

A Russian Military Framework for Understanding Influence in the Competition Period

Tom Wilhelm

Information has become a destructive weapon just like a bayonet, bullet or projectile.

—Vladimir Slipchenko

To the U.S. Army, a competition period is described as actions over time that exploit the operational environment conditions in order to gain a position of advantage below the threshold of armed conflict. At the crux of competition is the ability to create a strategic and operational standoff

to gain freedom of action in any domain. This is done through the integration of political and economic actions, unconventional and information warfare, and the actual or threatened employment of conventional forces.¹ “Russia exploits the conditions of the operational environment to achieve its objectives by fracturing alliances, partnerships, and resolve, particularly through the effective use of information in undermining friendly will.”² In various forms, this description of Russian influence is prolific throughout Western security analysis. The prevailing views often



include the notion that much of Russian influence over events is planned and orchestrated. This is certainly true in many instances; however, identifying the wiring of Russian influence can be difficult as it can not only come from planned operations but also from standard geopolitical practice, spontaneous civic activities, and many other actions and events that contribute to achieving Russian objectives.³ The actors can come from across the entire government and yet not be whole-of-government. Russian influence can involve many aspects of Russian society and other governments and their societies, and it can include extralegal networks too. Adding to this are other insoluble factors such as the opaque institutional dynamics in Kremlin decision-making and the secret activities of the Russian security services including its armed forces and General Staff. Confounding outsiders even more is that any event and activity can be denied or can be the result of *bardak* (a particular Russian understanding of fiasco).⁴ But events that occur while competitively vying to shape and control the security environment can also be confusing for the Russians themselves and for the military in particular. As leading Russian military theorists I. A. Chicharev, D. S. Polulyah, and V. Yu. Brovko observe, the operational environment is characterized by “the confusion of military and non-military array of tools [that] belong

to modern hybrid wars.”⁵ For the Russian military establishment—a keeper of Russian strategic culture and its premier planning institution, the General Staff—this has been alarming, and members have been working to come to grips with it.

There are a variety of frameworks that provide a way to understand how

Russian influence plays out in the current operational environment. These frameworks are often focused on particular military events or explained at sociocultural and political-strategic levels. These models range from case study analyses to a summing-up of Russian mentality and tradition, to Kremlinology, and to mirror reflections of what the military claims the West is doing to Russia.⁶ All offer invaluable insight; however, in terms of a distinctive framework built from Russian military insight, developments of the

General Staff reveal a useful model for examining all levels of influence in the competition period.

The Russian military does not directly or fully illuminate what it does in conceiving, developing, implementing, and coordinating actions to affect what it describes as the “amalgam of calculation and risk” of its adversaries.⁷ To a significant degree, its process is dogmatic, secretive, and opportunistic at the same time. Moreover, sometimes Russian influence events obviously involve the armed forces, and at other times, the armed forces seem to grapple and play catch-up with actions that defy their deep culture of planning.⁸ Nevertheless, surveying some of the General Staff’s doctrinal developments resulted in a structured exposure to how the Russian military may look at influence, particularly in the competition period. There is also the potential to see how they can be expected to deal with it going forward, even emerging with a more consolidated and central role among the state’s security institutions.



Emblem of the General Staff of the Russian Armed Forces
(Graphic courtesy of Wikimedia Commons)

Russia's Defence Minister Sergei Shoigu holds a virtual meeting of the Russian Defence Ministry Board in Moscow on 29 April 2020 that includes Chief of the General Staff Valery Gerasimov, other key General Staff members, and other Russian military leaders. The meeting was held to discuss a variety of issues including measures to mitigate adverse impacts of the COVID-19 pandemic. (Photo courtesy of the Russian Ministry of Defence)



Influencing the Defense of the Russian World and the Goal of Information Warfare

As described in the official military policy, Russia will take military measures to provide for “the safety of the vital interests” of individual Russians, the society, and the state.⁹ Military risks and threats include a “rivalry of proclaimed values and models of development.”¹⁰ The policy, however, instructs the military establishment to apply measures “only after political, diplomatic, legal, economic, informational, and other non-violent instruments have been exhausted” but does not preclude the military’s participation, support, or the development of its capacities in any of these domains.¹¹ In fact, as the doctrine further notes, “There is a tendency towards shifting military risks and military threats to the information space.”¹² This is a telling statement because information warfare is something Russians have developed significantly in their military science over decades. Empowered by this doctrine, which equates to national policy in Russian statecraft, the General Staff’s contemporary list of information warfare components indicates an imaginatively broad vision. It includes international media centers, military bases abroad, human rights organizations, movie and computer gaming industries, private military companies, and even “the need to use world-renowned

