BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY
https://buletinul.unap.ro/index.php/en/

Considerations on the role of information (-psychological) operations in Russian military thinking

Eveline MĂRĂȘOIU, Ph.D. Candidate*

*National University of Political Studies and Public Administration, Bucharest, Romania
e-mail: eveline.marasoiu@gmail.com

Abstract

Russian military thinking and strategic documents attribute information warfare (and its associated concepts) to external authors only. This creates a vacuum in terms of how Russia actually implements itself information-psychological operations and how this fits into the broader Russian military thinking. This article looks at how information (-psychological) operations (IOs) are applied pragmatically through the prism of specific and well-established Russian concepts, such as Reflexive Control, Asymmetry and Initial Period of War, with a specific focus on the current conflict in Ukraine. It also looks at specific capabilities and formation in the field of IOs, as pertaining to the military field.

Keywords:
psychological operations; Russian thinking; reflexive control; Asymmetry; Initial Period of War.

When talking about Information Warfare and its associated concepts, Russian (RU) military theory and strategic documents only recognize this phenomenon as an external one – activities undertaken exclusively by the adversaries – against RU or against third parties (Pallin 2019). This leaves a gap in understanding how information activities are integrated into Russian military thinking and practice. This article aims, therefore, to highlight the role of information (-psychological) operations in Russian military thinking, by addressing, in particular, its relevance in the context of specific Russian military concepts, such as *Reflexive Control (RC)*, *Asymmetry* and *Initial Period of War* (IPW). To better understand this, the article offers some brief illustrations, especially in reference to the current (2022-*ongoing*) war in Ukraine. Furthermore, this article will also present certain elements related to formation and capabilities in this area.

The specification *information (-psychological) operations* derives from a bi-dimensional understanding of *information* in Russian strategic culture, which encompasses an information-technical dimension (cyber, EM, etc.) and an information-psychological dimension (referring to the communicated part of information, which has the potential of triggering psycho-social or cognitive effects). This form of conceptualization can be observed, *inter alia*, in the *information warfare* definition, provided in the 2011 Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space: *"a confrontation between two or more States in the information space with the purpose of inflicting damage to information systems, processes and resources, as well as to critically important structures and other structures;* ***undermining the political, economic and social systems; carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government, as well as forcing a state to make decisions in their interests.****"* (Ministry of Defence of the Russian Federation 2011). To be more specific, *"information-psychological warfare affects the unconscious, irrational states of people, their emotions, feelings, instincts, prejudices, preconceptions, and the mythological constructs of the population of a potential enemy… This is achieved through the mass introduction to people's awareness of a multitude of false stereotypes of perception and thought, and of perverted notions about views dominating their environment as well as about events occurring in the world"* (Sitnova and Polyakov 2018, 8).

For the purposes of this article, the author shall use the following working definition of information (-psychological) operations (IOs), which excludes the information-technical dimension: *Information Operations (IOs) are integrated, non-kinetic actions manipulating the Information Environment, coordinated by a state (or the military apparatus of a state), targeting either foreign governments or segments of foreign population, aimed at (a) influencing or paralyzing the decision-making process (either directly or through shaping the domestic public opinion) of another international actor, or (b) inflicting damage to that actor, with the strategic aim of consolidating the relative power of the state conducting IOs.*

It is worth noting that Russian military theory distinguishes between *standard* and *strategic information war*. The former refers to the use of deception within a military operation (i.e., the use of camouflage), while the latter is more widely associated with information-psychological operations. Accordingly, the attributes of IOs (strategic information warfare) are (1) asymmetry, (2) attacks upon multiple layers of society, and (3) attacks upon the same target by multiple attackers, aiming at different areas of cognition (Pynnöniemi 2019).

The following sections will (1) analyse the role of IOs within the framework of key concepts of Russian military thinking and science – RC, asymmetry and IPW, and will (2) address certain characteristics of formation and capabilities on IOs in the Russian military-security complex.

