

Natalia OLSZANECKA 

Nicolaus Copernicus University, Faculty of Political Science and Security Studies, Toruń, Poland

## Future War: The Russian Perspective

### Wojna przyszłości: perspektywa rosyjska

#### • Abstract •

In a multipolar world, military security issues still occupy a key place in the public debate. Military technology is one of the most developing sectors in the world. There is no doubt that the United States and the People's Republic of China have dominated this sector in recent years. The Russian defense industry is associated with outdated equipment, technology and corruption. Nevertheless, recent conflicts show that the Russian Federation has mastered the elements of information war. "New war" theory was advanced by Mary Kaldor to characterize warfare in the post-Cold War era. According to newest research, nowadays military conflicts employ some elements of both conventional and cybernetic combat, while military operations are supported by domestic and international propaganda. The main goal of this article is to determine what type of conflict is contemporary Russia preparing for and in what ways.

**Keywords:** Russian Federation; military technology; conflict; future war; security; "new war"

#### • Abstrakt •

W wielobiegunowym świecie kwestie bezpieczeństwa militarnego w dalszym ciągu zajmują kluczowe miejsce w debacie publicznej. Technologia wojskowa to jeden z najbardziej rozwijających się obszarów gospodarki na świecie. Nie ulega wątpliwości, że w ostatnich latach w tym sektorze dominowały Stany Zjednoczone i Chińska Republika Ludowa. Rosyjski przemysł zbrojeniowy kojarzony jest na ogół z przestarzałym sprzętem, technologią oraz wszechobecną korupcją. Niemniej ostatnie konflikty pokazują, że Federacja Rosyjska dobrze opanowała elementy wojny informacyjnej. Mary Kaldor jest autorką teorii „nowej wojny”, dzięki której charakteryzuje działania wojenne po zimnej wojnie. Według najnowszych badań współczesne konflikty zbrojne wykorzystują elementy zarówno walki konwencjonalnej, jak i cybernetycznej, a działania zbrojne są wspierane przez propagandę krajową i międzynarodową. Głównym celem artykułu jest określenie, do jakiego typu konfliktu przygotowuje się współczesna Rosja.

**Słowa kluczowe:** Federacja Rosyjska; technologia wojskowa; konflikt; wojna przyszłości; bezpieczeństwo; „nowa wojna”

## Introduction

In the 20<sup>th</sup> century, the term ‘war’ meant, above all, a military conflict between at least two entities, fought mainly on land, at sea and/or in the air, and the images of potential future wars were extrapolations of such warfare, utilizing upgraded versions of current technologies. However, the turn of the 21<sup>st</sup> century made those concepts obsolete. Technological development triggered the emergence of new ways of conducting military actions. War nowadays employs some elements of both conventional and cybernetic combat, while military operations are supported by domestic and international propaganda. As far as war in the future is concerned, it is widely known that the US Department of Defense conducts research in the area of synthetic biology, quantum information science, cognitive neuroscience, and behavioral modelling. The US invests in technologies operating in electromagnetic spectrum, hypersonic vehicles, laser weapons and autonomous systems. In the case of the Russian Federation, it is more difficult to find reliable information about the state’s current military research; however, recent conflicts (in Ukraine and in Syria) show that the Russian Federation has mastered the elements of information war. This article attempts to solve the research problem formulated in the question: what type of war is contemporary Russia preparing for and in what ways? The study is based on content analysis and adopts primary and secondary research techniques, i.e., desk research. The sources are categorized according to the following classification: the analysis covers content within the research field defined by territory (the Russian Federation), subject (Russian military forces and secret service), substantive scope (reform of Russian military forces), and time (2012–2018), while the choice of sources for the analysis was dictated by relevance and reliability. The main research hypothesis is that the activities of the Russian Federation currently focus on two aspects – preparing for the “new war” and maintaining the capability of fighting in conventional or nuclear wars.

The focus in the first part of the article is on the analysis of strategic planning documents and structural changes in Russian military forces and its secret service. The second part investigates non-military and military aspects of a future war.