Through its media outlets, Russian combat-system developers assert that Russian military robots (as shown in the photo) using sophisticated artificial information will soon have “nearly human capabilities” that will enable them to independently evaluate the changing conditions they face, plot new courses of action, communicate and coordinate with other machines, and make battlefield decisions without human involvement. Such assertions are at least in part intended to intimidate prospective adversaries. (Photo from RT)

academics, such as Nobel laureates.”¹³ According to the military, the goal of influence domination, in this context, is described as protecting national interest by “countering” and “suppressing” attacks against the promotion of Russia and its defense of a *Russkiy mir* (Russian world).¹⁴ In the information domain, Russian military science divides information warfare into informational-technical, which can incorporate cyberattacks and electronic warfare, and informational-psychological, which includes a wide range of activities aimed at creating unpredictability. In the latter, legitimate appearances are maintained but content is changed and the context of information is transformed to fit objectives.¹⁵ According to the military, the ultimate effect of influencing operations would be to have an adversary “self-disorganize” and “self-disorient.”¹⁶

Words matter. The significance of this in Russian military thought is also evidenced in the evolution of

its military terminology. Russian terms of operational art have doctrinal weight. The military, often through the Military Academy of the General Staff and related higher military educational institutions, chooses and uses words carefully after deliberate consideration over time. The lexicon of Russian military science is used to ensure that planning proceeds toward calculable ends and that force-wide developments are anchored to a common ground. In the realm of influence and influence operations, some key terms associated with Russian information warfare have been deliberately evolved in this way, revealing motivations and directions of the General Staff. Some terms are in a state of consideration, indicating that there is still ongoing General Staff doctrinal developments; still, other terms have appeared to guide the General Staff work in the current operational environment. For example, the term “propaganda,” holding onto its Red Army roots, still exists officially to mean the government’s “purposeful” wisdom.¹⁷ However, the military hardly uses it in that positive sense in its current writings, and instead, the nondoctrinal, negative sense of the term pops up more often as something practiced against it. “Counter-propaganda,” once a common feature of the Russian military lexicon and used to explain negative information contrived by adversaries, is in a kind of doctrinal term limbo, and Russians seem to be searching for other ways of expressing this.¹⁸ Some old terms are receiving a face-lift: “sabotage,” for instance, has been expanded to embrace the context of information operations; the doctrinal terms for “deception,” “misdirection,” and “disorientation” are becoming synonyms in describing influence effects.¹⁹ The standard definition of “defense” now includes the “use of precision weapons and highly effective means of information warfare.”²⁰ Other terms like “controlled chaos technology” in the “cultural-philosophical sphere” of “hybrid war” are newer concepts and in a state of discussion and development, along with “information packet” and “simulacra” related to “reflexive control,” which is inclining an adversary to make decisions on his or her own accord that are predetermined to favor the protagonist.²¹ “Disorganization” aims at creating “mismanagement”; “fragmentation,” similarly, refers to actions that disrupt the enemy’s decision-making at crucial times but particularly highlights isolation of key players from making those decisions.²² Operations

launched to accomplish this are “information strikes.”²³ The purpose of “specially created channels” to insert erroneous information may include organizations such as the General Staff’s Main Intelligence Directorate but expressly includes the public media.²⁴

This evolution of terms signals that the General Staff is building a very particular foundation. It is an understanding of not just how information warfare is contextualized in forecasting and describing the nature of conflict but how influence actions can be operationalized or at least dealt with in a more calculable way. For instance, taken together, these concepts are much more than planning and mounting an operation to divert, mask, or deceive an enemy in a tactical moment; the aim is to ultimately shape or change the nature of the conflict itself.