Information Operations as part of Reflexive Control (RC), Asymmetry, and Initial Period of War (IPW)

Reflexive Control plays a key role in Russian military art and thinking and it is applied in a wide spectrum of areas. Russian military science provides several definition of this concept, the most recent dating from 2017: *"The method (technique) of reflexive control of an enemy is the devices and techniques for implementing measures and actions that incite the enemy to act in a corresponding way that is advantageous for our side… Reflexive control can make it possible to change the enemy's goals and his methods of operation in favour of one's own forces, i.e., to contribute to the creation of favourable conditions to accomplish the assigned mission"* (Chausov 2017, 52). While describing the reflexive control techniques (intended to produce information-psychological effects), Chausov includes the dissemination of false information, with the aim of inducing the adversary to generate new objectives and operating methods (Chausov 2017, 53).

Thomas, who has studied in depth Russian military thinking and RC, offers an aggregated definition of the latter concept based on RU military body of knowledge: *"The term is defined in general as providing a stimulus (information, an action, etc.), to make an opponent to do something for himself (organize in a specific way, develop certain weaponry, manoeuvre, etc.) that he is doing for the initiator of the action. To utilize the concept, the proponent must know how an opponent things and processes information, and what his prejudices, likes, and dislikes are. Targeting can be as detailed as a psychological profile of specific officers in command positions"* (Thomas 2019, 4.1). The same author further explains how, while not explicitly stated, the RC concept is deeply embedded in the definition of information warfare provided by the RU Ministry of Defence in the 2011 Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space (Ministry of Defence of the Russian Federation 2011, 5) – *"forcing the state to make decisions in the interests of the confronting party."*

The main elements of RC include: distraction; information overload; paralysis; exhaustion; deception; division; pacification; deterrence; provocation; suggestion; pressure (Thomas 2004).

Information Operations are an essential feature of Reflexive Control, complementing intelligence, cyber measures, electronic warfare and electromagnetic actions. To better understand the application of RC, this sub-section shall offer some concrete examples, both from a theoretical perspective and from a pragmatic point of view, in so far as they involve the use of IOs.

- *Distraction:* In the context of the current (2022-ongoing) war against Ukraine, Russia attempted to instil the perception of a real threat to the flank of the targeted country – from Belarus, with the aim of forcing Ukraine to change its plans (Intelligence Online 2023).
- *Overload of information:* The 2008 invasion of Georgia offers a good example of how RU inflated the information environment with various narratives about the current situation on the ground, including through blaming the Georgian authorities for their aggressive actions (Fraser 2022).
- *Paralysis:* The threats issued by Russia on cutting off energy supplies to Europe in 2022, after invading (again) Ukraine (Lawson 2022) were meant to paralyse the West from offering additional military support to the attacked country by creating the perception of a threat to a vital European interest / weak spot.
- *Exhaustion*: As the war is still ongoing, it is hard to access or assess public information concerning the potential attempts of RU to exhaust UA armed forces by forcing them into useless operations. However, one potential illustrative scenario has been identified by the Institute for the Study of War (ISW): *"Russian President Vladimir Putin may be setting conditions for further Russian cross-border raids into northeastern areas of Ukraine, likely in an effort to further domestic information operations and pin Ukrainian forces against northern border areas. […] The threat of cross-border raids from Belgorod, Bryansk, and Kursk oblasts into northern and northeastern Ukraine is likely an attempt to force Ukraine to deploy limited elements to these areas to protect against such attacks, thus dispersing Ukrainian troops to an extent in advance of a likely Russian offensive operation in the coming months. ISW has previously reported similar Russian distraction and dispersion operations in Zaporizhia Oblast"* (Stepanenko, et al. 2023).
- *Deception:* In the early stages of the latest Russian-Ukrainian war, Moscow attempted to deceive Kyiv into keeping its armed forces far away from the capital, with the strategic aim of rapidly conquering the key-city (Zabrodskyi, et al. 2022).
- *Division:* Russia's decision to further cultivate energy ties with Hungary, by speeding up the construction of two new nuclear reactors in the middle of its full-blown war against Ukraine (Davies 2022) is one of the leviers employed by the Kremlin to sow division among the Euro-Atlantic partners – especially given its interest to avoid further adoption of sanctions at the EU level.

