APRIL 2020

Improvisation and Adaptability in the Russian Military

EDITOR
Jeffrey Mankoff

AUTHORS
Samuel Bendett
Stephen Blank
Joe Cheravitch
Michael B. Petersen
Andreas Turunen

A Report of the CSIS Russia and Eurasia Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

APRIL 2020

Improvisation and Adaptability in the Russian Military

EDITOR
Jeffrey Mankoff

AUTHORS
Samuel Bendett
Stephen Blank
Joe Cheravitch
Michael B. Petersen
Andreas Turunen

A Report of the CSIS Russia and Eurasia Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. Senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS is ranked the number one think tank in the United States as well as the defense and national security center of excellence for 2016-2018 by the University of Pennsylvania's "Global Go To Think Tank Index."

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, D.C. 20036
202-887-0200 | www.csis.org

Acknowledgments

This publication was funded by the Russia Strategic Initiative, U.S. European Command in Stuttgart, Germany. The opinions, conclusions, or recommendations contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. government.

Contents

Introduction

As the U.S. military pivots back to a world shaped by great power competition, it faces the need of coming to grips with the evolving capabilities and doctrines of its principal rivals, China and Russia. The Russian military, in particular, is rapidly updating its tools and techniques in ways that challenge traditional thinking about great power competition. Having learned from its failures during the Cold War, Moscow is no longer building a force that mirrors those of its rivals. Instead, Russia is investing in areas where it enjoys, or could enjoy, a comparative advantage. Some of these areas are familiar to students of the Cold War, such as a navy that emphasizes attacks on a foe's critical infrastructure. Others, like the growing incorporation of drones in the air, at sea, and on land, are new. If nothing else, Russia's military is adaptive. It also comparatively well-funded, with a solid technological base that, even if it struggles at times to produce completely new systems, allows Russia to be largely self-sufficient.

The development and incorporation of new technologies by the Russian military go hand-in-hand with new thinking about the nature of warfare (especially great power warfare) in the twenty-first century. Russian strategic thought remains focused above all on developing capabilities to counter the technologically superior U.S./NATO militaries. That focus is reflected in doctrinal statements and in the pronouncement of Russian officials, and in force planning. As in the Cold War, it has something of a global element, even if Europe remains the central front. It also incorporates tools and techniques of asymmetric conflict, including psychological and information operations.

To promote better understanding of the Russian military's evolving capabilities and doctrines, the CSIS Russia and Eurasia Program (REP), with support from United States European Command (EUCOM) has undertaken to gather in this short volume a series of papers from leading analysts of the Russian military designed to give planners and executors a clear sense of just where the Russian military is headed. The papers are grouped into two sections: ideas and capabilities. In the first section, Stephen Blank (Foreign Policy Research Institute) analyzes the Russian military's global ambitions, while Andreas Turunen (Conflict Studies Research Center) looks at the evolution of Russian military doctrine on electronic warfare, and Joe Cheravitch breaks down Russia's approach to psychological operations. Section two focuses on capabilities, with Michael Petersen (U.S. Naval War College) examining the Russian navy's ability to carry out counter critical infrastructure missions and Samuel Bendett (Center for Naval Analyses) looking at Russia's drone capabilities.

These papers grow out of the work done over the past year by the Russian Military Capabilities Working Group, a forum co-hosted by REP and the Center for Naval Analyses that provides a space for established and upcoming experts on all aspects of Russian security policy to hear from one another and from outside speakers about work being done at the cutting edge of Russian military analysis. With the support and interest of EUCOM, we asked members of the group to submit proposals for short papers, which would be discussed and workshopped within the group before being submitted for publication. While the papers are the work of their individual authors, they all benefitted from the collective input and wisdom of the Russian Military Capabilities Working Group. We are very thankful to the group members who took the time to read and comment on the papers, to EUCOM for its interest and financial support for the project, and to Carnegie Corporation of New York for funding the Russian Military Capabilities Working Group.

Jeffrey Mankoff

Senior Fellow

Russia and Eurasia Program

Section 1: Ideas

A Russian Global Expeditionary Force?