Influence and Russian operational art. In 2015, then chief of the Russian General Staff’s Main Operational Directorate, Gen.-Lt. Andrei V. Kartapolov, published an article in the *Journal of the Academy of Military Science* that described “new-type war.” His article, a work of trend analysis, solidified the General Staff’s previous forecasting and historical surveys. The most famous of these was done by S. G. Chikinov and S. A. Bagdonov that was understood by Western analysts as “Russian new-generation warfare,” and was also used by Chief of the Russian General Staff Valery Gerasimov’s own publication on foresight, the erstwhile “Gerasimov doctrine.” Critically, Chikinov and Bagdonov believed that strategic goals would not be accomplished unless information superiority was assured; Gerasimov’s work indicated that the ratio of nonmilitary to military measures in future war was four to one.²⁵ In terms of military art in what the West recognizes as the competition period, Kartapolov noted a “set of indirect actions” that

Tom Wilhelm has served as the director of the Foreign Military Studies Office (FMSO) since 2007. FMSO conducts open-source research, focusing on the foreign perspectives of understudied and unconsidered aspects of the operational environment. Over his career as a U.S. Army foreign area officer, he has worked and served with Russians and the Russian military in diplomatic assignments, operational missions, field training exercises, arms control implementation, and academic programs.



characterize “new-type war” including “hybrid war.” This list of the forms and methods—a specific nomenclature of Russian military science—was based on the General Staff’s historical analysis of what it believed the West had been doing to attack Russia since before the end of the Cold War.²⁶ Given his position at that time and now as the deputy minister of defence and chief of the Main Military-Political Administration, Kartapolov’s description of the methods can be seen as serving a couple of critical purposes. First, it has been a beacon over key developmental years to orient the General Staff’s doctrinal work and planning focus. Second, it has also illuminated Russian intentions with regard to the nature of contemporary conflict with great consistency.²⁷ In this context, Kartapolov’s description can be understood as a road-map of Russian development and practice.

An Applied Look at Kartapolov’s Framework

The framework has eight parts and involves more than just the military institution:

(1) political, economic, informational, and psychological pressure;

A damaged Buk missile is displayed 24 May 2018 during a news conference by members of the joint investigation team, comprising authorities from Australia, Belgium, Malaysia, the Netherlands, and Ukraine, in Bunnik, Netherlands. Moscow continued to deny involvement in the destruction of Malaysia Airlines Flight 17, even as an international team of investigators said that detailed analysis of video images and photos had unequivocally established that the Buk missile that brought down the plane over eastern Ukraine nearly four years ago came from a Russian-based military unit. (Photo by Francois Lenoir, Reuters)

- (2) disorientation of the political and military leadership;
- (3) spreading dissatisfaction among the population;
- (4) support of internal opposition in other countries;
- (5) preparing and deploying armed opposition;
- (6) deployment of special forces;
- (7) conduct of subversive acts; and
- (8) employment of new weapon systems.²⁸

Some exemplars can help demonstrate how the General Staff may consider influencing actions through the competition phase and initial phase of warfare. (This is not meant to be a definitive list or analysis of events.)

Political, economic, informational, and psychological pressure. As an influence method, political, economic, informational, and psychological pressure can include commonly practiced military engagements and multilateral exercises that Russia uses to develop and to shape political and military relations and partnerships. For instance, military advancements in robotics and increased presence in the Arctic encourage a sense of competitive advantage to outsiders. This is classic, effective military propaganda in accordance with the Russian definition.

Disorientation of the adversary's political and military leadership. Most major Russian media remain quasi-controlled by the Kremlin and thus serve to disseminate Kremlin-approved messages at home and abroad. Each of the major television and radio stations also offer military-themed programs, many of which are supported by the Ministry of Defence and not only highlight the latest military developments and promote the image of the military but also inculcate the Kremlin's threat portrayal. President

Vladimir Putin's descriptions of new "invincible" weapon systems promote a sense of Russian strength and an alternative strategic security environment in which Russia has advantage. These activities have propaganda value in promotion of Russian objectives but can also disorient outside observers and decision-makers.