➢ *Pacification:* The period leading up to the February 2022 invasion of Ukraine is a clear example of how RU aimed to use this element to persuade Ukraine and the West that its large military build-up in the proximity of UA's border were there only for training purposes (Reuters 2021). At the same time, Moscow was engaging in *overload*, claiming that it is Ukraine that amasses troops at the border and suggested that Kyiv intends to conduct a military offensive operation against the separatist regions (Reuters 2021).
➢ *Deterrence:* Kremlin's threats to potentially using nuclear arms (tactical or strategic) against Ukraine (Crawford 2022), including by noting that the recently acquired/occupied (Ukrainian) territories fall under the protection of the nuclear umbrella, pursued a double-deterrent objective: on the one hand, it aimed at displaying its military superiority towards Ukrainian armed forces, military leaders and broader population, thus aiming at discouraging and deterring further military operations by Ukraine; on the other hand, it targeted the West – attempting to scaremonger Euro-Atlantic political leaders and population, in order to limit the politico-military support granted to Ukraine.
➢ *Provocation:* One might argue that certain actions conducted by Russia in the Initial Period of War, such as the recognition of breakaway regions in Donbass on the 21st of February 2022, alongside the deployment of "peacekeeping troops" in these areas (DW 2022) had as one of its aims to provoke an overreaction from Ukraine. In case Kyiv had decided to send its troops to the breakaway regions, it is likely that it would have lost some of the support of its Western partners, thus leading to a disadvantageous situation.
➢ *Suggestion*: The Kremlin has been engaged in a coordinated defamation campaign against Ukraine and its leadership, meant to discredit the country's international reputation, as well as decrease morale. Examples include false claims about alleged poisoning by UA of RU soldiers (Reuters 2022) or accusing UA for the *"destruction of the population of Donbass"* (Zakharova 2022) – the latter constituting also a basis for an alleged legal justification for RU's invasion. RU also engages in information activities aimed at *humanizing the assailant*, with the purpose of obtaining support and sympathy from the broader international community (especially the Global South) (Benabid 2022).
➢ *Pressure:* RU also attempted to discredit the President of Ukraine, Volodymir Zelenski, and the military leadership in the eyes of the population, in attempts to undermine unity and support for the continuation of defence of the homeland. By way of illustration, false narratives were spread about the President allegedly fleeing the country, commanders abandoning troops or widespread capitulation of troops (Bergengruen 2022).

Asymmetry is another core element in Russian military thinking – embraced not only at the level of the military establishment (MoD), but also the Kremlin. Given that Russia rejects the idea that it conducts hybrid warfare (reserving the use of

this term only for actions conducted by other parties – the West primarily), the asymmetric concept is better suited to understand Russian military views. Most recently, the 2021 NSS explicitly proclaims (in Art. 99) the legitimacy of both symmetric and asymmetric measures to respond to and prevent unfriendly actions from other states (President of the Russian Federation 2021).

The basic idea behind the concept of asymmetry is that a weaker power (from an economic and/or military standpoint) shall exploit vulnerabilities in the opponent and employ asymmetric and cost-efficient tools and strategies (Thomas 2019). Nonmilitary means, including information operations and reflexive control, represent an important tool in asymmetry. By way of illustration, IOs (and RC) can be used to achieve *surprise*, to *disorganize* the opponent (i.e., disorganizing the military control and command, the state administration, achieving psychological effects over the opposing forces and population), and during *indirect operations* – which can often be conducted through nonmilitary organizations (forms) (Thomas 2019).

Even in the context of the current war waged by Russia against Ukraine, Russia still considers itself in a broader confrontation – with the West (led, in Moscow's view, by the U.S.). In this sense, RU can be perceived as the weaker party. RU has used IOs in an attempt to induce surprise in the broader Western world by denying firmly any intentions to invade Ukraine and engaging instead in a *maskirova* – under the false pretence of negotiating new security arrangements with the U.S. and NATO prior to the invasion (Roth 2021). Moreover, the narratives about potential escalation – either through the use of nuclear arsenal (explained above) or through hinting at the possibility of extending the geographical area of operation to NATO Allies in the event of delivery of certain military equipment to Ukraine (Al Jazeera 2023) – are meant to disorganize the West by instilling fear in the Euro-Atlantic societies and, thus, diminishing the support at the level of population for maintaining the course on helping Ukraine.

