank, *Signs of New Russian Thinking About the Military and War*, Eurasia Daily Monitor Volume: 11 Issue: 28, 2014. 13.02.2014.

information is becoming an integrator of multidimensional campaigns⁸, conducted with the use of all available instruments of influence, which is also reflected in the current military doctrine of the RF⁹.

Due to its ability to achieve cognitive effects, Russian disinformation and propaganda has become a permanent part of the international information space¹⁰. These activities have been conducted continuously for centuries and have been characterized by a multi-vector message narrative. Currently, disinformation and propaganda are key elements of multifaceted information and psychological activities aimed at the security of democratic states. Internationally, there is an increased activity of the RF undertaken on information platforms that allow for broadcasting on multiple radio and television channels, providing photographic and infographic content, and spreading information through social media and mobile devices. The RF authorities influence social media through sponsored troll farms that run blogs and tweets on behalf of the Kremlin. Providing false information or distorting it is becoming a daily occurrence¹¹. The media regularly disseminate information that reflects Moscow's point of view. Western narratives are called into question and influences the formation of public opinion abroad¹². By means of false messages, attempts are made to influence all areas of the functioning of European states or to discredit them in the international arena. Conflicts are fueled and social unrest is aroused, which is supposed to lead to political crises and lower level of citizens' security¹³.

Russian information war is a powerful instrument of international influence. It is a means to achieve psychological superiority, frustration, and moral decomposition in the societies of the states the RF wishes to dominate or subjugate. Information campaigns are carefully planned, according to the need to produce specific strategic effects. The RF uses information war to achieve its goals in international, regional and domestic policy, which indicates its

⁸ K. Ven Bruusgaard, *Crimea and Russia's Strategic Overhaul*, Parameters, Vol. 44, No. 3, Autumn 2014, pp. 81–90.

⁹ *Vojennaja doktrina Rossijskoj Fiedieracyi* [The Military Doctrine of the Russian Federation], Москва 2014.

¹⁰ HA. Conley, J. Mina, R. Stefanov and M. Vladimirov, *The Kremlin Playbook. Understanding Russian Influence in Central and Eastern Europe*, Lanham • Boulder • New York • London 2016, p. 2.

¹¹ *Russia Military Power. Building a Military to Support Great Power Aspirations*, Defense Intelligence Agency, Washington 2017, p. 40.

¹² L. Robinson, TC. Helmus, RS. Cohen, A. Nader, A. Radin, M. Magnuson and K. Migacheva, *Modern Political Warfare. Current Practices and Possible Responses*, Santa Monica 2019, p. 67.

¹³ A. Polyakova and SP. Boyer, *The Future Of Political Warfare: Russia, The West, And The Coming Age Of Global Digital Competition*, The New Geopolitics Europe 2018, p. 3.

geopolitical significance¹⁴. In Russia, it is believed that the implementation of foreign policy objectives is not possible without the use of the information sphere, especially the media¹⁵.

The problematic situation identified in this way leads to the formulation of the main research problem: How does the RF use information war to conduct international competition and what challenges does this pose to European security? The main research problem was fragmented and the following specific problems were identified: 1) What is the genesis and evolution of Russian information war? 2) What is the significance of information influence in Yevgeny Messner's theory of rebel war? 3) In what is the strategic aspect of information war expressed and what are the notional dilemmas? 4) What is the operational practice of information war?

The considerations were conducted on the ground of international competition reducing them to identifying the role of information war in achieving the foreign policy objectives of the RF. The theoretical framework on which the article is based is anchored in the essence of political war, the main principles of which were developed by George F. Kennan¹⁶ once its Russian counterpart, expressed in the concept of a new generation of war. In political war¹⁷, the state affects the opposing side with all available instruments, including intelligence, diplomacy, and most of all information without waging war, understood in its classical sense¹⁸. Similarly, next generation war eschews the kinetic use of military force in favor of other, non-kinetic mechanisms of international influence. The concept of next generation war reflects an innovative way of thinking about the conduct and resolution of conflict and involves multi-level efforts aimed at destabilizing state functions and altering state internal order. Unlike conventional warfare, the center of gravity of next-generation war is focused on the public¹⁹.

¹⁴ T. Čížik, (ed.), *Information Warfare – New Security Challenge for Europe*, Centre for European and North Atlantic Affairs (CENAA), Bratislava 2017, p. 9.

¹⁵ L. Robinson, at all, ... p. 61.

¹⁶ GF. Kennan, [w:] GD. Harlow, GC. Maerz, eds., *Measures Short of War: The George F. Kennan Lectures at the National War College, 1946–1947*, Washington 1991. Accessed October 16, 2019. https://www.files.ethz.ch/isn/139669/1991-05_Measures_Short_War.pdf.

¹⁷ In the conducting of political warfare, there are no set rules of influence. You can do anything that is in the national interest, for example, use persuasion, intimidation, deception, corruption, penetration, subversion, negotiation, bluffing, psychological and economic pressure, seduction, blackmail, theft, fraud, rape and even murder. Generalizing, it can be assumed that state actors interact with the opposing party through non-military instruments, including intelligence, diplomatic, economic, information and other means without waging war, understood in its classical sense (Kennan, 1991: 8).

¹⁸ War is an armed conflict between states, blocs of states, nations or social classes, the continuation of policy by violent means to achieve certain political, economic or ideological interests (Small, 1971: 494).

¹⁹ M. Banasik, *Wojna hybrydowa w teorii i praktyce Federacji Rosyjskiej* [Hybrid warfare in the theory and practice of the Russian Federation], Bellona nr 4/2015, Warsaw 2015, pp. 157–192.

It is based on the assumption that the main battle space is the human mind, therefore all activities should be focused on informational and psychological activities²⁰. It is anticipated that it will also be possible to achieve the set political goals by influencing the behavioral sphere, at the core of which lies the manipulation of behavioral algorithms, habits, activities and stereotypes, as well as interfering in the cultural sphere²¹. However, one should not draw hasty conclusions and think that the new generation of war is limited to informational or psychological operations. Military force still plays a significant role in achieving strategic goals, as exemplified by Syria²².

GENESIS AND EVOLUTION OF RUSSIAN INFORMATION WAR

Modern Russian information war theory derives directly from special propaganda, first taught as a subject at the Russian Military Institute of Foreign Languages in 1942, and traces its roots to Marxist-Leninist ideology²³. The Kremlin has long sought information domination within the country and beyond its borders. Using a variety of instruments of informational impact, it has influenced events and people's behavior in states considered to be competitors and those remaining under Russia's sphere of influence. Some of the strategies, already used at the stage of the October Revolution and later in the Soviet Union, were subject to modification in accordance with changes in the political and military situation in the world. At this point it should be noted that the information space was used to conduct international competition both in peacetime and wartime²⁴.

After winning the revolution, issues of agitation and propaganda were of great importance to the Bolsheviks between 1918 and 1924. The Soviet administration sought to control the flow of information within the country through censorship and public diplomacy. Its propaganda and disinformation efforts shaped the term *agitpropaganda* as a result of combining the words agitation and propaganda. The agitation part was aimed at the emotions of the recipient, while propaganda was aimed at the mind. *Agitpropaganda* was regarded by the authorities as an information weapon, so the Soviet regime used it to create the conditions for achieving long-

²⁰ J. Bērziņš, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*, Policy Paper 2, Center for Security and Strategic Research, National Defence Academy of Latvia 2014, p. 5.

²¹ TL. Thomas, *Russian Forecasts of Future War*, *Military Review*, May-June 2019, p. 91.

²² J. Bērziņš, *The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria*, *The Journal of Slavic Military Studies*, 2020. 355-380, <https://doi.org/10.1080/13518046.2020.182410>.