Spreading dissatisfaction among the target population. Many Russian influence activities have made headlines. One such event is the Malaysian airliner (MH-17) that was shot down over a separatist-controlled territory in Ukraine. In this case, the Russian military establishment supported its government's response with the use of outdated satellite imagery,

dubious weapons transfer documentation, and simulations of a fabricated Ukrainian surface-to-air missile or military aircraft attack. Today, a majority of Russians believe that their country was blameless as do some Ukrainians and even the Malaysian prime minister at the time, Mahathir Mohamad, who stated his support of Russia's "no-proof" position.²⁹ Overall, this effort could be seen as an array of decoy actions that fragmented unifying condemnation of Russia.

Support of internal opposition in other countries.

One way Russia supports internal opposition abroad is with state-sponsored paramilitary organizations. The use of these quasi-state forces develops pro-Russian constituency, discredits other narratives, and acts as an

instigating force or alternative police. This could be considered a disorganizing activity. The Cossacks who were deployed as alternative, pro-Russian police forces in the immediate aftermath of the Crimean seizure are an example of these citizen militias coordinating and integrating in Russian military operations. In the current Russian military encyclopedia, the



Col.-Gen. Andrei Kartapolov, chief of the Main Operational Directorate of the Russian General Staff, conducts a press conference 19 November 2015 detailing the results of Russian air strikes in Syria. (Photo courtesy of Ministry of Defence of the Russian Federation)

Union of Cossacks is specifically noted as a legitimate organization of the "defensive work of the masses."³⁰

Preparing and deploying armed opposition.

Within the targeted state, the support of separatist militias in Eastern Ukraine has many examples. In late May 2014, for instance, a group of outside fighters who supported Ukrainian separatists—the Vostok Battalion—led a series of attacks in and around Donetsk. The fighters, many of whom said they were Chechen, appeared in Ukraine less than one month after Chechen head of state Ramzan Kadyrov threatened to send troops to fight in Ukraine. (Chechnya is a federal territory of Russia.)

Deployment of special forces. The deployment of special forces may include a range of military forces, so “special” in this case means more than just special operations forces. The iconic “Polite People” who facilitated the takeover of Crimea are one example. Another example includes regular armed forces soldiers deployed in deception, such as those members in support of Ukrainian separatists groups. More recently, special forces can be seen in its broadest, interagency sense in November 2018 when three Ukrainian navy ships were seized en route to a Ukrainian port in the Sea of Azov.³¹ The coordinated operation included forces from several agencies and services including the Russian military. In Syria, the Russian Military Police, as the principal force in securing and delivering humanitarian aid, support the strategic Russian image in this conflict. This demonstrates the whole-of-government part of new-type war and might be considered “specially packaged information” aimed to reflexively influence the opinions of other states.

Conduct subversive acts. Russia will conduct subversive acts such as its role with General Staff’s Main

the competition period. Unit 26165, the military’s cyber hacking unit, is one well-known example. It was widely noted that during the Ukrainian conflict, other cyber/software spying and attacks anonymously contacted adversary soldiers on their cell phones to intimidate or persuade them into quitting their posts.³² Russia also jammed GPS signals during NATO military exercises and conducted provocative proximity and laser operations against various commercial and military satellites.³³ Although obviously offensive, the tests of hypersonic munitions fit the new-type war paradigm by informationally “defending” Russia in the competition period.

Taken together as prescribed by the Russian General Staff and viewed as methods of Russian military science, the framework that Kartapolov anointed may be richer than other sociocultural and strategic models and provide a holistic understanding of how the Russian military may observe and deal with influence activities.

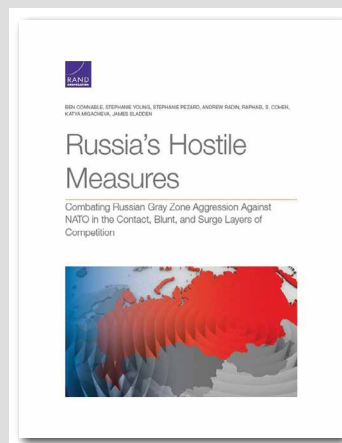
“ВнепреД!” (Forward!)