## Future war, or “new war”

In its traditional meaning ‘war’ is understood as an act of violence aimed at forcing an opponent to obey our will (Clausewitz, 2007, p. 13). War is financed by a state, and its parties are also states. The aim of warfare is to satisfy certain interests. Wars are fought with military forces. Historically, wars broke out for geopolitical and ideological reasons, and their ultimate goal was to defeat an enemy in a battlefield, conquer its territory and thus strengthen the power of the victorious state. However, in the mid-1990s, many analysts began to claim that this definition did not encompass the contemporary warfare, which led to the emergence of a theory of “new wars”. “New wars” are civil or domestic conflicts and break out in authoritarian states. They are based mainly on identity policy – strengthened by new technologies – and are stimulated by personal or group interests (Malantowicz, 2013, p. 52). Despite the discrepancies as to some details, supporters of this theory agree that contemporary war requires new conceptualization (Mello, 2010).

Analyzing “new wars”, it is necessary to notice their three prominent features, first of which is the weakening of a state’s monopoly to use force. In result of this process, the traditional distinction between those who fight (combatants) and civilians is becoming increasingly blurred, and attacks are aimed at civilians and infrastructure (Münkler, 2006, p. 135). The second feature are economic issues: it has been noticed that “new wars” are driven by economic aspirations rather than political and ideological ones. While studying the causes of conflicts, Paul Collier and Anke Hoeffler developed a model in which they measured greed and dissatisfaction. They discovered that with regard to the causes of conflicts, the greed factor was stronger than dissatisfaction (Collier & Hoeffler, 2004, p. 588). The third feature is conflict asymmetry, which concerns actors, military capabilities, methods of waging war and pursuing military policy. According to Mary Kaldor, combat methods in “new wars” are similar to the strategy of guerrilla war, yet with one basic difference: guerrilla war is aimed at winning “hearts and minds”, while the aim of new warfare is to fuel “fear and hate” (Kaldor, 1999, p. 8).

In 2005, General James Mattis and Lieutenant Colonel Frank Hoffman took a step further and coined the term “hybrid war”. One of its dimensions involved “psychological or information operations”. In process of time, the term started to mean warfare where in order to defeat an enemy, all available tools are employed, including terrorist, rebellious, criminal and conventional actions as well as information operations on a large scale (Freedman, 2019, p. 302). Analyzing Russia’s military operations in Ukraine since 2014, it must be said that it satisfies the criteria for a hybrid war and falls within the scope of the “new war” concept.

## Strategic planning documents

When discussing the prospect of future war, first of all it is necessary to focus on Russia's official strategic planning documents, the most important of which is the Military Doctrine of Russia, including views on preparation for armed protection of the state and its interests. On December 26, 2014, the RF President Vladimir Putin approved an amendment to the Military Doctrine of the Russian Federation. It does not mention Russia's enemies, merely stating that the world has become more dangerous due to "increasing global competition" between contradictory values. The Doctrine again acknowledges that nuclear weapon remains an important deterrent to nuclear and conventional military conflicts. What is currently recognized as military threats are deployments of foreign forces in the territories of states bordering Russia; creation and development of strategic missile defense systems, the undermining of global stability and the violation of the balance of forces in nuclear missile sphere; implementation of "global strike"; intention to place weapons in space; and the development of strategic, precise, non-nuclear weapon systems (Malendowski, 2017, p. 82). The greatest threats recognized by the document include the growing military capacity of NATO and the increasing proximity of its military infrastructure to Russia's borders, as well as indirect and asymmetric activities (*Voyennaya doktrina Rossiyskoy Federatsii*, 2014). For the first time the Military Doctrine contains a point about defending Russia's national interests in the Arctic<sup>1</sup> (which suggests the state's readiness for global competition for energy resources) and about requirements imposed on the administration with regard to a constant readiness for mobilization in the case of war.

Moreover, the document speaks about the necessity to counteract the use of new information warfare technologies against society. The new Doctrine emphasizes promotion of patriotism and preparation of young Russians for military service. The document refers also to hybrid war and thus to the necessity to anticipate subliminal aggression in the strategies of neighboring countries (Madej & Świeżak, 2015). An analysis of the new Military Doctrine shows that the authorities intend to base the state's military potential on conventional forces rather than nuclear deterrence.

In this study, particular attention should be paid also to the Doctrine of Information Security of the Russian Federation, approved on December 5, 2016.

---

<sup>1</sup> Russia has planned active actions, including military ones. They concern the construction of six military bases in the Arctic with a modern radar guidance system, the creation of a military command structure and the organization of permanent Arctic forces (the white army).