²³ E. Lucas and P. Pomeranzen, *Winning the Information War*, Washington 2016, p. 6.

²⁴ *Information Security Doctrine of The Russian Federation*, Moscow 2000, p. 11.

term political goals. The high effectiveness of the Bolsheviks' propaganda work was appreciated even by their class enemies²⁵.

Initially, the propaganda machine was directed at the people of the Soviet Union. Gradually as it developed it was used to expand Soviet influence abroad and became one of the key elements of foreign policy. The Soviet Union financed ventures that, at their core, were critical of Western democracies and promoted the ideas of communism. As part of this policy, for example, peace movements in Europe that opposed the implementation of the US nuclear program were supported. Another example is the use of well-known Western thinkers and artists²⁶ to promote the ideas of the Soviet Union.

While the mechanisms of current Russian propaganda are similar to those of the past, the contemporary version no longer focuses on leftism, anti-colonialism, and labor, which made it valued during the Cold War. Instead of these ideologies, Russian propaganda is a postmodern negation of the liberal conception of Western society. It centers around the claim that democracy is a sham and politicians are bizarre hoaxes. The propaganda lacks a coherent message and the narrative is often contradictory. For example, Russian propaganda supports both left and far-right movements and all forms of protest. The only unifying feature of the news message is hostility and distrust of Western democratic society systems. Soviet propaganda was anchored in ideological truth claims, while the contemporary Russian variant of influence can be compared to a kaleidoscope, in which piercing lights are immediately transformed into multiple versions of reality²⁷.

A key component of foreign policy from the Russian Civil War to the Cold War was disinformation. The term has entered the international lexicon but has not always been understood correctly by the West. Disinformation in the Russian sense is not limited to false information intended to mislead the enemy. It is more a deliberate technique of deception used to achieve specific political goals²⁸. A carefully constructed false narrative, is covertly inserted into the communication system to deceive decision makers and the public being influenced. Disinformation can be political, economic, military or even scientific. To achieve the intended goal, any disinformation message should at least partially correspond to reality or generally accepted views, especially when the potential victim is experienced in the use of

²⁵ V. Brovkin, *Russia after Lenin*, Londyn and New York 2005, p. 81.

²⁶ Bernard Shaw argued that the Soviet Union was misperceived and misrepresented in the West (Drey, 2016).

²⁷ E. Lucas and P. Pomeranzev, *Winning ...*, p. 7.

²⁸ L. Bittman, *The KGB and Soviet Disinformation: An Insider's View*, Washington 1985, p. 50.

propaganda practices. After all, it is difficult to gain trust without reliable, verifiable information.

Strategic disinformation has always been aimed at misleading the adversary on fundamental questions of state policy, military and economic status, and scientific and technological progress achieved²⁹. For the Soviet leadership, disinformation was a key element of active measures to achieve specific political goals without resorting to military force, indicating the very broad scope of its use. The Soviet Union interfered in the policies of other states through active covert disinformation interventions. This consisted mainly of influencing European governments, undermining confidence in its leaders and state institutions, disrupting relations with other states, or discrediting and weakening opponents of pro-Russian authorities³⁰.

Disinformation in the Russian sense is a key component of psychological operations and is primarily aimed at manipulating the feelings of the recipient. It manifests itself as more than just the dissemination of false information by Russian-language television channels or Internet trolls. It is an attempt to sow doubt and confusion about Western political processes so that the victim is unable to learn the truth about reality. In short, the old strategies are implemented through new tools provided by digital media³¹.

During the Cold War, disinformation went one step beyond secretly injecting information into an adversary's communications system to deceive decision makers and the public. In the 1980s, the term "reflexive control" (rus. рефлексивное управление) defining the practice of strategic rivals making predetermined, unfavorable decisions for themselves. They were based on prepared information messages that changed the perception of reality³². In this context, reflexive control is a key asymmetric enabler of critical benefits to the impacted party by neutralizing the adversary's strengths and forcing the adversary to choose courses of action that are beneficial to the achievement of Russian political objectives³³. The focal point of reflexive control is the intangible inner nature of the adversary, his ideas and concepts of action. These elements constitute a kind of lens through which all information about the

²⁹ L. Bittman, *The KGB and Soviet Disinformation: An Insider's View*, Washington 1985, p. 51.

³⁰ E. Lucas and P. Pomeranzev, *Winning ...*, p. 7.

³¹ C. Collison, *Russia's Information War: Old Strategies, New Tools*. How Russia Built an Information Warfare Strategy for the 21st Century and What the West can Learn from the Ukraine Experience, 2017, p. 13.

³² M. Ajir and B. Vaillant, *Russian Information Warfare: Implications for Deterrence Theory*, Strategic Studies Quarterly, Fall 2018, Maxwell AFB 2018, p. 72.

³³ K. Giles, J. Sherr and A. Seaboyer, *Russian Reflexive Control*, Ontario 2018, p. 4.

external world is perceived. Information campaigns used in reflexive control are not limited to influencing a single decision. Influencing the adversary can lead him to reject subsequent decisions until he is choosing between a bad decision and an even worse one, with each option benefiting Russia³⁴.

Control over an opponent's decision, which ultimately involves taking a certain behavioral strategy over him, is not achieved either directly or by force. Rather, it is a matter of providing arguments from which he can logically infer the necessity of his own decision, but one that is predetermined. This can be achieved by applying pressure, by influencing the formulation of conclusions from assessments of the situation, by shaping the opponent's goals of action and algorithms of decision making, or finally by making him choose the moment of decision³⁵.

THE SIGNIFICANCE OF INFORMATION INFLUENCE IN YEVGENY MESSNER'S CONCEPT OF REBEL WAR

In the Russian Federation it is recognized that war is a complex, non-stationary, non-linear, stochastic phenomenon, difficult to predict and control³⁶. Any attempt to make war easy and safe according to the idea of direct contact warfare leads to destruction and disaster, therefore it is believed that future conflicts will be played out in the so-called "gray zone"³⁷, on unknown territory, in an unknown environment, against an unknown enemy and an unknown coalition. It will also not be possible to determine the exact time when the war will begin or end. A significant contribution to the theory of such wars was made by Yevgeny Messner, alongside such theorists as Frank Hoffman, Ivan Arreguín-Toft, Brian Bond, Arthur K. Cebrowski, John J. Garstka, and David S. Alberts³⁸. In the official documents of the General Staff of the Russian Federation it is assumed that modern wars are mostly hybrid and hybrid-information warfare³⁹. It is estimated that hybrid war is not a new phenomenon, and its theory was first articulated by Y. Messner, calling it "мятежевойна". Color revolutions, in which aggressive informational and

³⁴ K. Giles, *Handbook of Russian Information Warfare*, Rome 2016, p. 20.

³⁵ CW. Blandy, *Provocation, Deception, Entrapment: The Russo-Georgian Five Day War*, London 2009, p. 2.

³⁶ I.M. Kosachev, Yu.E. Kuleshov, I.M. Anoshkin, *Obosnovanie neobkhodimosti sozdaniya edinoy sistemy vozdušno-kosmicheskoy oborony soyuznogo gosudarstva v vostochnoevropeyskom regione kollektivnoy bezopasnosti*, Vestnik Voennoy Akademii Respubliki Belarus', No 1 (50) 2016, p. 54.

³⁷ M.J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, Army War College Press, December 2015.

³⁸ I.M.Kosachev, at all, *Obosnovanie ...*, p. 54.