The General Staff is gaining a central role among Russian security organizations for the development,

integration, and coordination of the national concepts and the doctrine for the defense of the state. Specifically, in a draft of an upcoming presidential decree, the General Staff is designated as the supervising organization for the armed forces, the National Guard troops, the other military formations and agencies

such as the Federal Security Service, Federal Protective Service, Ministry of Emergencies, and the country’s defense industrial complex, as well as other law enforcement agencies and local authorities regarding issues of defense. Putin himself declared this to be “the military organization,” creating a legal bridge over any gaps between the military and nonmilitary space in terms of coordinating state efforts and evolving that security

The RAND report *Russia’s Hostile Measures: Combating Russian Gray Zone Aggression Against NATO in the Contact, Blunt, and Surge Layers of Competition* provides analysis stemming from research focused on examining the diverse means and methods Russia is using to threaten the security and undermine the stability of members of NATO. It is part of the larger research project, “Russia, European Security, and ‘Measures Short of War,’” sponsored by the U.S. Army Deputy Chief of Staff, G-3/5/7. The purpose of the overall project was to provide recommendations to inform the options that the Army presents to the National Command Authorities to leverage, improve upon, and develop new capabilities and address the threat of Russian aggression in the form of measures short of war. To view *Russia’s Hostile Measures*, visit https://www.rand.org/pubs/research_reports/RR2539.html.



Intelligence Directorate officers in a spate of assassination, sabotage, and other *mokroye delo* (wet work) abroad. Besides achieving objectives of the attack, the informational and influencing aspects of these operations also serve to disorient, fragment, and disorganize in accordance with Russian operational art.

Employing new weapons systems. Russia has been employing new weapons systems to achieve influence in



collective from what was previously described in the national military policy.³⁴ It also makes good use of the General Staff's deep culture and institutional design for detailed planning. The General Staff has downplayed this, indicating that the decree mostly provides clearer legal authorities for functions already undertaken such as mobilization and arms exports. However, concomitant initiatives that are enhancing centralized, secure command and control (e.g., the National Defence Management Center, the consolidated National Guard, and sovereign and military communication networks) make it easy to imagine more integrated, whole-of-government defense and security activities networked through the General Staff. It is also not hard to see how the Russian military, in such a supervisory position, will be able to better argue for desired funding and other state resources. At the very least, such development will help the General Staff develop doctrine that overcomes the inherent confusion it loathes while waging more effective influence in the competition period.

In the period of conflict that precedes actual combat, competition for influence is the most prevalent.

Not far from the Donetsk International Airport in Donetsk, Ukraine, a man from the Vostok battalion of the Donetsk's People's Republic patrols the city's Oktyabrsky residential area 16 December 2014. (Photo by Valery Sharifulin/TASS/Alamy Live News)

According to the Russian General Staff, this period is persistent and pervasive. It is seen and experienced by many but can also be elusive to investigation and analytic frameworks. Not everything is an information operation. To get better clarity, Russian military science provides a useful porthole. From doctrinal discussions over time, the General Staff has revealed a structured perspective aimed at justifying a broad use of information warfare and other supportive activities, especially for the competition period. That framework and consensus on the key forms and methods—derived from their military science—gives an outside observer a Russian-based opportunity to consider influencing actions that can simultaneously range from sociocultural to strategic to tactical. It gives the Russians their best institution to bring that together. ■

Notes

Epigraph. Makhmut Akhmetovich Gareev and Vladimir Slipchenko, *Future War* (Fort Leavenworth, KS: Foreign Military Studies Office [FMSO], 2007), 33.

1. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 6 December 2018), vi, 6–7.

2. *Ibid.*, vi.

3. For highlights of implementation of Russian influence actions and information operations in the Ukrainian conflict, see Michael Kofman et al., *Lessons from Russian Operations in Crimea and Eastern Ukraine* (Santa Monica, CA: RAND Corporation, 2017).

4. Sarah A. Topol, "What Does Putin Really Want?," *New York Times* (website), 25 June 2019, accessed 11 February 2020, <https://www.nytimes.com/2019/06/25/magazine/russia-unit-ed-states-world-politics.html>. Quoting Ruslan Pukhov, director of the Centre for Analysis of Strategies and Technologies, a Russian military think tank: "Every time some Western observer says 'Russians did this, Russia did that,' I say: 'You describe Russians like they are Germans and Americans. We are not ... if you don't know the word bardak, you are an idiot and not an analyst of Russia. Because bardak is disorder, it's fiasco.'"