BY STEPHEN BLANK

Introduction

Despite numerous assertions to the contrary, Russia has developed a strategy, forces, and strategic objectives for global power projection since 2006, when President Vladimir Putin advocated creating forces for global, local, and national contingencies and began training them.[1] Moscow began creating private military forces for use abroad in the 1990s.[2] By 2010, elements of Russia's airborne forces participated in an EU operation to support UN peacekeepers in Chad.[3] Today, Russian forces or proxies are deployed or fighting in Syria, Libya, the Central African Republic, Mozambique, Madagascar, and Venezuela and have participated in failed coups in Montenegro, Greece, and Macedonia. Moscow even offered to send peacekeeping forces to Afghanistan after the recent U.S.-Taliban accords.[4] Clearly, Moscow can sustain these forces. Moreover, Russia has obtained, been offered, or seeks air and navy bases in Venezuela, the Levant, the Horn of Africa, and the Sahel. It may also covet bases in South Asia as it clearly seeks an enhanced presence there.[5] Meanwhile, Russian military literature discusses power projection forces because contemporary war largely occurs in the Middle East, Africa, Venezuela, and other failed states.[6]

[1] Vladimir Putin, "Annual Address to the Federal Assembly," President of Russia Official Website, May 10, 2006, http://en.special.kremlin.ru/events/president/transcripts/24201; Reuben F. Johnson, "The Expansion Process Has Begun," *The Weekly Standard* XII, no. 4 (October 10, 2006).

[2] Sergei Sukhankin, "From 'Volunteers' to Quasi-PMCs: Retracing the Footprints of Russian Irregulars in the Yugoslav Wars and Post-Soviet Conflicts," *Eurasia Daily Monitor*, June 25, 2019; Thomas D. Arnold, "The Geoeconomic Dimensions of Russian Private Military and Security Companies," *Military Review* (November/December 2019): 10-11.

[3] *ITAR-TASS*, Open Source Center CEP 20100266950173, February 26, 2010.

[4] "Russia To Send Troops To Afghanistan If the Country's Official Authorities Ask," Ariana News, March 7, 2020, https://ariananews.af/russia-to-send-troops-to-afghanistan-if-the-countrys-official-authorities-ask/.

[5] Alexey Kuprianov, Kulani Wijayabahu, and Shakti De Silva, "International Relations In South Asia: Russia's and Sri Lanka's Views," Russian International Affairs Council, November 29, 2019, https://russiancouncil.ru/en/activity/policybriefs/international-relations-in-south-asia-russia-s-and-sri-lanka-s-views/.

[6] Valery Gerasimov, "Razvitie Voyennoi Strategii v Sovremennykh Usloviiakh. Zadachi Voyennoi Nauki," *Vestnik Akademii Voyennykh Nauk* 67, no. 2 (2019): 6–11. An English language version is available for those who do not read Russian: "The Development of Military Strategy under Contemporary Conditions. Tasks for Military Science" trans. Harold Orenstein and Timothy Thomas, *Military Review*, November 2019, https://www.armyupress.army.mil/journals/

Power Projection and the Navy

The ambition to project power beyond the Russian Federation's borders dates back to at least 2003.[7] But it has only materialized more recently due to Russia's military reforms, buildup, and lessons from operations in Crimea, Donbas, and Syria. Russia regards these wars as laboratories for future military developments, going beyond the innovative use of weapons.[8] Russia remains a learning military (and government) regarding lessons of contemporary warfare that other powers ignore, disregard, or may simply be incapable of assimilating. Failure to grasp this fact and/or the lessons Russia is learning and applying will breed more global instability, as the attempted coups in the Balkans and war in Ukraine demonstrate.

In 2014, Defense Minister Sergey Shoygu and his deputy, Anatoly Antonov, advocated establishing a global network of air and naval bases to extend Russia's global military presence.[9] Shoygu cited Russia's need for refueling bases near the equator and noted that "It is imperative that our navy has the opportunities for replenishment."[10] While the navy's priority might be homeland defense, naval taskings obviously will far transcend that requirement even though ocean-going ships are being reduced.[11] The commander in chief of the navy, Admiral Viktor Chirkov, concurrently cited the navy's "ocean strategy" and emphasized a large-scale procurement campaign to realize it globally.[12] Even if Chirkov's procurement program remains largely aspirational, incomplete, and has been superseded, and despite the navy's many well-known problems, these new capabilities have considerably increased Russian naval, air, and air defense projection capabilities since 2014. And the navy, in particular, is gaining new strike capabilities for power projection.