Seemingly, it is a very general document, but in-depth analysis makes it possible to discern the direction of cybersecurity development in Russia. First of all, information security is included under strategic national interests. Among the most serious threats are terrorist organizations; institutions and intelligence services of other states developing communication and information technologies which pose a threat to Russia's critical infrastructure (electricity, energy, transport management); organizations and institutions weakening the sovereignty of the state and its cultural values by disseminating non-objective and false information about Russia; the aspiration of certain states to dominate the information sphere; challenges related to financial crime; stealing of personal data via the Internet; inefficiency in domestic IT business; and the country's dependence on advanced technologies and the products based on them (*Doktrina informatsionnoy...*, 2016), thereby the need to create domestic equivalents of foreign technologies has been highlighted. The document also notes the increase in intelligence activity against Russia and expresses concern over the increase of offensive operations in cyberspace (Kuczyńska-Zonik, 2017, pp. 97–105).

The list of main threats involves also the use of information in military and political conflicts and in attacks on the state's infrastructure. As Aleksandra Kuczyńska-Zonik emphasizes, Russia itself has repeatedly shaped foreign, historical and military policy, resorting to propaganda directed at Russian society and the international recipients (Kuczyńska-Zonik, 2017).

When discussing strategic documents, what should also be mentioned is the so-called "Gerasimov doctrine". This term was coined after the speech on contemporary war that was given by the Chief of the General Staff of the Armed Forces of Russia, Valery Gerasimov, at the Academy of Military Sciences in February 2013. The main theses of his speech were published in the newspaper "Military-Industrial Courier". Prior to the speech, the main threat was attributed to "colorful revolutions" in post-Soviet countries, but Gerasimov saw the main danger in US policy, based on maintaining hegemony at all costs. In his opinion, what is needed is to gain strategic and geopolitical advantage by both military and non-military means. The non-military ones include diplomacy, espionage, economic pressure, swaying the sympathies of local people, forming alliances, breaking off relations, creating political opposition or changing the political leadership in a state which opposes Russia. As regards military measures, Gerasimov emphasized the importance of precise long-range weapons which would be the first means applied to destroy critical infrastructure of an attacked state. Importantly, the ratio of non-military to military means should be 4:1. According to Gerasimov, there is no need for cannons and tanks to defeat the enemy if there are far more effective ways to win.

Computer hacking, TV propaganda and deception can demoralize the opponent and weaken alliances (Malgin, 2018). His theory of modern war does not imply any direct attack on the enemy but rather the “hacking” of its society. Gerasimov said that the goal is to achieve an atmosphere of constant unrest and conflict in a hostile country, and hybrid action can be initiated by a “fifth column” or secret armed forces (Freedman, 2019, p. 303).

Gerasimov’s speech is considered an expression of contemporary Russian strategy, based on the ideas of total war and of politics being at the same level as war – both philosophically and technically. This approach assumes a guerrilla war waged on all fronts that uses a wide range of allies and tools – hackers, media, business, fake news – as well as conventional and asymmetric fighting methods. Thanks to the Internet and social networks, such operations have become possible (McKew, 2017).

## Military aspect of the future war

Although Gerasimov finds the military aspect of future armed conflicts less important than the non-military one, since 2008 the Armed Forces of the Russian Federation have been undergoing reform. According to the official data on the website of the Russian Ministry of Defense, modernization is progressing on schedule. In 2006, less than 15% of military equipment in Russia was modern (*Russia Sets Its Arms Priorities*, 2006); in 2019, modern armament accounted for 64% of the equipment of the Russian Armed Forces (it is assumed that by 2020 it will be 70–100%). Thus, with regard to the number of modern weapons Russia has already reached a level similar to NATO states.

In 2017, Russia’s military spending dropped by one fifth (to 66.3 billion dollars), the first reduction in almost two decades. This situation resulted from the poor economic condition of the state. In 2018, Russia spent 61.4 billion dollars (3.9% of GDP) on armaments, which is 3.5% less than a year before (*The Military Balance*, 2018).

Table 1. Percentage of Modern Armament in the Russian Armed Forces

| Type of arms | 2019 | 2020 goal |
|--------------|------|-----------|
| Submarines   | 67%  | 71%       |
| Warships     | 65%  | 71%       |
| Aircraft     | 67%  | 71%       |

Tab. 1 – cont.

| Type of arms           | 2019 | 2020 goal |
|------------------------|------|-----------|
| Helicopters            | 81%  | 85%       |
| Anti-ballistic systems | 100% | 100%      |
| Artillery              | 73%  | 79%       |
| Armoured vehicles      | 75%  | 82%       |
| Multipurpose vehicles  | 65%  | 72%       |

Source: Ministry of Defense of the Russian Federation (2013).