³⁹ P.E. Kraynyukov, V.G. Abashin, D.A. Singilevich, *Protivodeystvie primeneniyu protivnikom v gibridnoy voyne informatsionno-psikhologicheskogo oruzhiya*, in: *Sovremenny miroporyadok i ego vliyanie na natsional'nuyu bezopasnost' Rossiyskoy Federatsii*, Moskva 2020, p. 260.

psychological actions play a key role, are cited as evidence⁴⁰. Unfortunately, Y. Messner's studies are known mainly to a narrow circle of geopolitical military experts⁴¹.

In the West, war is understood instrumentally. In contrast, Russian theorists such as Genrykh Leer, Alexandr Svechin, Aleksandr Golovin, Y. Messner, and Makhmut Gareev argued that war is not limited to military action, but also encompasses the economic, financial, business, and cultural spheres. In Russia, the idea of waging war through a combination of military and non-military means, called hybrid warfare found fertile ground, but it was not born in the West! This theory originated in the works of Y. Messner, the theory of network-centric and information-centric warfare⁴². According to Ofer Fridman, the Russian theory of hybrid war and its evolution called new generation war has nothing to do with F. Hoffman and the theory that was presented in the West after the annexation of Crimea in 2014, and is exclusively Russian military thought⁴³. When analyzing the Western and Russian theories of hybrid warfare, one can come to the conclusion that the Russian theory is more advanced as it is based on a broader philosophical and theoretical foundation⁴⁴.

Taking into account the arguments presented, it can be considered that the prototype of the concept of new generation wars, on the basis of which the Russian Federation is currently engaged in international competition, is the theory of rebel war formulated by Y. Messner⁴⁵. A well-known Russian theorist predicted the spread of the phenomenon of international terrorism and made a bold thesis that state security actors would not be prepared to counter such new threats⁴⁶. In his reflections on future conflicts, he pointed to the blurring of the distinction between the state of war and peace, between regular and irregular actions. The Russian strategist argued that the dominant form of struggle in the new wars, which he called rebellious, would be irregular actions. He included to them diversion, sabotage, terror, guerrilla and insurgent activities⁴⁷. He believed that in rebellion wars the boundaries between regular armed forces and ordinary citizens engaged in armed struggle would also become blurred.

⁴⁰ Ibidem, p. 260.

⁴¹ A.I. Buravlev, *O zadachakh mnogokriterial'nogo vybora*, Vooruzhenie i èkonomika No1 (55)/2021, p. 117.

⁴² O. Fridman, *Gibridnaya vojna ponyaty*, Review of International Relations, 5(50), 79-85, King's Research Portal 2016, p. 81.

⁴³ M. Göransson, *Understanding Russian thinking on gibridnaya vojna*, Hybrid Warfare: Security and Asymmetric Conflict in International Relations, London 2021, p. 83–94.

⁴⁴ O. Fridman, *Gibridnaya ...*, p. 81.

⁴⁵ L. Sykulski, *Rosyjska koncepcja wojen buntowniczych Jewgienija Messnera* [Yevgeny Messner's Russian Concept of Rebel Wars], *Przegląd Geopolityczny*, tom 11, 2015, Warsaw 2015, p. 105.

⁴⁶ Y. Messner, *Choczesz...*, p. 405.

⁴⁷ Ibidem, pp. 90 - 91.

Messner believed that, regardless of the applicable laws, every citizen had the right to participate in both overt and covert combat. He believed that the boundaries of the area where the future conflict would take place would become unclear. There will also be difficulties in distinguishing the actors of the warring parties, and the level of aggression will be of varying amplitude. It will also be impossible to distinguish between legitimate and illegitimate modes of international competition. He believed that regular armies would lose their monopoly on conflict resolution, which could lead to the emergence of new forms of conducting international rivalry, non-compliance with the principles of international law and war ethics⁴⁸. Y. Messner's concept assumed to avoid official state involvement in formal war. Instead, it envisioned the use of special subunits with no identifying marks, so that those involved in hostilities could not be treated as soldiers under international law. In addition, the state initiating the hostile action will be able to officially dissociate itself from such events, especially if the situation gets out of hand. Formally, therefore, there is a "de-stateization" of armed groups and the conflict itself, which from the outside may resemble a civil war and internal chaos. The more so as the main burden of fighting is shifted to urban areas, which is one of the factors characteristic for Y. Messner's conception⁴⁹.

Y. Messner assumed that the new forms of conducting international rivalry would involve civilian actors and ordinary citizens organized into national movements, insurgencies, and rebellions. Central to this rivalry would be the psychological aspect. He justified that in regular armies, psychology is generally of little importance and is only a complementary element. However, for fighting insurgents, separatists, terrorists or rebels, psychology plays a key and primary role. Y. Messner put forward a thesis that guerrilla wars and terrorist wars will constitute a separate type of war, which can be called psychological wars⁵⁰. In rebel wars, the psychology of the rebellious masses will override the armament of the regular troops and will be the decisive factor in victory or defeat. He argued that the psychological effect should be achieved not only through the use of surprising strategy and tactics aimed at the enemy troops, but above all at the enemy population, by intimidating it, exerting pressure, using blackmail,

⁴⁸ Ibidem, p. 70.

⁴⁹ L. Sykulski, *Rosyjska koncepcja wojen buntowniczych Jewgienija Messnera* [Yevgeny Messner's Russian Concept of Rebel Wars], *Przegląd Geopolityczny*, tom 11, 2015, Warsaw 2015, p. 109.

⁵⁰ Y. Messner, *Chociesz...*, p. 141.

guerrilla war⁵¹ and terrorist⁵². The author devoted much attention to conflicts bearing the hallmarks of revolution⁵³. In this aspect, he operated with the notion of semi-war, which he understood as undercover actions without overt signs of engaging in conflict. He indicated that aggressive diplomacy would play a large role in such semi-wars. He called it white-glove politics, using various forms of pressure and even international intimidation, imposing will or reaching consensus under pressure⁵⁴. He believed that diplomacy would be combined with subversive activities. Such semi-wars will involve guerrillas, terrorists, saboteurs, saboteurs, hooligans, devastators and propagandists, using the means of mass information. Demonstrations and demonstrations, unrest, terror, recruiting and calling for rebellion, will be aimed at changing the mentality of the people and constructing a new social system. In the opinion of Y. Messner, the overarching goal of the new generation war strategy will be to seek to destabilize state structures and, consequently, the collapse of the state. The feature of war will be omnipresent chaos, which is a negation of the theory of linear wars. In chaos it will not be possible to distinguish the defending side, as is the case in classical wars. It will not be clear where the attacking and defending sides are located. There will be difficulties in physically distinguishing defended objects. There will be no visible boundaries between the warring sides, especially in the cities where future conflicts will take place. Chaos will not be created haphazardly, but in a deliberate, systematized, and premeditated manner by central leadership. The most important element in future wars will be the belief in a just cause and overcoming the opponent's fighting spirit⁵⁵.

An effective weapon in the conducting of international competition will be information influence. Its goal will be to create discontent among social groups, divide political elites, as well as lower the reputation of the state, political isolation and hostile influence on

⁵¹ Y. Messner believed that the strength of the guerrillas lay in the fact that in small groups they could penetrate where regular troops could not. They attack like mosquitoes on a giant, stabbing, poisoning, drinking blood until the enemy falls. Guerrillas can change the location of their operations like swift water or a swift wind (Messner, 2005, p. 394).

⁵² Y. Messner, *Choczesz...*, p. 109.

⁵³ Y. Messner believed that the global revolutionary war had already begun during the Cold War. He pointed to revolutionary and anti-colonial independence movements in Africa, hunger marches in Washington, actions by European neo-fascists, and other types of protests, believing them to be directed from Moscow or Beijing. He considered revolutions, for example, the 1956 revolt in Hungary and the actions of the Death Squads in Latin America. Even in those days, he recognized the power of Islamic extremism, supported by ideology (Messner, 2005, p. 420).