Because the navy has failed to develop a sustainable capability for what the West calls a SODCIT (strategic operations to destroy critical infrastructure targets) mission, the alternatives it has developed give it a dual-use global power projection capability in tandem with potential foreign basing.[13] The new submarines, frigates, and corvettes that Russia has built and is building may be designed primarily for littoral and near-sea operations. They are also, however, being used for power projection, and their new missile capabilities—the dual-use Kalibr', Tsirkon, and Onyx missiles—have a serious global

military-review/online-exclusive/2019-ole/november/orenstein-gerasimov/; Patrick Tucker, "Russia Is Perfecting the Art of Crushing Uprisings Against Authoritarian Regimes," *Defense One*, July 12, 2019, https://www.defenseone.com/technology/2019/07/russia-perfecting-art-crushing-uprisings-aid-authoritarian-regimes/158396/; Aleksandr Dvornikov, "Shtaby Dlia Novykh Voin," *Voyenno-Promyshlennyi Kur'er*, July 23, 2018, https://vpk-news.ru/articles/43971.

[7] "Aktual'nye Zadachi Razvitiia Vooruzhennykh Sil Rossiiskoi Federatsii" *Krasnaia Zvezda* no. 190, October 11, 2003; Denis Trifonov, "'Ivanov Doctrine' Reflects Moscow's Growing Confidence In The CIS And Beyond," *Central Asia Caucasus Analyst,* November 19, 2003, http://www.cacianalyst.org/publications/analytical-articles/item/8554-analytical-articles-caci-analyst-2003-11-19-art-8554.html.

[8] Gerasimov "Razvitie Voyennoi Strategii"; Dvornikov, "Shtaby Dlia Novykh Voin."

[9] Bruce Jones, "Russia Searches For Strategic Airbase Partner," *Jane's Defense Weekly*, March 4, 2014, http://www.janes.com/article/34916/russia-searches-for-strategic-airbase-partners.

[10] Ibid.

[11] Bruce Jones, "Russian Navy Ocean-Going Warship Numbers To Be Radically Reduced," *Jane's Defense Weekly*, February 21, 2020, https://www.janes.com/article/94464/russian-navy-ocean-going-warship-numbers-to-be-radically-reduced.

[12] *Ministry of Defense of the Russian Federation,* Foreign Broadcast Information Service, March 2, 2015.

[13] SODCIT is a "strategic operation to destroy critically important targets." See Michael Petersen, *Strategic Deterrence, Critical Infrastructure, and the Aspiration-Modernization Gap in the Russian Navy* (Washington, DC: CSIS, 2020).

intermediate and long-range strike capability.[14] Samuel Bendett also reports that, based on its Syrian experience, Russia has committed itself to giving all of its services unmanned capabilities. For the navy, these comprise unmanned underwater vehicles (UUVs) and unmanned surface vehicles (USVs) that give Russian ships greater intelligence, surveillance, and reconnaissance (ISR) range and capability, along with capabilities for anti-submarine warfare (ASW), maritime border projection, demining, and even combat strike capabilities.[15] Unmanned systems may also be used for maritime ISR and situational awareness, including UUVs that could mimic a submarine's signature or carry small torpedoes.[16]

Moreover, the navy and government have reaffirmed their global aspirations. Russia's 2017 Naval Doctrine states that:

> Military-naval activity represents the state's wholly directed activity toward the formation and support by military means of auspicious conditions in the world ocean for the persistent development of the Russian Federation and realization of the fundamental priorities of its national security.[17]

Military-naval activity is a component of state activity that is executed in the world ocean to prevent aggression against Russia and realize high priority state interests. The navy defends Russia's status as a great naval power globally, is an important part of international stability and strategic deterrence, and conducts an independent naval policy as an equal participant in international naval activity.[18] Furthermore, there is also an explicit requirement for power projection (marine or naval infantry) embedded in that doctrine.