5. I. A. Chicharev, D. S. Polulyah, and V. Yu. Brovko, "Hybrid War: Reconstructionism vs. Deconstructionism," *The Journal of the Academy of Military Science* 65, no. 4 (2018): 58.

6. Dmitry (Dima) Adamsky, "Moscow's Syria Campaign," *Russie.Nei.Visions*, no. 109 (Paris: Institut français des relations internationales [Ifri], July 2018), 7–8. Using the Syrian campaign, Adamsky outlines strategic principles of preservation of controlled tensions, reasonable sufficiency in military involvement, and flexibility.

Also see, for example, Katri Pynnoniemi, "Information-Psychological Warfare in Russian Security Strategy," in *Routledge Handbook of Russian Security*, ed. Roger E. Kanet (Abingdon, UK: Routledge, 2019), 222, which notes a Russian model based on the Russian mentality and national traditions as having four aspects: "formation of positive image of Russia as a country that is effectively solving international conflicts; conduct of psychological operations at the individual and mass consciousness level both in the conflict zone and beyond; the role of Russian special services in conducting psychological operations; [and] protection of the domestic audience and state decision-making bodies from the foreign information-psychological influence."

See also Graeme P. Herd, "Putin's Operational Code and Strategic Decision-Making in Russia," in Kanet, *Routledge Handbook of Russian Security*, 17. Herd explains that "Putin's 'operational code' is driven by the personality of Putin (a function of his education, training, life experiences and psychological-emotional state)."

Also see Janis Berzins, *Russian New Generation Warfare in Ukraine: Implications for Latvian Defence Policy*, Policy Paper #2 (Riga, Latvia: Center for Security and Strategic Research, National Academy of Defence of Latvia, April 2014), 6. The eight-phase model is derived from Russian General Staff Academy work in S. G. Chekinov and S. A. Bagdonov, "The Nature and Content of a New-Generation War," *Military Thought*, no. 10 (2013): 13–15.

Heather A. Conley et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Washington, DC: Center for Strategic and International Studies, October 2016), accessed 14 February 2020, <https://www.csis.org/analysis/kremlin-playbook>. The authors describe a "unvirtuous cycle" of corrupt political and economic influence resulting in "state capture."

See also a comparison of several models in James P. Farwell, "Adversarial Tactics to Undercut US Interests in New Generation Warfare 2019" (Boston: NSI, 3 May 2019), 6–9.

See also Timothy L. Thomas, *Russian Military Thought: Concepts and Elements*, MITRE MP190451V1 (McLean, VA: Mitre Corporation, August 2019), 1-1. Thomas describes a deliberate process of "disorganizing an opposing force, reflexively controlling them, examining numerous forms and methods of applying force by branch of service, and finding innovative ways to employ military art," particularly with a focus on the initial phase of war. Thomas additionally lists the military process as a "mixture of vision, deception, deterrence, outright power, innovative thought, preparation, and the development of alternate realities" (*ibid.*, 12-7).

7. I. N. Vorobyev and V. A. Kiselev, "From Modern Tactics to the Tactics of Network-Centric Actions," *Military Thought* 17, no. 3 (2008): 84–91, quoted in Timothy L. Thomas, *Kremlin Kontrol* (Fort Leavenworth, KS: FMSO, 2017), 186.

8. For example, the Russian General Staff discusses the need for new procedures to overcome shortcomings between national level and armed forces level security assessments in S. P. Belokon and O. V. Kolomoiez, "Scientific-Methodological Problems of Estimating National and Military Security of the Russian Federation," *The Journal of the Academy of Military Science* 61, no. 4 (2017): 4–17. Compare that with Ruslan Pukhov's bardak quote in Sarah A. Topol, "What Does Putin Really Want?"; and Mark Galeotti's coined condition "ad hococracy," in Mark Galeotti, "What Exactly are Kremlin Ties," *The Atlantic* (website), 12 July 2019, accessed 14 February 2020, <https://www.theatlantic.com/international/archive/2017/07/russia-trump-putin-clinton/533370/>.

9. "Military Doctrine of the Russian Federation," Presidential Decree No. Pr-2976 (Moscow: The Kremlin, 2014), sec. 1, para. 8a, accessed 14 February 2020, <https://www.offiziere.ch/wp-content/uploads-001/2015/08/Russia-s-2014-Military-Doctrine.pdf>.