The **Initial Period of War** also plays an essential role in Russian military science and art. IPW covers the situation when *"warring states conduct operations before the start of war to achieve objectives or to create favorable conditions for committing their main forces. Outer space, information warfare, and new weapon capabilities all help inform the shape needed for the IPW. These weapons enable sides before the start of operations to conceal the status and intent of their armed forces and the nature of any planned attacks"* (Thomas 2019, 8.5). It is noteworthy that *"nearly every Russian and Soviet deployment over the past half century, with the notable exception of this year's [2022] invasion of Ukraine, opened with soldiers appearing first in civilian clothing or unmarked uniforms"* (Kramer 2022) – a type of deception that aims to foster advantages in the combat theatre during IPW.

Some analysts argue that, in the context of the current war against Ukraine, RU either deviated from its doctrine concerning IPW (Boulegue 2022) or simply failed

(Massicot 2023). In terms of information-psychological operations, as described above, RU attempted to hide its invasion intentions, discredit the Ukrainian political leadership and provoke Kyiv to make strategic mistakes. However, coordinated and consistent declassified intelligence from Allies, especially from the U.S. and the UK, revealed RU's true intentions and countered (sometimes, pre-emptively) operations in the information environment (both during and after the IPW) (Dilanian, et al. 2022).

Other analysts argue that the use of the nuclear scaremongering (which pre-dated the February 24th, 2022 invasion) had a deterrent effect on Western support actions in Ukraine's benefit: *"Pervasive anxiety about Russian nuclear use has inhibited Western relief efforts, e.g., the campaign for a no-fly zone or for sending Ukraine aircraft. Western restraint has encouraged repeated and unrestrained Russian threats of nuclear use that are taken as inherently credible ones, even as Western deterrence is not seen as credible"* (Blank 2022).

Formation and capabilities

One of the most notable official statements in this regard belongs to the Russian Minister of Defence Sergei Shoigu, who, in February 2017, claimed that RU developed an information war force which, judging from the statement, puts an emphasis on the information-psychological component. *"The Information operations forces have been established, that are expected to be a far more effective tool than all we used before for counter-propaganda purposes. […] Propaganda should be smart, competent and effective,"* the Minister declared (TASS 2017).
Even prior to that point, Russian military scientists (Kazakov and Kiriushin 2015, 39) were affirming the need for commanders to have a dedicated group of qualified personnel in the information-psychological area, who can ensure the integration and execution of IOs as part of the RC tasks.

Russian analyst Alexander Perendzhiyev observed that *"according to information on the Defense Ministry official website, there are several subunits in the department's structure for now whose zone of responsibility can include information operations. Above all this is the Main (Intelligence) Directorate, the Main Directorate for the Development of Information and Telecommunications Technologies […], as well as the Press Service and Information Directorate […]. The General Staff Eighth Directorate's 5th Scientific Company located in Krasnodar probably also plays a certain part"* (Latsinskaya, Braterskiy and Kalinin 2017).

A presidential decree in 2018 established a new structure within the MoD – the Main Military-Political Directorate of the Armed Forces (GVPU) – headed by a Deputy Minister. According to the laws regulating the work and organization of the MoD, the tasks of GVPU related to the organization of the military-political work of the MoD, promote the activities of the Russian Armed Forces (RAF), strengthen the

legitimacy, prestige and authority of the MoD and the military service, and maintain and consolidate the patriotic tradition (President of the Russian Federation 2018). More specifically, GVPU is directly responsible, *inter alia*, for:

> *- "the organization of information and propaganda work and state-patriotic education of the personnel of the Armed Forces of the Russian Federation;*
> *- organization of military-special, psychological and cultural-leisure work in the Armed Forces of the Russian Federation;*
> *- creation of conditions for the exercise by the servicemen of the Armed Forces of the Russian Federation of the constitutional right to freedom of religion, taking into account the characteristics of military surveillance" (GlobalSecurity.org 2018).*

The structure and functions of the new GVPU are similar to its Soviet predecessor, while ideology is based on the history, culture and values of the Russian Federation (Thomas 2019, 8.23-8.24).