> [The navy possesses] strategic nuclear and conventional naval forces and the ability to implement its combat potential in virtually any area of the World Ocean; and the ability to deploy naval expeditionary groups in a short period of time into the areas of conflict and remain in these areas for an extended period of time without violating the sovereignty of other states: as well as a high level of readiness for actions, including strikes on critically important enemy targets.[19]

Policy and Operations

Meanwhile, Moscow has extended abroad a policy long applied to the former Soviet Union to facilitate these operations. This four-step policy aimed to strengthen Russia's power projection instruments and capabilities. First, it entailed strengthening military capabilities "to cover a wide range of requirements from conducting crisis management operations aimed at averting transnational threats and peacekeeping operations, to unconventional and conventional warfare operations aimed at asserting its interests and deterring external actors."[20]

[14] Ibid.; Stephen Blank, "Behind Moscow's Arms Control Offensive," *Eurasia Daily Monitor*, March 4, 2010.

[15] Samuel Bendett, *Russian Unmanned Vehicle Developments: Syria and Beyond* (Washington, DC: CSIS, 2020).

[16] Ibid.

[17] "Osnovy Gosudarstvennoi Politiki Rossiisskoi Federatsii v Oblasti Voenno-Morskoi Deyatel'nosti Do 2030 Goda," Russian Federal government's website for legal information, July 20, 2017, http://publication.pravo.gov.ru/Document/View/0001201707200015?index=1&rangeSize=1.

[18] Ibid.

[19] Ibid.

[20] Margarete Klein, *Russia's Military Policy In the Post-Soviet Space: Aims, Instruments, and Perspectives*, *SWP Research*

The second aspect is bilateral or multilateral military cooperation with a range of partners (e.g., the late 2019 naval exercises with China and Iran, and with China and South Africa, Tsentr' 2019, and operations with the Egyptian armed forces). Indeed, the Iranian maneuvers expressly aimed—at least in Iran's assessment, as in Venezuela's case below—to tell Washington that intervention risked Russo-Chinese support for Iran.[21] Third comes Russia's efforts to cement ties within or with non-Western multilateral security organizations.[22] The fourth element, arms sales, gives Russia a foothold in purchasing states; that may well be their principal purpose.[23]

Recent force developments have produced a flexible template based on the particular conditions of the crisis or war in question and Russia's assessment of what will advance its interests there. Since the Crimean annexation, elements of the following formations have been located abroad: private military companies; elements of *spetsnaz* forces, naval infantry (increasingly designated for these missions); airborne, naval, and air forces; general-purpose forces' C2 element; the state military in affected countries where they retain some capability like Syria and Venezuela; allied forces (Iran and Hezbollah in Syria); proxy militias (e.g., Hafter in Libya); irregulars recruited from Cossack Balkan, Ukrainian, and other volunteers; and presumed elements of the GRU and other intelligence organizations. Russian law also lets Moscow use FSB and even National Guard units for such overseas operations under an anti-terrorism rubric.[24]

The only political criteria for intervening abroad evidently is if there exist pro-Russian forces of sufficient capability that Moscow can utilize for its objective, and second, if it can keep the level of intervention below the point of generating a serious Western response. Obviously, those criteria are linked: if pro-Russian forces are insufficient or lacking, Moscow's commitment, risks, and exposure grow commensurately. This ensemble of forces can be used as needed at little financial or political cost and with plausible deniability. Moscow can pretend its forces are not fighting abroad, offload the burden of extended distant operations upon private military company forces (PMCs) or local forces, and defang internal criticism about casualties.[25]

By 2019, Shoygu informed the Duma that Russian forces could fight anywhere in the world.[26] In Venezuela, Moscow deployed two planes and 100 military personnel ostensibly to install "special military equipment," but also to "support the Maduro regime."[27] Among

Paper (Berlin: German Institution for International and Security Affairs, 2019), https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2019RP01_kle.pdf. The similarity of her language to that of the naval doctrine should be noted.

[21] "Iranian Admiral Reveals What Prompted Russia, China To Join Iran For Tripartite Drills," Sputnik, December 29, 2019, https://sputniknews.com/military/201912291077893855-iranian-admiral-reveals-what-prompted-russia-china-to-join-iran-for-tripartite-drills/.