⁵⁴ Y. Messner, *Choczesz...*, p. 110.

⁵⁵ *Ibidem*, p. 109.

international opinion⁵⁶. The primary factor and decisive for victory or defeat in the new generation war will be the psychological state of the rebellious masses, therefore it is advisable to integrate the impact of information with the conducting of long-term psychological activities⁵⁷. Unlike classical war, the goal of next-generation war will not be to capture the territory of an enemy state, but to capture the consciousness of its people.

Y. Messner believed that subversion war is a psychological war⁵⁸, therefore it will be focused on defeating the reason and spirit of the attacked nation and seizing its consciousness⁵⁹. It can be seen from the above statement that in a rebel war, the psychology of the masses relegates to the background the weapons at the disposal of the regular armies, and psychology itself becomes the determining factor in victory or defeat. Violence and intimidation, terrorist and guerrilla actions play a decisive role, while classical weapons play a secondary role. Thus, psychology becomes a substitute weapon, and the philosophy of its use can be compared to the use of pornography, drugs or brainwashing.

Based on the presented arguments, one can conclude that there will be a paradigm shift in the conduct of armed struggle. In classical interstate wars, the most important goal of combat was to capture and hold territory. In new generation wars, the goal of the action will be to conquer the minds of the population of the enemy state. In past wars the front line separated regular armies, in future wars there will be no boundaries either between the parties to the conflict, or the area of operations, or between the hostile society and the combatants, or between the legal and illegal ways of conducting armed struggle⁶⁰. The psychology of a fighting nation will be the fourth dimension of struggle⁶¹. The actors involved will be directed and supported logistically and financially from outside by the state, which will not officially be involved and will not be a party to the conflict.

Y. Messner believed that the strategy of waging a new generation of war is more difficult than the classical one because of the abundance of targets. The key in it will be to shatter the unity of the nation and lower its morale, as well as to defeat that part of the hostile society that

⁵⁶ Ibidem, pp. 232 - 246.

⁵⁷ L. Sykulski, *Rosyjska koncepcja wojen buntowniczych Jewgienija Messnera* [Yevgeny Messner's Russian Concept of Rebel Wars], *Przegląd Geopolityczny*, tom 11, 2015, Warsaw 2015, p. 110.

⁵⁸ In subversion warfare, it is best to approach the enemy from behind and use his own weapons. The effectiveness of subversion lies in the method of combat employed. The use of guerrilla warfare and subversion is usually effective, as well as the use of manipulation and cynicism (Cierniak, 2012).

⁵⁹ Y. Messner, *Chociesz...*, p. 394.

⁶⁰ Ibidem, p. 70.

⁶¹ Ibidem, pp. 135 and 395.

is able to resist. This will be aided by the seizure or destruction of objects of key importance to the functioning of society and the evocation of negative images in the minds of the people⁶².

The overarching strategic goal of rebel war is the enslavement of the enemy nation. This is not about the physical dimension. It is more about the psychological effects achieved as a consequence of destroying the ideology, sowing doubt, leading to disillusionment and despondency, and reasserting the conviction of the rightness of the ideas imposed and ultimately the recognition of their superiority. The means of achieving strategic goals is propaganda, which has the same importance and significance as achieving military victories or using terrorist attacks.

Agitation will also play a major catalyst in the conducting of international competition. |Y. Messner distinguished between offensive agitation, aimed at weakening the rival, and defensive agitation, strengthening the fighting spirit of one's own society⁶³. He was also a proponent of revealing half-truths claiming that one half-truth is for one's own and the other is for the enemy, therefore war requires the art of waging it in a psychological dimension A⁶⁴. As history has shown, his words came true completely, especially after V. Putin came to power.

THE STRATEGIC ASPECT OF INFORMATION WAR-NOTIONAL DILEMMAS

In Russian terminology, the term "information war" is used alongside the term "information confrontation." Both of these terms cover a wide range of strategic actions in which information is treated as a tool, target, or information domain. Conceptually, information war operationally integrates such distinct forms of strategic influence as psychological operations, strategic communication, intelligence and counterintelligence operations, so-called maskirovka⁶⁵, disinformation, electronic war, impairment of communications capabilities, degradation of navigational support, psychological pressure, and destruction of adversary information technology capabilities⁶⁶. The operational concept of information war encompasses all the activities listed above creating a system, methods and tasks dedicated to influencing the perception of reality and the behavior of decision-makers and citizens of the

⁶² An example of such a facility would be the World Trade Centre towers destroyed in the terrorist attack.

⁶³ Y. Messner, *Choczesz...*, p. 134.

⁶⁴ *Ibidem*, p. 135.

⁶⁵ Maskirovka includes, but is not limited to, camouflage, deception, subversive actions, psychological operations, sabotage, espionage, and propaganda (Roberts, 2015).

⁶⁶ K. Mshvidobadze, *The Battlefield on Your Laptop*, 21.03.2011.

state, as well as the international community. It uses a systemic approach, based on perception management, targeting the enemy's leadership and changing its orientation so that it makes decisions favorable to Russia, while leading to a sense of helplessness on the part of the state to create grounds for negotiations on Moscow's terms⁶⁷.

Based on an assessment of the Russian doctrinal documents, it can be assumed that Russian information campaigns are multidisciplinary in nature and include the political, economic, military, social, and cyber spheres, as well as intelligence, diplomacy, psychological operations, communications, and education (Vojna). The information war conducted by the Russian Federation involves the use of the Russian-speaking diaspora, which is widely represented in the world, influencing the consciousness of the masses, both at home and abroad, and creating conditions for conducting a civilizational struggle between Russian Eurasian culture and Western culture, which has deep social, social, military and technological roots. At present, information war is becoming a lever through which the state with greater efficiency can apply a variety of instruments of influence in international competition and achieve the assumed political goals. Information is directly related to the geopolitics conducted for the benefit of the Russian state. Through coordinated manipulation of the information sphere, including newspapers, television, websites, blogs, and other mass media, attempts are made to create a virtual reality, influencing the public's perception of the world, in a manner favorable to the RF, and even to replace the image of truth with pro-Russian fiction⁶⁸.

According to Russian experts, one of the features of the war of the future will be information confrontation (Vojna). It seems that this concept most closely reflects the nature of informational interaction in terms of the international competition conducted by the RF. The use of the term war is rather a fashion for military semantics in international relations. One should not misuse the word "war" and confuse the phenomenon of war with its attributes, forms of its conduct and ways of influencing the opposing side. The use of the term "information war" may be unauthorized, because war is in its essence a complex socio-political phenomenon. It involves confrontation between political systems, classes, nations and states, with armed violence aimed at achieving specific political goals. It means the conducting of

⁶⁷ A.J.C. Selhor, *Russia's Perception Warfare. The development of Gerasimov's doctrine in Estonia and Georgia and its application in Ukraine*, Jaargang 185 Nummer 4 – 2016, p. 151.

⁶⁸ *Little Green Men: A Primer on Modern Russian Unconventional Warfare*, Ukraine 2013–2014, Fort Bragg 2016, p. 15.

warfare, including the overall mobilization of both people and economy. To be successful in warfare, military strategy is also needed⁶⁹.