To summarize the reform of the armed forces (particularly the issue of rearm-ing), it should be noted that, as always, strategic nuclear forces have been a priority<sup>2</sup> and were modernized first. In other areas, modernization depended largely on the capabilities of the domestic defense industry. Russian military technology is primarily associated with heavy conventional armaments. The best modern weapons in Russia are the T-14 Armata tank, the Su-35 fighter, the Mi-28 attack helicopter as well as the P-800 Oniks anti-ship cruise missile and the Pantsir-S1 surface-to-air missile system. Many technologies have been successfully upgraded; however, the modernized ships are based on projects from the Soviet era. Other successfully delivered models include the Su-30, Su-34 and Su-35 fighters as well as hundreds of modernized T-72B3s and T-90 MBTs. This shows that the Russian defence industry still faces huge problems with the production of more sophisticated weapon systems (Radin et al., 2019, pp. 100, 221).

It is worth noting that orders for the navy have been suspended due to problems in the shipbuilding industry and the conflict with Ukraine. Also, two thousand T-14 Armata tanks ordered in 2015 were not produced. Currently, these plans have been cancelled<sup>3</sup> – only twenty copies of the experimental variant have been delivered (*W Minoborony...*, 2016). The order for the fourth-generation electric-powered submarines – the *Lada* class (Project 677) – was also delayed as the Russian shipbuilding industry was unable to develop a new propulsion system to the Navy's requirements. The second of the ordered ships (*Kronstadt*) was launched on September 20, 2019, after 13 years of work (Dura, 2018).

<sup>2</sup> In the 2018 State Armament Programme for 2018–2027 the priority will be given again to spending on nuclear forces, which indicates that Russia will focus primarily on maintaining its deterrence capabilities.

<sup>3</sup> The plan is to produce only 100 items.

Lately, Russia has also been developing weapons of new generation. One of the most famous projects in recent years was the production of the fifth-generation fighter (PAK-FA/T-50/Su-57), of which ten prototypes have been built so far. However, in 2018, Russian Deputy Minister of Defense Yuri Borisov announced during a television interview that the fifth-generation Su-57 fighter would not go into mass production due to high production costs, suspension of India's participation in the program, and problems with engine production (Behrendt, 2018).

When it comes to the so-called weapon of the future, Russia is currently working on several projects that would ensure a strategic advantage over its rivals. These projects include:

- a new generation of intercontinental ballistic missiles, "Sarmat":  
They are to be in service in 2019–2020. One rocket is able to carry 15 to 20 warheads, 750 kilotons each. In December 2017, it successfully completed a test launch at the Plesetsk Cosmodrome. This new missile is supposedly capable of reaching the US even by a trajectory over the South Pole, thus circumventing the warning and defence systems, which are concentrated in the north (Kristensen & Korda, 2019).
- the hypersonic glide vehicle "Avangard":  
A missile able to travel at Mach 20. Moreover, when approaching the target, the glider performs deep maneuvering, both horizontal and vertical, which makes it invulnerable to any air and missile defence systems. In December 2018, the missile completed a series of tests and is to enter combat duty until 2027 (Baraniec, 2018).
- the hypersonic air-launched ballistic missile "Kinzhal":  
This system has no equivalent in the world. The missiles can travel at up to six times the speed of sound and thus fly relatively low, being virtually undetectable by radar. On December 1, 2018, the system was included in the pilot program at the airports of the Southern Military District (Hrolenko, 2018).
- the 5P-42 Filin systems:  
These systems are supposed to cause hallucinations and blurred vision. They are based on special lasers that blind and confuse enemies due to their intense, varyingly modulated beams of light. The systems were installed on the previously mentioned 677 Lada submarines (*Novyj «Filin» Rosteha oslepil pravonarušitelej*, 2018).
- the unmanned helicopter-type aerial vehicle "Voron 777-1":  
Russia has encountered great difficulties in their efforts to make the battlefield digital by automation and robotization of weapons. The country used



to produce the unmanned Outpost vehicles based on an Israel Aerospace Industries patent. However, the contract was terminated by Israel after Russian aggression in Ukraine. In 2017, the “Iskatel” Design Office of the Moscow Aviation Institute presented a model of an unmanned helicopter-type aerial vehicle “Voron 777-1” with a 50 kg operation load. It was designed for electronic warfare and the use of firearms (*«Voron 777-1»...*, 2017).