10. *Ibid.*, sec. 2, para. 9.

11. *Ibid.*, sec. 1, para. 5.

12. *Ibid.*, sec. 2, para. 11.

13. V. K. Novikov and S. V. Golubhikiv, "Analysis of Information War in the Last Quarter of a Century," trans. Harry Orenstein, *The Journal of the Academy of Military Science*, no. 3 (2017): 1–14, referenced in Thomas, *Russian Military Thought*, 8-20.

14. "Doctrine on Information Security of the Russian Federation," Presidential Decree No. 646 (Moscow: The Kremlin, 5 December 2016), sec. 23(a) and 23(b), accessed 14 February 2020, http://www.mid.ru/en/foreign_policy/official_documents/-as-set_publisher/CptlCkB6BZ29/content/id2563163. Section 21 notes the military's policies and obligations, particularly protecting Russia's "historical foundations and patriotic traditions"; "Putin's Russian World," *The Moscow Times* (website), 6 May 2014, accessed 14 February 2020, <https://www.themoscowtimes.com/2014/05/06/putins-russian-world-a35150>.

15. Michael Connell and Sarah Vogler, "Russian's Approach to Cyber Warfare" (Arlington, VA: CNA, March 2017), 3, accessed 14 February 2020, https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf; Timothy Thomas, "Russian Information Warfare Strategy: Can the Nation Cope in Future Conflicts?," *The Journal of Slavic Military Studies* 27, no. 1 (2014): 101–2; Pynnoniemi, "Information-Psychological Warfare in Russian Security Strategy," 220; *Condensed Encyclopedic Dictionary*, s.v. "Operations of Informational-Psychological Warfare," comp. V. B. Venprintsev (Moscow: Goryachaya Liniya–Telekom, 2011).

16. Pynnoniemi, "Information-Psychological Warfare in Russian Security Strategy," 218–19.

17. There are numerous examples spread over official Russian military literature. See, for example, A. A. Bartosh, "A Model of Hybrid Warfare," *Military Thought* 28, no. 2 (2019): 9.

18. See, for instance, "Doctrine on Information Security of the Russian Federation," sec. 21(e), which outlines the military policy using the expression "countervailing information and psychological information." See a comparison of "purposeful propaganda" and avoidance of the term in Bartosh, "A Model of Hybrid Warfare," 9, 14–17. Also see the sort of term avoidance in description of "protection against adversary information and psychological impact" in L. A. Kolosova et al., "Moral and Psychological Support System for Combat Troops," *Military Thought* 28, no. 2 (2019): 167.

19. The selected terms (propaganda, counterpropaganda, sabotage, deception, misdirection, defense, controlled chaos technology, information packet, simulacra, reflexive control, disorganization, fragmentation, information strikes, and specially created channels) were compared among the official Russian Ministry of Defence online encyclopedia, accessed 1 July 2019, <http://encyclopedia.mil.ru/encyclopedia/dictionary/list.htm>; N. N. Tyutyunnikov, "Military Thought in Terms and Definitions," *Military Thought* 27, nos. 1–3 (2018); *Condensed Encyclopedic Dictionary*, s.v. "Operations of Informational-Psychological Warfare"; *Military Encyclopedic Dictionary*, ed. A. P. Gorkin et al., vol. 2 (Moscow: Institute of Military History of the Ministry of Defence of the Russian Federation, 2001); *Soviet Military Encyclopedia*, ed. A. M. Prokhorov (Moscow: Military Press, 1986).

20. Tyutyunnikov, "Military Thought in Terms and Definitions," 242.

21. Bartosh, "A Model of Hybrid Warfare," 15; A. S. Brychkov, V. L. Dorokhov, and G. A. Nikonorov, "The Hybrid Nature of Future Wars and Armed Conflicts," *Military Thought* 28, no. 2 (2019): 30; for enhanced explanations and references regarding reflexive control, see Thomas, *Kremlin Kontrol*, 175–98.

22. Tyutyunnikov, "Military Thought in Terms and Definitions," 1:319–20.

23. *Ibid.*, 3:137.