Thus, it seems that war should not have connotations of informational impact. Nevertheless, it can be considered that informational interaction is a process belonging to the phenomenon of war. In RF, it is assumed that both the term "information war" and "information confrontation" are legitimate concepts, as they express the struggle of opposing parties for quantitative, qualitative and speed advantages in acquiring, analyzing and using information (Vojna). It is clear that information confrontation, like other types of confrontation, can be defensive and offensive in nature. The defensive character consists in protecting one's own information from the impact of the enemy. The offensive character is expressed in disorganizing the functioning or eliminating the enemy's information infrastructure and disrupting the processes of exercising operational control over security actors and the capabilities they use. In relation to information confrontation, the term information intervention or information aggression can be used interchangeably. Due to the fact that we are now dealing with new generation wars⁷⁰, the role of information confrontation is rapidly increasing. It is expressed in the struggle against control systems, in the imposition of its own rules of competition on the opponent and in the pursuit of military and technical superiority (Vojna). Information confrontation is constantly evolving along with the development of modern methods of conducting combat. It focuses mainly on finding the weakest points in adversary's command, control, communication, information support systems and cognitive processes, which is supposed to increase the effectiveness of influence in other than military spheres of confrontation. A critical part of the adversary's command and control systems are its information assets, the disruption or destruction of which will lead to an immediate reduction in operational capabilities. The pinnacle achievement and, at the same time, the key to conducting an information confrontation would be for the RF to have a global information system capable of controlling European states and, above all, of reducing the effectiveness of their capabilities (Vojna).

According to Valentin Kiselev, informational confrontation materializes in actions aimed at securing the desired influence on the mental sphere, emotional and behavioral attitudes, and

⁶⁹ O. Fridman, *Gibridnaya ...*, p. 81.

⁷⁰ In the Russian Federation, it is assumed that the new generation war will take place in the information sphere, which in general corresponds to the Western notion of political war.

moral and psychological state of the opponent⁷¹. Therefore, it can be concluded that information confrontation will involve affecting information networks and/or information, and its main efforts will be focused on state institutions and officials responsible for making the most important decisions in the state. The main forms, methods and techniques of information confrontation will be conducting psychological operations and creating the effect of a permanent Russian presence, misleading the adversary, radio-electronic interference and physical destruction of important information infrastructure facilities, as well as influencing key state officials and conducting aggressive in its nature operations in cyberspace⁷².

Sergei Chekinov and Sergei Bogdanov believe that in future wars, without the use of overt aggression, international rivalry will focus on the information domain. This is supported by the fact that information will play an integrative role in the functioning of the political, military, economic, technological and environmental spheres. Therefore, new forms of influence will gain importance, in which mass media and social networks and global online networks will be widely used, as well as hitherto unknown forms of information communication⁷³.

In the Russian literature devoted to affecting the cognitive sphere of the enemy, alongside the concept of information war, the terms cyberspace, cyberwar, cyberattack have become well-established, the contents of which suggest antagonism or even combat conducted in the virtual world. The concept overriding the mentioned terms is cybernetics, understood as the science of management, communication and information processing. The main object of study of cybernetics are the so-called cybernetic systems, which are treated abstractly, regardless of their material nature. Cybernetics develops general principles for the creation of control systems and automation systems, and information is a key element of them⁷⁴. As noted earlier, cyberspace includes information and management processes. Therefore, it is possible, on the one hand, to understand cyberspace as a part of the information space, limited to the area related to information management technologies and, on the other hand, to information technologies. The processes of receiving, transmitting and processing information called

⁷¹ W.A. Kisielew, *K kakim vojnám nieobchodimo gotovít Woorúžennyje Síly Rossii*, *Vojennaja Mysl*, Nr 4, Moscow 2017.

⁷² Ibidem.

⁷³ SG. Chekinow and SA. Bogdanow, *Prognozirowanije charaktiera i sodierzhanija vojn buduszczego: problemy i suždienija* [Predicting the Nature and Content of Future Wars: Problems and Judgments], *Vojennaja Mysl*, Nr 10, Moscow 2015, pp. 44 - 45.

⁷⁴ Pl. Antonovich, *O sushchnosti i sodierzhanii kibervoinny* [On the essence and meaning of cyberwarfare], *Voennaya Mysl' № 07/2011*, Москва 2011, pp. 39 – 46.

information processes are a component part of cyber management processes. Therefore, in the RF it is assumed that the information space is a part of the cyber space. This is due to the fact that in the case of information space and cyber space it is quite difficult to apply spatial relations in the usual sense, since they are built and accepted mentally in people's imagination, thus in a virtual way. The above logic leads to the conclusion that the synonym of cybernetic space is virtual space⁷⁵.

Russian claims that cognitive processes take place in the information space, which refers to both information processes and human consciousness, rather than in cyberspace, are correct. This can also be evidenced by the Russian Federation's separation of two separate domains of information war in the information sphere, namely information-technical, targeting systems for receiving, collecting, processing and transmitting information, and information-psychological, targeting armed forces personnel and civilians⁷⁶. At this point, it should be noted that cyberspace activities do not directly relate to the information-technology domain, understood as an integral part of the information space. Instead, they are used to conduct information-psychological operations. It should be noted, however, that some activities in both domains are undertaken constantly, regardless of the state of the relationship with the strategic rival⁷⁷.

Operations in cyberspace are conducted within the broader concept of information war⁷⁸. Cyberspace is regarded as a medium through which a state can dominate the information landscape. It is also considered a domain in which warfare is possible. Cyberspace makes it possible to integrate the conduct of propaganda, disinformation and psychological operations at the same time, which is reflected doctrinally. Information war should be used at the earliest possible stage of competition, in order to achieve certain political benefits without the need to use military force. If used, the goal of information war should be to shape a positive response from the international community (The Military, 2010)⁷⁹. The provisions of the 2010 military doctrine suggest that information war should be used prior to the commencement of a military operation in order to confuse and demoralize the adversary and justify the need for aggression.

⁷⁵ Ibidem.

⁷⁶ TL. Thomas, *Russian Information Warfare Theory: The Consequences of August 2008*, [in:] *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, Blank SJ, Weitz R (red.), Carlisle 2010, p. 275.

⁷⁷ K. Giles, *Handbook ...*, p. 9.

⁷⁸ TL. Thomas, *Nation-State Cyber Strategies: Examples from China and Russia*, 2017, p. 12.

⁷⁹ *The Military Doctrine of the Russian Federation*, Moscow 2010.

Thus, information war conducted in cyberspace, becomes a legitimate tool of international influence in both peacetime and wartime⁸⁰.

Modern technologies can provide a higher level of effectiveness of the operational capabilities of the RF and enable exploitation of the weaknesses of the strategic rival. Unlike the information campaigns of the past, they provide the opportunity to achieve strategic effects more quickly by influencing the cognitive sphere of the rival. Modern information technologies make it possible to remotely influence all major institutions and critical infrastructure of the state that the RF wishes to influence. They make it possible to enter the territory of a rival entity in an unconventional way without the need to use conventional military forces. Moreover, thanks to modern information technologies it is possible to support from the outside any opposition to the legitimate authorities, and even to carry out terrorist attacks, which contributes to the achievement of the strategic objectives of the competition, which may be the creation of instability and chaos and the degradation of states without the use of armed violence⁸¹.

Cyberspace in the conducting of information war is relegated to a supporting role in the Russian Federation's achievement of information dominance at all stages of the international competition. According to the traditional Leninist view of reality, ideological internal and external threats are permanent, and the struggle against them in the information space is a never-ending process. In other words, in this struggle it knows no boundaries, either physical or temporal. This contrasts sharply with Western, and especially American, conceptions of the use of cyberspace, which is seen as a separate sphere of influence dedicated to information war and its associated psychological aspects⁸². According to Russian assumptions, operations in cyberspace are strategic and long-term, not operational or tactical. It should be emphasized that the key in conducting Russian information war is to achieve psychological⁸³.