The Ministry of Defense of the Russian Federation is planning to spend 306 billion dollars in the next decade on the purchase of military equipment, its modernization, repair, as well as research and development. The amount allocated to the new changeover program (covering the years 2018–2027) is similar to that of the GPV-202 program. However, due to high inflation, the new program is less ambitious than the previous one. The goals of the new program are to increase mobility and capacity, improve logistics as well as strengthen control and command, with the priority given to modernization of the strategic nuclear triad. The program is secret, but it is predicted that the navy will receive less funds and priority will be given to smallest units. On the other hand, ground forces may expect increased funding (Dyner, 2018).

## Non-military aspect of the future war

According to Gerasimov, the non-military aspect of future and present conflicts, besides diplomacy, focuses largely on “hacking” the enemy’s society. First of all, elements of information and psychological warfare are applied here<sup>4</sup> (Darczewska, 2014) – shaping public opinion by fake information, propaganda, and cyberattacks. In Russia, the “information war” (Giles, 2016, p. 12) is understood, unlike in the West, as influencing mass consciousness in the interstate competition of civilization systems within information space, achieved by adopting special methods of controlling information resources, and used as “information weapons”. This means that an information war is not only simultaneous with military operations. It is not even limited to the initial phase of the conflict when information about the rival is being compiled. Instead, it is a continuous activity, carried out regardless of the relations with a given opponent, and continuing in peacetime (Giles, 2016, p. 4).

---

<sup>4</sup> Russian theory of information wars has a long tradition in the country. It derives directly from the theory of spec propaganda, which as a separate subject began to be taught in 1942 at the Military Institute of Foreign Languages.

The information war aims at setting Russia's opponents (e.g., NATO countries) against each other, creating chaos and controlling other states' internal political processes. An example of this type of action is the conflict in Ukraine – during the protests in 2014, the Kremlin supported the pro-Russian extremists and the Ukrainian ultra-nationalists. Russia fuelled the conflict, which was later used as an excuse for the annexation of Crimea. The next target was the United States. There is a high probability that American voting machines were hacked, and it is certain that prior to the elections, fake news and disinformation was deliberately and intentionally disseminated on social networks, and digitally stolen material was sometimes used to manipulate American society (Polyakova, 2019).

There are several ways in which Russia wages an information war:

- reflexive control:

These are the methods by which information tailored for a partner or an opponent can reach them. This information is to impel them to make a voluntary decision in line with the antagonist's assumptions (Thomas, 2004). These methods include supporting the internal opposition of states, spreading dissatisfaction among the population, shaping national and international public opinion, implementing secret operations through cyberattacks. One of the tools that Russia uses is the media, e.g., Russia Today (RT), a multilingual, government-funded information site, where the Russian perspective on global events is presented. An example of reflexive control was the building of a narrative about the Malaysian airlines air crash (Emerson, 2015).

- influencing decision-makers:

Russia is trying to influence foreign decision-makers by disinformation, taking advantage of the fact that Western politicians receive the same information and use the same channels as their voters. Even if disinformation is not effectively included in the policy-making chain and spreads only on social media, it is still Russia's success as public opinion circle emerges where Russian narratives are presented as facts (Giles, 2016, p. 22).

- weakening and destabilization:

The information war strategy includes extensive, long-term weakening of opponents, based on information control, e.g., censorship of school textbooks, thanks to which the Russians construct their version not only of current events but also of history. Regaining control over the national information space is an ongoing process that started soon after President Putin took power in 2000. In recent years, this process has accelerated and spread to the Internet. Russians are increasingly isolated from alternative sources of information (Giles, 2016, p. 24).

- cybernetic and information operations:  
Russia uses various types of cyberweapons, including DDoS attacks to gain control over the Internet's infrastructure. In the case of the annexation of Crimea, the Internet traffic exchange point in Simferopol was physically seized and connections with the continent were disrupted, contributing to Russian dominance over the information zone on the peninsula (Harris, 2014).
- troll farms and botnet:  
One of the most significant aspects of the Russian information campaign in Western public awareness is the ubiquitous activity of trolls (people-operated accounts on Facebook, Twitter, Google online, etc.) and bots (operated by automated processes) that interact directly with readers in various media. Research on Russian trolls developed at the beginning of 2014. An example of this type of activity is the IRA, i.e., Internet Research Agency, which co-operates with Russian intelligence (Ramesh, 2019). Russia used trolls, for example, in Syria – analysts found over 3,000 posts about Syria on Instagram and Facebook. The trolls supported Syrian President Bashar Al-Assad, emphasized that Russia was defending its legitimate Syrian president and was doing everything to prevent ISIS from taking over the country. The narrative was tailored to the recipients (Mierzyńska, 2018).