The high significance of GVPU can be observed in the context of RU's war against Ukraine (which started on February 24, 2022) and, in particular, through a look at its leadership. While Col. Gen. Andrey Kartapolov was responsible for setting up the new Directorate and led it for over three years (30 July 2018 – 5 October 2021), his successor, Col. Gen. Gennady Zhidko was able to remain in this position for less than a year (12 November 2021 – 28 July 2022). The official reason for the latter's dismissal was the lack of preparedness of the RAF to execute combat missions in Ukraine (Luzin 2023). The new Deputy Minister in charge of the GVPU (as of the 28 July 2022) is Col. Gen. Viktor Goremykin, believed to have been a counter-intelligence officer who subordinated to the FSB (ibid.).
The Russian General Staff Academy offers a training module on information conflict (Thomas 2019).

In RU military thinking, full government control over media is critical to achieve information superiority over the enemy. Chekinov and Bogdanov evoked, in this context, the potential of the media realm for stirring up chaos, confusion and demoralization at the level of the targeted public (Chekinov and Bogdanov 2012, 25-27). This trend was further amplified within the context of the Ukraine war: *"Russia has tried to restrain the access of Russian people to messages produced by Western actors by manipulating the content available on its TV channels, banning access to Western social media platforms, and even passing a bill that motivated the withdrawal of Western journalists from the country. Furthermore, Vladimir Putin 'warned' Russian citizens to not trust the information reported by American and European 'politicians, political scientists, and journalists' because what they write and say allegedly is an 'empire of lies'"* (Buarque 2022).

A 2016 study of the U.S. Army emphasized that RU *"uses a style of mission command with their IO campaigns,"* while the use of technological advances, especially electronic warfare allows the Kremlin to target individuals directly and specifically

(for instance, by sending personalized text messages to UA soldiers, threatening their loved ones while using credible details), which *"can have a tremendously negative psychological impact on young soldiers that are out of direct contact with their loved ones"* (U.S. Army Asymmetric Warfare Group 2016).

This method, however, is part of the *whole-of-government* (or even *whole-of-society*) approach that Russia is applying to information operations, thus also relying on capabilities outside the purview of the military. *"The whole-of-government approach has important consequences for the nature of the Russian method. While the American military tends to focus on the capabilities of a foreign military, this approach underestimates Russia's information warfare capabilities as most of them are not organic to the Russian armed forces"* (Tashev, Purcell and McLaughlin 2019, 139-140).

Conclusion

As Russian strategic culture does not recognize information warfare/IOs as something internal, attributing these activities exclusively to external actors, this article aims to bridge this gap by exploring how IOs are actually embedded in well-established concepts of Russian military art and science. To gain a better understanding of the way these elements of thought are applied in practice, this research focuses on their concrete application, with a focus on the ongoing war in Ukraine. However, as hostilities are still unfolding, it is expected that more information will surface at later stages. It also remains to be seen if the elements presented above will remain the same or undergo significant modifications in Russian military thinking, given certain failures.

The research also examines concrete capabilities and formation processes related to information(-psychological) operations in Russia. A key element in this regard is the whole-of-government/whole-of-society approach, which, primarily due to full state control over the media, offers Russia a distinct advantage compared to Western/democratic countries. However, the opaqueness of public information available regarding Russian security and defense architecture makes it difficult to offer a comprehensive account of Russian capabilities and formation processes in this area. As additional information surfaces in the public sphere, further research in this area will offer value-added insights, better informing Euro-Atlantic decision-making processes.

References

Al Jazeera. 2023. *'A whole new level' of war if NATO arms Ukraine, Russia warns.* January 19. https://www.aljazeera.com/news/2023/1/19/a-whole-new-level-of-war-if-nato-arms-ukraine-russia-warns.