According to Russian theorists, information war in cyberspace is of strategic importance because it disorganizes the functioning of the state and influences the formation of pro-Russian attitudes in the affected society. In this context, information operations in cyberspace provide the Russian government with a clandestine means to achieve the goals of international

⁸⁰ TL. Thomas, *Nation-State Cyber Strategies: Examples from China and Russia*, 2017, p. 266.

⁸¹ Yu. Danik, T. Malyarchuk and Ch. Briggs, *Gibridnaya vojna: khay-tek, informatsionnye i kiber konflikty* [Hybrid warfare: high-tech, information and cyber conflicts], *Connections* QJ16, no. 2 (2017), p. 9.

⁸² M. Connell and S. Vogler, *Russia's Approach to Cyber Warfare*, Washington 2016, p. 5.

⁸³ *Ibidem*, p. 6.

competition in peacetime, while allowing it to maintain a degree of plausible deniability about Russia's involvement in disinformation campaigns⁸⁴. In the top leadership of the Armed Forces of the RF, there is a belief that through the use of modern technologies, information and psychological war largely lays the groundwork for the possibility of achieving significant political successes in the international arena⁸⁵.

INFORMATION WAR IN OPERATIONAL PRACTICE

In the Russian Federation, it is believed that the implementation of foreign policy objectives is not possible without the use of the information sphere, especially the media⁸⁶. To this purpose, Russia has developed an extensive, well-functioning media arsenal primarily embedded in the Rossiya Segodnya and RT platforms. They have the capacity to broadcast on multiple radio and television channels, provide photographic and infographic content, and spread information across social media and mobile devices. Authorities influence social media by sponsoring troll farms that run blogs and tweets on behalf of the Kremlin. They manipulate information and try to change the narrative in Russia's favor⁸⁷. The media regularly disseminates information that reflects the regime's point of view and casts doubt on Western messages and thus influences the formation of public opinion abroad⁸⁸. The RF seeks to moderate the discussion on social media by placing political advertisements on various platforms and promoting selected news stories, often using a false narrative. For example, in October 2017, during a hearing before a U.S. Senate Judiciary subcommittee, Twitter lawyers revealed that 1.4 million tweets came from Russian bots during the 2016 presidential election. These efforts were designed to fuel political and social divisions⁸⁹. Through alternative messages, Russia attacks or undermines the credibility of individuals or institutions perceived

⁸⁴ SG. Chekinov and SA. Bogdanov, *Voennoe iskusstvo na nachal'nom ètape XXI stoletiya: problemy isuzhdeniya* [The Art of War at the Beginning of the 21st Century: Problems and Judgments], Voennaya Mysl' No. 1, 2015, Moscow, pp. 32 - 43.

⁸⁵ SG. Chekinov and SA. Bogdanov, *O kharaktere i soderzhanii voyny novogo pokoleniya* [On the Nature and Content of the New Generation War], Voennaya Mysl' No. 4, Moscow 2013, 13–24.

⁸⁶ L. Robinson, at all, ... p. 52.

⁸⁷ *Russia Military ...*, p. 40.

⁸⁸ L. Robinson, at all, ... p. 67.

⁸⁹ H. Shaban, C. Timberg, E. Dwoskin, *Facebook, Google and Twitter testified on Capitol Hill. Here's what they said*, Washington Post 31.10.2017.

to have a negative impact on Russian interests. Specifically, this includes the promotion of news articles clearly hostile to the European Union and NATO⁹⁰.

An example of strategic-scale propaganda campaigns and deliberate manipulation of information is the conflict in Ukraine. In a disinformation campaign unprecedented in scale, all available television channels, radio, newspapers and Internet resources were used. At the beginning of the Ukrainian crisis, disinformation was integrated with ideological, political, social, cultural diversion, provocations and diplomatic activity. The mechanisms of information influence were intended to lend credibility to Moscow's peaceful intentions and to mask the shortcomings of its argumentation as to the use of military force⁹¹. Furthermore, Russian state media portrayed the Maydan revolution as a fascist and extremely Russophobic movement. The narrative they created was an important instrument in Moscow's information war, which played a very important role in mobilizing local pro-Russian forces⁹². The information impact focused on the Ukrainian society was simultaneously combined with a large-scale information campaign of foreign influence. Russian media platforms conducted public opinion-oriented disinformation activities against Western states. Additionally, Moscow attempted to use pro-Russian foreign media outlets that presented the Kremlin's political views on social media⁹³.

With regard to the conflict with Ukraine, the Russian Federation at the strategic level for a long time, through reflexive control, succeeded in confusing the West about the number of troops deployed by them and their real political-military objectives. Moreover, Moscow succeeded in creating a situation in Ukraine that could not be fully considered either in the context of the laws of war or peaceful relations under modern international norms, due to the flow of Russian weapons and the military assistance provided to the separatists. As a result, the Russian Federation was considered one of the signatories to the Minsk agreements rather than a belligerent party. Nor was Moscow held primarily responsible for causing the crisis situation in Ukraine⁹⁴. On the tactical aspect in Crimea, the systematic Russian campaign of reflexive

⁹⁰ L. Morris, M. Mazarr, M. Jeffrey, W. Hornung, S. Pezard, A. Binnendijk and M. Kepe, *Gaining Competitive Advantage in the Gray Zone. Response Options for Coercive Aggression Below the Threshold of Major War*, Santa Monica 2019, p. 18.

⁹¹ J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska - studium przypadku* [Anatomy of Russian information warfare. The Crimean operation - a case study], (in:) Punkt widzenia 2014, nr 42, wyd. OSW, Warsaw, p. 5.

⁹² H. Riesinger and A. Golts, *Hybrider Krieg in der Ukraine. Russlands Intervention und die Lehren für die NATO* [Hybrid War in Ukraine. Russia's Intervention and the Lessons for NATO], „Osteuropa” 2014, nr 9–10, p. 125.

⁹³ A. Shekovtsov, *The challenge of Russia's antiinformation warfare*, in: *Diplomaatia, Sonderheft*, April 2014.

⁹⁴ C. Kasapoglu, *Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control*, Research Paper NATO Defense College No. 121, Rome 2015, p. 6.

control was successful in providing Russian forces with critical cover in the form of successful deception to deploy and maneuver troops to take control of key facilities and positions, as well as deep penetration to cripple any potential Ukrainian response. On an operational level, Russian military groupings along border areas during the covert invasion of Crimea served not only to cripple Ukrainian military formations, but also to mislead leaders in Kiev and the West as to the true intent and scope of the impact in Ukraine⁹⁵.

Russia is increasingly using cyberspace for its political and military campaigns. It makes it possible to disrupt the functioning of an attacked state by causing the denial of services provided by critical infrastructure. For example, in December 2015, Russia planned and executed a sophisticated attack on the Ukrainian power grid leaving 230,000 Ukrainian residents without electricity the day before Christmas. The attackers invalidated the operators' password access to the system and also turned off backup generators⁹⁶. In June 2017, the so-called NotPetya virus, which resulted from a targeted attack on Ukrainian accounting systems, spread to 64 states and affected large multinational companies, logistics operators, government agencies, telecommunications providers, and financial institutions. The name NotPetya referred to the covert nature of the attack, which appeared as a ransomware attack (Petya), but was actually designed to destroy and delete information from information systems in Ukraine. It turned out that NotPetya was a cyber form of masquerade intended to misrepresent the true source and intent of the attack. In February 2018, the U.S. administration attributed NotPetya to Russian armed forces⁹⁷.

The Russian Federation combines cyberattacks with psychological operations and the opportunities afforded by social media platforms. In January 2017, Russian influence was aimed at discrediting anti-Kremlin presidential candidate Hillary Clinton. The U.S. intelligence community noted that the Russian goal in the U.S. presidential election was to undermine public faith in the democratic process, which it sought to achieve through a strategy that combined covert cyber intelligence operations with overt actions by Russian government agencies and proxy entities⁹⁸.