## Conclusions

As the research shows, Russia sees future conflicts as a departure from extensive direct fighting, which is undoubtedly becoming a part of the category of “new wars” – hybrid wars. At present, the Russians, according to the Gerasimov doctrine, are wielding an extensive and effective information and psychological war. Moreover, their future victory is to be ensured by attacks on civilian administrative and economic facilities in the first phase of the conflict. To meet this goal, first of all, hypersonic and long-range weapons are perfected. The Russians are testing new weapons as well as support and command systems. Strategic nuclear forces that implement the deterrence doctrine remain a priority. However, there are no major investments in exoskeletons and other equipment that would improve the soldier's combat capabilities on the battlefield, nor are the Russians developing unmanned programs as much as their greatest competitors.

## References:

- Baraniec, V. (2018, December 28). «Komsomolka» uznala glavnye sekrety raketnogo kompleksa «Avangard». Retrieved from: <https://www.kp.ru/daily/26926.2/3974284/>.
- Behrendt, P. (2018, July 13). *Co dalej z Su-57?* Retrieved from: <http://www.konflikty.pl/aktualnosci/wiadomosci/co-dalej-z-su-57/>.
- Clausewitz, C. (2007). *On War*. Oxford: Oxford University Press.
- Collier, P., & Hoeffler, A. (2004). Greed and Grievance in Civil War. *Oxford Economic Papers*, 56(4), 563–595. DOI: 10.1093/oep/gpf064.
- Darczewska, J. (2014). *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*. Warszawa: Ośrodek Studiów Wschodnich im. Marka Karpia. Retrieved from: [https://www.osw.waw.pl/sites/default/files/anatomia\\_rosyjskiej\\_wojny\\_informacyjnej.pdf](https://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf).
- Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii Utverzhdena Ukazom Prezidenta Rossiyskoy Federatsii ot 5 dekabrya 2016 g. №646* (2016). Retrieved from: <http://base.garant.ru/71556224/>.
- Dura, M. (2018, September 23). *Rosja: Wodowanie trzynastoletniego okrętu podwodnego typu „Łada”*. Retrieved from: <https://www.defence24.pl/rosja-wodowanie-trzynastoletniego-okretu-podwodnego-typu-lada>.
- Dyner, A.M. (2018, February 8). *Nowy rosyjski program zbrojeniowy na lata 2018–2027 – znaczenie dla Polski i NATO*. Retrieved from: <http://www.polska-zbrojna.pl/home/articleshow/24718?t=Nowy-rosyjski-program-zbrojeniowy-na-lata-2018-2027-znaczenie-dla-Polski-i-NATO>.
- Emerson, J.B. (2015, June 29). *Exposing Russian Disinformation*. Retrieved from: <http://www.atlanticcouncil.org/blogs/new-atlanticist/exposing-russian-disinformation>.
- Freedman, L. (2019). *Przyszła wojna*. Bellona: Warszawa.
- Giles, K. (2016). *Handbook of Russian Information Warfare*. Fellowship Monograph 9. Rome: NATO Defense College.
- Harris, S. (2014, March 3). *Hack Attack: Russia's First Targets in Ukraine: Its Cell Phones and Internet Lines*. Retrieved from: <http://foreignpolicy.com/2014/03/03/hack-attack/>.
- Hrolenko, A. (2018, March 10). *Giperzvukovoe orużie Rossii i kosmičeskoe vozbużdenie Pentagona*. Retrieved from: <https://lt.sputniknews.ru/20180310/oruzhie-russia-pentagon-5346549.html>.
- Kaldor, M. (1999). *New and Old Wars: Organized Violence in a Global Era*. Stanford, CA: Stanford University Press.
- Kristensen, H.M., & Korda, M. (2019). Russian Nuclear Forces. *Bulletin of the Atomic Scientists*, 75(2), 73–84. DOI: 10.1080/00963402.2019.1580891.
- Kuczyńska-Zonik, A. (2017). Strategia bezpieczeństwa informacyjnego Federacji Rosyjskiej. In: J. Trubalska, & Ł. Wojciechowski (Eds.). *Bezpieczeństwo państwa w cyberprzestrzeni* (pp. 97–105). Lublin: WSEI.
- Madej, A., & Świeżak, P. (2015). Informacja na temat „Doktryny wojennej Federacji Rosyjskiej”. *Bezpieczeństwo Narodowe, III*, 177–178.
- Malantowicz, A. (2013). Civil War in Syria and the ‘New Wars’ Debate. *Amsterdam Law Forum*, 5(3), 52–60. DOI: 10.37974/ALF.260.