Benabid, Mohamed. 2022. "Communication Strategies and Media Influence in the Russia-Ukraine Conflict." *Policy Brief.* Policy Center for the New South. April. https://www.policycenter.ma/sites/default/files/2022-04/PB_25-22_Benabid%20EN.pdf.

Bergengruen, Vera. 2022. *How Putin Is Losing at His Own Disinformation Game in Ukraine.* February 25. https://time.com/6151578/russia-disinformation-ukraine-social-media/.

Blank, Stephen. 2022. *Information Series*, June 15. https://nipp.org/information_series/stephen-blank-russian-nuclear-strategy-in-the-ukraine-war-an-interim-report-no-525-june-15-2022/.

Boulegue, Mathie. 2022. *We must think Russian deterrence outside the box.* March 21. https://thehill.com/opinion/international/598982-we-must-think-russian-deterrence-outside-the-box/.

Buarque, Beatriz. 2022. *Russia has tried to restrain the access of Russian people to messages produced by Western actors by manipulating the content available on its TV channels, banning access to Western social media platforms, and even passing a bill that motivated the withdra.* March 9. https://sites.manchester.ac.uk/political-perspectives/2022/03/09/true-fake-news-or-conspiracy-theory-a-look-inside-the-ukrainian-information-war/.

Chausov, F. 2017. "Command and Control of Battle on the Basis of a Reflexive Analysis of the Situation." *Morskoi Sbornik (Navy Journal)* (17).

Chekinov, S. G., and S. A. Bogdanov. 2012. "The Initial Period of Wars and their Impact on a Country's Preparations for Future War." *Military Thought* 11.

Crawford, Stuart. 2022. *Nuclear Scaremongering.* August 24. https://ukdefencejournal.org.uk/nuclear-scaremongering/.

Davies, Alys. 2022. *Russia to build two nuclear reactors in Hungary.* August 27. https://www.bbc.com/news/world-europe-62695938.

Dilanian, Ken, Courtney Kube, Carol E. Lee, and Dan De Luce. 2022. *In a break with the past, U.S. is using intel to fight an info war with Russia, even when the intel isn't rock solid.* April 6. https://www.nbcnews.com/politics/national-security/us-using-declassified-intel-fight-info-war-russia-even-intel-isnt-rock-rcna23014.

DW. 2022. *Russia recognizes independence of Ukraine separatist regions.* February 21. https://www.dw.com/en/russia-recognizes-independence-of-ukraine-separatist-regions/a-60861963.

Fraser, Cameron. 2022. *How Russian disinformation tactics were utilised in the context of the 2008 5-day war.* November 3. https://idfi.ge/en/how_russian_disinformation_tactics_were_utilised_in_the_context_of_the_2008_5_day_war.

GlobalSecurity.org. 2018. *Main Military-Political Administration (GVPU).* https://www.globalsecurity.org/military/world/russia/mo-gvpu.htm.

Intelligence Online. 2023. *Russia ramps up strategic disinformation campaign north of Ukraine.* January 17. https://www.intelligenceonline.com/government-intelligence/2023/01/17/russia-ramps-up-strategic-disinformation-campaign-north-of-ukraine,109902674-art.

Kazakov, V.G., and A.N. Kiriushin. 2015. "All-Inclusive Command and Control of Combat Operations." *Journal of the Academy of Military Science* 4.

Kramer, Andrew E. 2022. *Phantom Retreats and Stolen Bones: The War of Deceit in Ukraine.* November 9. https://www.nytimes.com/2022/11/09/world/europe/ukraine-russia-war-weapons.html.

Latsinskaya, M., A. Braterskiy, and I. Kalinin. 2017. "Russia Sent Troops onto the Internet: Shamanov Explained Why Information Troops are Necessary." *Gazeta.ru.* February 22.

Lawson, Alex. 2022. *'Gas blackmail': how Putin's weaponised energy supplies are hurting Europe.* July 15. https://www.theguardian.com/world/2022/jul/15/gas-blackmail-how-putins-weaponised-energy-supplies-are-hurting-europe.