⁹⁵ Ibidem, p. 6.

⁹⁶ K. Zetter, *Inside the cunning, unprecedented hack of Ukraine's power grid*, wired 08.03.2017.

⁹⁷ A. Polyakova and SP. Boyer, *The Future ...*, p. 14.

⁹⁸ Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution, U.S. Office of the Director of National Intelligence 07.01.2017.

Russian attempts to interfere in internal affairs, especially in the elections that have taken place in Europe, have been seen to varying degrees. Internet troll farms have been used to spread false information. Their actions were synchronized with the process of automatic generation of fictitious accounts using a bot virus. This model of strategic influence was used during the campaign of French presidential candidate Emmanuel Macron in spring 2017. Another example is the disinformation campaign conducted in October of the same year during the Catalan independence referendum in Spain. In each case, the tools and objectives were the same. Disinformation campaigns were used, cyber-attacks were carried out, supporters of the Russian Federation were promoted, surrogate actors were used, and political subversions were attempted, all of which were intended to divide society and destabilize the internal situation of the state under attack⁹⁹.

CONCLUSIONS

The Russian perception of contemporary international rivalry is based on the idea of playing out the struggle in people's minds, and its foundation is the concept of new generation war. Past experience in Chechnya and Ukraine and an assessment of the theory confirm that the Russian Federation's international rivalry is focused on multidimensional and multilevel efforts aimed at destabilizing the functions of states and changing their internal order. It is important to note that the new generation war is a permanent war, which means that with it comes the concept of a permanent adversary. In the current geopolitical structure, it is clear that for Russia the adversary is Western civilization, its cultural values, political system and ideology¹⁰⁰. In these conditions, information war becomes a perfect mechanism for conducting international rivalry to frustrate and decompose the moral society and to enable the achievement of psychological advantage, which consequently creates the conditions for achieving its goals.

The conclusions of the conducted research allow us to claim that the Russian concept of conducting information war should not be identified with either Western concepts of conducting information operations or information activities. Its scope is much broader, and the forms and methods of using information allow for the integrated use of various instruments of

⁹⁹ A. Polyakova and SP. Boyer, *The Future ...*, p. 3.

¹⁰⁰ J. Bērziņš, *Russia's New ...*, p. 4.

influence, which makes it an extremely sophisticated and effective mechanism of international influence.

Information war should not be confused with operations conducted in cyberspace. Russia treats cyberspace activities as a subset of a much broader informational impact conducted as part of international competition. Since 2014, Russian information war has commonly been erroneously reduced to disinformation in non-specialist literature. The Russian approach to information war is much broader than spreading lies and maintaining a false narrative. Russian state and non-state actors use history, culture, language, nationalism, and discontent to conduct information campaigns aimed at achieving the strategic goals of the ongoing international competition. Accordingly, they creatively select tools and unconventional methods to influence the opposing side. Information war waged by the RF has the character of confrontation with European states in the information space, and its consequence is the destruction of information systems, processes and resources. It is also critical to weakening any political, military, economic and social system. In the RF, it is believed that mass brainwashing of people leads to destabilization of society and the state. Moreover, it forces the confronting state to make decisions in the interests of the attacking side.

In influencing Europe, the RF will exploit human gullibility, the vulnerabilities of the social media ecosystem, and the lack of public awareness and policy makers. However, over the next three to five years, the tools used by Russia will become more sophisticated and difficult to detect. Technological advances leading to the creation of advanced artificial intelligence and the acquisition of new cyber capabilities will open up opportunities for malware and viruses to undermine democracy in a more stealthy and far more effective manner than has been the case to date¹⁰¹. Moreover, increasingly sophisticated cyber tools, primarily tested by Russia in Eastern Europe, are already affecting the systems of other European states. It seems that massive strikes in cyberspace in combination with other, informational instruments of influence are inevitable, so one should be aware that sooner or later they will come to be faced.

Challenges and threats to European states in the information domain are not static, but are constantly and rapidly evolving. The RF learns from its own operational experience and adapts the tools, forms and methods of information influence to the situation and the needs of achieving specific political goals of international competition. Therefore, an adaptive attitude

¹⁰¹ T. Hwang, *Digital disinformation: A primer*, Atlantic Council, Washington 2017.

of the international community to the threats posed by the Russian information war is necessary. Secondly, it should be taken into account that in conducting information operations the Russian Federation will strive to achieve effects simultaneously on the whole territory of the attacked state, both in the physical and virtual information domain. It is also worth remembering that in conducting international competition the RF uses a holistic approach. This means that Europe should be prepared to counter information campaigns integrated with subversive, special and unconventional operations aimed at changing the legitimate authorities of the state that the RF will influence in the future.

Funding

The author received no financial support for the research, authorship, and/or publication of this article.

REFERENCES LIST

- Ajir M. and Vailliant B., *Russian Information Warfare: Implications for Deterrence Theory*, Strategic Studies Quarterly, Fall 2018, Maxwell AFB 2018.
- Antonovich Pl., *O sushchnosti i soderzhanii kibervoyny* [On the essence and meaning of cyberwarfare], Voennaya Mysl' № 07/2011, Moskva 2011.
- Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution, U.S. Office of the Director of National Intelligence 07.01.2017.
- Banasik M., *Wojna hybrydowa w teorii i praktyce Federacji Rosyjskiej* [Hybrid warfare in the theory and practice of the Russian Federation], Bellona nr 4/2015, Warsaw 2015.
- Bērziņš J., *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*, Policy Paper 2, Center for Security and Strategic Research, National Defence Academy of Latvia 2014.
- Bērziņš J., *The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria*, The Journal of Slavic Military Studies, 2020. 355-380, <https://doi.org/110.1080/13518046.2020.182410>.
- Bittman L., *The KGB and Soviet Disinformation: An Insider's View*, Washington 1985.
- Blank S., *Signs of New Russian Thinking About the Military and War*, Eurasia Daily Monitor Volume: 11 Issue: 28, 2014. 13.02.2014, <https://jamestown.org/program/signs-of-new-russian-thinking-about-the-military-and-war/>, accessed 22.02.2021.
- Brovkin V., *Russia after Lenin*, Londyn and New York 2005.
- Buravlev A.I., *O zadachakh mnogokriterial'nogo vybora*, Vooruzhenie i ekonomika No1 (55)/2021; <http://www.viek.ru/55/131-138.pdf>, accessed 11.11.2021.
- Chekinov SG. and Bogdanov SA., *O kharaktere i soderzhanii voyny novogo pokoleniya* [On the Nature and Content of the New Generation War], Voennaya Mysl' No. 4, Moscow 2013.
- Chekinov SG. and Bogdanov SA., *Voennoe iskusstvo na nachal'nom ètape XXI stoletiya: problemy isuzhdeniya* [The Art of War at the Beginning of the 21st Century: Problems and Judgments], Voennaya Mysl' No. 1, Moscow 2015.