- Malendowski, W. (2017). Doktryna wojenna Federacji Rosyjskiej w XX i XXI wieku. Cele – zadania – kierunki działania. *Przegląd Strategiczny*, 10, 55–94. DOI: 10.14746/ps.2017.1.4.
- Malgin, A. (2018, March 23). *Doktrina Gerasimova: seyat' khaos i razdor*. Retrieved from: <https://avmalgin.livejournal.com/7598076.html?page=2>.
- McKew, M.K. (2017, September 7). *Doktrina Gerasimova*. Retrieved from: <https://inosmi.ru/politic/20170907/240217819.html>.
- Mello, P.A. (2010). In Search of New Wars: The Debate about a Transformation of War. *European Journal of International Relations*, 16(2), 297–309. DOI: 10.1177/1354066109350053.
- Mierzyńska, A. (2018, December 24). *Rosjanie się nie cofnęli – cyberwojna z USA trwa! Zagrożenie dla Polski*. Retrieved from: <https://oko.press/rosjanie-sie-nie-cofneli-cyberwojna-z-usa-trwa-zagrozenie-dla-polski/>.
- Ministry of Defense of the Russian Federation (2013). *Plan deyatel'nosti na 2013–2020 gg* [Action Plan for 2013–2020]. Retrieved from: [https://mil.ru/mod\\_activity\\_plan/constr/lvl/plan.htm](https://mil.ru/mod_activity_plan/constr/lvl/plan.htm).
- Münkler, H. (2006). Was ist neu an den neuen Kriegen? Eine Erwiderung auf die Kritiker. In: A. Geis (Ed.). *Den Krieg überdenken. Kriegsbegriffe und Kriegstheorien in der Kontroverse* (pp. 133–150). Baden-Baden: Nomos.
- Novyy «Filin» Rostekha oslepit pravonarushitelej (2018, December 20). Retrieved from: <https://rostec.ru/news/novyy-filin-rostekha-oslepit-pravonarushiteley/>.
- Polyakova, A. (2019, June 18). *Five Years after the Revolution of Dignity: Ukraine's Progress and Russia's Malign Activities*. Retrieved from: <https://www.brookings.edu/testimonies/five-years-after-the-revolution-of-dignity-ukraines-progress-russias-malign-activities/>.
- Radin, A., Davis, L.E., Geist, E., Han, E., Massicot, D., Povlock, M., Reach, C., Boston, S., Charap, S., Mackenzie, M., et al. (2019). *The Future of the Russian Military: Russia's Ground Combat Capabilities and Implications for U.S.-Russia Competition*. Santa Monica: RAND Corporation.
- Ramesh, G. (2019, July 10). *Russia Continues Information Warfare*. Retrieved from: <https://www.afcea.org/content/russia-continues-information-warfare>.
- Russia Sets Its Arms Priorities* (2006, January 18). Retrieved from: <http://www.rferl.org/content/article/1143555.html>.
- The Military Balance* (2018). London: International Institute for Strategic Studies.
- Thomas, T. (2004). Russia's Reflexive Control Theory and the Military. *Journal of Slavic Military Studies*, 17(2), 237–256. DOI: 10.1080/13518040490450529.
- «Voron 777-1» smozhet ne tol'ko letat', no i strelyat' (2017, June 16). Retrieved from: <https://tvzvezda.ru/news/opk/content/201706161625-5ddc.htm>.
- Voyennaya doktrina Rossiyskoy Federatsii* (2014). Retrieved from: <http://news.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf>.
- W Minoborony nazvali čislo zakuplennyh tankov «Armata»* (2016, April 19). Retrieved from: [https://lenta.ru/news/2016/04/19/armata\\_100/](https://lenta.ru/news/2016/04/19/armata_100/).