24. Russian Ministry of Defence online encyclopedia.

25. Chekinov and Bagdonov, "The Nature and Content of a New-Generation War," 13–15. The authors continued their argument with the observation about the necessity of information superiority in S. G. Chekinov and S. A. Bagdonov, "A Forecast for Future Wars: Meditation on What They Will Look Like," *Military Thought*, no. 10 (2015): 45; in Thomas, *Kremlin Kontrol*, 98. The 4:1 ratio is available at Valery Gerasimov, "The Value of Science in the Foresight: New Challenges Demand Rethinking the Forms

and Methods of Carrying out Combat Operations," trans. Robert Coalson, *Military-Industrial Kurier*, 27 February 2013. Charles Bartles, "Getting Gerasimov Right," *Military Review* 96, no. 1 (January–February 2016): 34. In his analysis of this work, FMSO analyst Bartles writes, "The important point is that while the West considers these nonmilitary measures as ways of avoiding war, Russia considers these measures as war."

26. A. V. Kartapolov, "Lessons of Military Conflict, Perspectives on the Development of the Related Forms and Methods," *The Journal of the Academy of Military Science* 51, no. 2 (2015): 26–36.

27. See verbatim use of Kartapolov without reference in Chiharev, Poluyak, and Brovko, "Hybrid War: Reconstructivism vs. Deconstructivism"; Brychkov, Dorokhov, and Nikonorov, "The Hybrid Nature of Future Wars and Armed Conflicts," 20–32.

28. Kartapolov, "Lessons of Military Conflict," 36. Also see a discussion of this at Timothy L. Thomas, "Thinking Like A Russian Officer: Basic Factors and Contemporary Thinking on the Nature of War" (Fort Leavenworth, KS: FMSO, April 2016), accessed 14 February 2020, <https://community.apan.org/wg/tradoc-g2/fmsom/fmsom-monographs/194971>.

29. Marnie O'Neill, "Malaysian PM Declares 'No Evidence' Russia Shot Down MH17," news.com.au, 31 May 2019, accessed 22 June 2020, <https://www.news.com.au/travel/travel-updates/incidents/malaysian-pm-declares-no-evidence-russia-shot-down-mh17/news-story/7cb88ca51f21007b625d1603a4d183bf>.

30. Russian Ministry of Defence online encyclopedia.

31. Roland Oliphant and Rob Crilly, "Russian Special Forces Storm Three Ukrainian Navy Ships Sailing through Disputed Waters Off Crimea," *The Telegraph* (website), 26 November 2018, accessed 25 March 2020, <https://www.telegraph.co.uk/news/2018/11/26/russia-fsb-special-forces-seize-ukraine-navy-ships-crimea/>, accessed 14 February 2020.

32. Victoria Vlasenko, "Spam Weapons: In Avdeevka, the Russian Army Used SMS Scare to Deter," RBC-Ukraine, 3 February 2017, accessed 25 March 2020, <https://daily.rbc.ua/rus/show/avdeevke-rossiyskaya-armiya-ispolzovala-ustrasheniya-1486123672.html>.

33. Ryan Browne, "Russia Jammed GPS during Major NATO Military Exercise with US Troops," CNN, 14 November 2018, accessed 25 March 2020, <https://www.cnn.com/2018/11/14/politics/russia-nato-jamming/index.html>; W. J. Hennigan, "Exclusive: Strange Russian Spacecraft Shadowing U.S. Spy Satellite, General Says," *Time* (website), 10 February 2020, accessed 25 March 2020, <https://time.com/5779315/russian-spacecraft-spy-satellite-space-force/>, accessed 10 February 2020.

34. Alexei Ramm, Alexei Kozachenko, and Roman Kretsul, "The Army at Centre of Defence: General Staff Appointed Senior among Security Agencies. It Is Planned to Make General Staff Responsible for Military Organisation in Russia," *Iz.ru*, 26 November 2019, accessed 18 February 2020, <https://iz.ru/930009/aleksei-ramm-aleksei-kozachenko-roman-kretsul/v-tcentre-oborony-genshtab-naznachaiut-starshim-sredi-siloviko>. Putin's expanded "military organization," described in Ramm, Kozachenko, and Kretsul, lists the nonmilitary actors much more specifically those in "a complex of state administration" found in the military policy "Military Doctrine of the Russian Federation," sec. 1, para. 8(j).