- Chekinow SG. and Bogdanow SA., *Prognozirowanije charaktiera i sodierżanija vojn buduszczego: problemy i sużdienija* [Predicting the Nature and Content of Future Wars: Problems and Judgments], Vojennaja Mysl, Nr 10, Moscow 2015.
- Cierniak J., *Subwersja czyli sztuka inteligentnego oporu* [Subversion or the art of intelligent resistance], Portal Krytyka.org, 13.06.2012, <http://krytyka.org/subwersja-czyli-sztuka-inteligentnego-oporu/>, accessed 03.07.2019.
- Čížik T., (ed.), *Information Warfare – New Security Challenge for Europe*, Centre for European and North Atlantic Affairs (CENAA), Bratislava 2017.
- Collison C., *Russia's Information War: Old Strategies, New Tools. How Russia Built an Information Warfare Strategy for the 21st Century and What the West can Learn from the Ukraine Experience*, 2017, https://jsis.washington.edu/ellisoncenter/wp-content/uploads/sites/13/2017/05/collison_chris_Russia%E2%80%99s-Information-War-Old-Strategies-New-Tools-How-Russia-Built-an-Information-Warfare-Strategy.pdf, accessed 11.11.2020.
- Conley HA., Mina J., Stefanov R. and Vladimirov M., *The Kremlin Playbook. Understanding Russian Influence in Central and Eastern Europe*, Lanham • Boulder • New York • London 2016.
- Connell M. and Vogler S., *Russia's Approach to Cyber Warfare*, Washington 2016.
- Danik Yu., Malyarchuk T. and Briggs Ch., *Gibridnaya vojna: khay-tek, informatsionnye i kiber konflikty* [Hybrid warfare: high-tech, information and cyber conflicts], Connections QJ16, no. 2, 2017.
- Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska - studium przypadku* [Anatomy of Russian information warfare. The Crimean operation - a case study], (in:) Punkt widzenia 2014, nr 42, wyd. OSW, Warsaw.
- Fridman O., *Gibridnaya vojna ponyaty*, Review of International Relations, 5(50), 79-85, King's Research Portal 2016; <https://core.ac.uk/download/pdf/195273338.pdf>, accessed 27.12. 2021.
- Giles K., *Handbook of Russian Information Warfare*, Rome 2016.
- Giles K. and Seaboyer A., *The Russian Information Warfare Construct*, Kingston 2019.
- Giles K., Sherr J. and Seaboyer A., *Russian Reflexive Controle*, Ontario 2018.
- Hoffman F., *The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War*, The Heritage Foundation 2016.
- Hwang T., *Digital disinformation: A primer*, Atlantic Council, Washington 2017.
- Information Security Doctrine of The Russian Federation*, Moscow 2000.
- Kasapoglu C., *Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control*, Research Paper NATO Defense College No. 121, Rome 2015, https://www.files.ethz.ch/isn/195099/rp_121.pdf, accessed 04.06.2015.
- Kennan GF., [w:] Harlow GD., Maerz GC., eds., *Measures Short of War: The George F. Kennan Lectures at the National War College, 1946–1947*, Washington 1991, https://www.files.ethz.ch/isn/139669/1991-05-Measures_Short_War.pdf, accessed 16.10.2019.
- Kisielew WA., *K kakim vojnám nieobchodimo gotowiť Woorużennyje Sify Rossii*, Vojennaja Mysl, Nr 4, Moscow 2017.
- Kosachev I.M., Kuleshov Yu.E., Anoshkin I.M., *Obosnovanie neobkhodimosti sozdaniya edinoj sistemy vozdušno-kosmicheskoy oborony soyuznogo gosudarstva v vostochnoevropejskom regione kollektivnoy bezopasnosti*, Vestnik Voennoy Akademii Respubliki Belarus', No 1 (50) 2016, https://varb.mil.by/nauka/vestnik/PDF/Vestnik_1-2016.pdf, accessed 31.03.2016.
- Kraynyukov P.E., Abashin V.G., Singilevich D.A., *Protivodeystvie primeneniyu protivnikom v gibridnoy voyne informatsionno-psikhologicheskogo oruzhiya*, in: *Sovremenny miroporyadok i ego vliyanie na natsional'nuyu bezopasnost' Rossiyskoy Federatsii*, Moskva 2020, https://www.rusarmyexpo.ru/business_program/4096/33362.html, accessed 27.09.2020.
- Little Green Men: A Primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014*, Fort Bragg 2016.

- Lucas E. and Pomeranzev P., *Winning the Information War*, Washington 2016.
- Mazarr M.J., *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, Army War College Press, December 2015.
- Messner Y., *Choczesz Mira, Pobiedi Miatieżewojnu!* [You want Peace, Defeat Rebellion!], Moscow 2005.
- Morris L., Mazarr M., Jeffrey M., Hornung W., Pezard S., Binnendijk A. and Kepe M., *Gaining Competitive Advantage in the Gray Zone. Response Options for Coercive Aggression Below the Threshold of Major War*, Santa Monica 2019.
- Mshvidobadze K., *The Battlefield on Your Laptop*, 21.03.2011, https://www.rferl.org/a/commentary_battlefield_on_your_desktop/2345202.html, accessed 06.11.2020.
- Polyakova A. and Boyer SP., *The Future Of Political Warfare: Russia, The West, And The Coming Age Of Global Digital Competition*, The New Geopolitics Europe 2018.
- Pronk D., *The Return of Political Warfare*, Strategic Monitor 2018-2019.
- Riesinger H. and Golts A., *Hybrider Krieg in der Ukraine. Russlands Intervention und die Lehren für die NATO* [Hybrid War in Ukraine. Russia's Intervention and the Lessons for NATO], „Osteuropa” 2014, nr 9–10.
- Roberts JQ., *Maskirovka 2.0: Hybrid Threat*, Hybrid Response, Washington 2015.
- Robinson L., Helmus TC., Cohen RS., Nader A., Radin A., Magnuson M. and Migacheva K., *Modern Political Warfare. Current Practices and Possible Responses*, Santa Monica 2019.
- Russia Military Power. Building a Military to Support Great Power Aspirations*, Defense Intelligence Agency, Washington 2017.
- Selhor AJC., *Russia's Perception Warfare. The development of Gerasimov's doctrine in Estonia and Georgia and it's application in Ukraine*, Jaargang 185 Nummer 4 – 2016.
- Shaban H., Timberg C., Dvoskin E., *Facebook, Google and Twitter testified on Capitol Hill. Here's what they said*, Washington Post 31.10.2017.
- Shanker T. and Landler M., *Putin Says U.S. is Undermining Global Stability*, The New York Times 2007, 11.02.2007.
- Shekovtsov A., *The challenge of Russia's antiinformation warfare*, in: *Diplomaatia, Sonderheft*, April 2014.
- Sukhankin S., *The Western Alliance In The Face Of The Russian (Dis) Information Machine: Where Does Canada Stand?*, SPP Research Paper, Volume 12:26 September 2019, Calgary 2019.
- Sykulski L., *Rosyjska koncepcja wojen buntowniczych Jewgienija Messnera* [Yevgeny Messner's Russian Concept of Rebel Wars], *Przegląd Geopolityczny*, tom 11, 2015, Warsaw 2015, 103–112.
- The Military Doctrine of the Russian Federation*, Moscow 2010.
- Thomas TL., *Nation-State Cyber Strategies: Examples from China and Russia*, 2017, <https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-20.pdf?ver=2017-06-16-115054-850>, accessed 11.11.2020.
- Thomas TL., *Russian Information Warfare Theory: The Consequences of August 2008*, [in:] *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, Blank SJ, Weitz R (red.), Carlisle 2010.
- Thomas TL., *Russian Forecasts of Future War*, *Military Review*, May-June 2019, 84–93.
- Ven Bruusgaard K., *Crimea and Russia's Strategic Overhaul*, *Parameters*, Vol. 44, No. 3, Autumn 2014.
- Vojennaja doktrina Rossijskoj Fiedieracyi* [The Military Doctrine of the Russian Federation], Москва 2014.
- Zetter K., *Inside the cunning, unprecedented hack of Ukraine's power grid*, *Wired* 08.03.2017.



Copyright (c) 2022 Mirosław Banasik & Andrzej Soboń.



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.