Luzin, Pavel. 2023. *The Political Considerations Behind Russia's Military Command Chaos.* January 26. https://jamestown.org/program/the-political-considerations-behind-russias-military-command-chaos/.

Massicot, Dara. 2023. "What Russia Got Wrong Can Moscow Learn From Its Failures in Ukraine?" *Foreign Affairs.* https://www.foreignaffairs.com/ukraine/what-russia-got-wrong-moscow-failures-in-ukraine-dara-massicot.

Ministry of Defence of the Russian Federation. 2011. "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space." ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle#1.

Pallin, Carolina Vendil. 2019. "Russian Information Security and Warfare." In *Routledge Handbook of Russian Security*, edited by Roger E. Kanet, 203-213. London: Routledge.

President of the Russian Federation. 2018. "Decree of the President of the Russian Federation of July 30, 2018 No. 454 "On Amendments to the Decree of the President of the Russian Federation of August 16, 2004 No. 1082 "Issues of the Ministry of Defense of the Russian Federation" and the Regulation." *Official Internet portal of legal information.* July 30. http://publication.pravo.gov.ru/Document/View/0001201807300078?index=1&rangeSize=1.

—. 2021. *Decree of the President of the Russian Federation on the National Security Strategy of the Russian Federation.* Moscow, July 2.

Pynnöniemi, Katri Pauliina. 2019. "Information-psychological warfare in Russian security strategy." In *Routledge Handbook of Russian Security Policy*, edited by Roger E. Kanet, 214-226. London: Routledge.

Reuters. 2021. *Russia accuses Ukraine of troop build-up, starts its own winter drills.* December 1. https://www.reuters.com/world/europe/russia-starts-regular-winter-military-drills-region-bordering-ukraine-2021-12-01/.

—. 2022. *Russia accuses Kyiv of poisoning some of its soldiers in Ukraine.* August 10. https://www.reuters.com/world/europe/russia-accuses-ukraine-poisoning-some-its-soldiers-2022-08-20/.

Roth, Andrew. 2021. *Russia issues list of demands it says must be met to lower tensions in Europe.* December 17. https://www.theguardian.com/world/2021/dec/17/russia-issues-list-demands-tensions-europe-ukraine-nato.

Sitnova, I., and A. Polyakov. 2018. "Fourth-Generation War: Priorities, Principles of Strategy, and Tactics." *Army Journal* 9.

Stepanenko, Kateryna, Karolina Hird, Riley Bailey, Layne Philipson, Nicole Wolkov, and Frederick W. Kagan. 2023. *Russian Offensive Campaign Assessment, February 1, 2023.* February 1. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-february-1-2023.

Tashev, Blagovest, Michael Purcell, and Brian McLaughlin. 2019. "Russia's Information Warfare Exploring the Cognitive Dimension." *MCU Journal* (U.S. Marine Corps University) 10 (2): 129-147.

TASS. 2017. *Russia's defense chief to mobilize new cyber army.* February 22. https://tass.com/defense/932439.

Thomas, Timothy L. 2004. "Russia's Reflexive Control Theory and The Military." *Journal of Slavic Military Studies* 17: 237-256.

—. 2019. "Russian Military Thought: Concepts and Elements." *MP190451V1.* Prod. The MITRE Corporation. McLean, Virginia: The MITRE Corporation.

U.S. Army Asymmetric Warfare Group. 2016. "Russian New Generation Warfare Handbook." December 1. https://info.publicintelligence.net/AWG-RussianNewWarfareHandbook.pdf.

Zabrodskyi, Mykhaylo, Jack Watling, Oleksandr V. Danylyuk, and Nick Reynolds. 2022. "Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022." *Royal United Services Institute for Defence and Security Studies.* November 30. https://static.rusi.org/359-SR-Ukraine-Preliminary-Lessons-Feb-July-2022-web-final.pdf.

Zakharova, Maria. 2022. *Archive Today.* February 28. https://www.facebook.com/maria.zakharova.167/posts/10227769395810054.