[22] Ibid.

[23] Stephen Blank and Younkyoo Kim, "Russia's Arms Sales Policy After the Ukraine Sanctions," *Asian Politics and Policy* XI, no. 3 (2019): 380-398.

[24] Klein, *Russia's Military Policy,* 16.

[25] Ibid., 17; Xinhua, "No Russian troops in Libya: Kremlin," China.org.cn, February 17, 2020, http://www.china.org.cn/world/Off_the_Wire/2020-02/17/content_75715051.htm.

[26] "Russian Defense Minister Says Army Now Capable of Remote Combat Missions," Sputnik, March 12, 2019.

[27] "Anatomy Of the Current Crisis In Venezuela, Part 1: US Meddling and Failed Coup Attempt," PRISM, April 24, 2019, https://www.prismm.net/2019/04/26/12327/; Jiri Valenta, "Russia's Military Should Leave Venezuela Immediately," BESA Center, April 21, 2019, https://besacenter.org/perspectives-papers/venezuela-russia-military/.

others, these forces comprised experts in cybersecurity.[28] Moscow had also dispatched mercenaries from the Wagner Group to Venezuela.[29] While leaders like Chief of Staff General Valery Gerasimov invoked Syria as a template for limited foreign military operations, Moscow's Venezuelan intervention more closely replicated the Soviet Union's strategy for Nicaragua (i.e., using just enough force to deter a U.S. intervention).[30]

Putin has hinted at a Russian base in Latin America as a possible retaliation against Washington's withdrawal from the Intermediate-Range Nuclear Forces (INF) treaty.[31] In fact, Venezuela offered Moscow use of a naval/air base at Lar Orchila Island, and Moscow dispatched Tu-160s bombers there in 2018.[32] Accordingly, we can expect regular visits by nuclear-capable planes and ships to the neighboring naval base, if not permanent deployments.[33] Moreover, Russian and pro-Russian forces in Venezuela could be the foundation for a permanent "counter-revolutionary" force to buttress the Maduro regime.[34] Persistent reports evoked this outcome in 2018-19.[35]

Russia's activities also encompass information and cyber-warfare in targeted states to achieve political leverage. Russia has sent "political technologists" to over 20 African countries to target voters with disinformation campaigns.[36] Russia has also sought to influence elections across Africa and used elements of the Wagner Group for cyber operations there.[37] Concurrently, Moscow has used the template described above in Libya and the Central African Republic as it refines in its "African laboratory" techniques first used in Syria to suppress "color revolutions" or launch its own uprisings to support pro-Russian forces and leaders.[38] Thus, it is developing a new formula for global expeditionary forces, melding both Russian and indigenous, regular, private, and irregular forces integrated by Russian command and control centers.[39]

Russian arms sales and exercises also facilitate power projection operations. In December 2019, Russia, China, and Iran conducted joint maritime exercises off Iran. Iranian officials

[28] Matt Spetalnik, "Russian deployment in Venezuela includes 'cybersecurity personnel': U.S. official," Reuters, March 26, 2019, https://www.reuters.com/article/us-venezuela-politics-russians-idUSKCN1R72FX.
[29] Cristina Maza, "Russian Secret Military Mercenaries Deployed To Venezuela To Protect Maduro From Coup, Capture: Report," *Newsweek*, January 25, 2019, https://www.newsweek.com/russian-military-venezuela-maduro-coup-1306071.
[30] Vladimir Frolov, "Why Moscow Sent Its Military Personnel to Venezuela," *Moscow Times*, April 2, 2019, https://www.themoscowtimes.com/2019/04/02/why-moscow-sent-its-military-personnel-to-venezuela-a65052.
[31] Stephen Blank, "Russia's New Venezuelan Base," *Second Line of Defense*, December 26, 2018, https://sldinfo.com/2018/12/russias-new-venezuelan-base-the-evolving-strategic-context/.
[32] Tom Demerly, "Russian Air Force Tu-160 Bombers Deploy To Venezuela," Aviationist, December 11, 2018, https://theaviationist.com/2018/12/11/russian-air-force-tu-160-bombers-deploy-to-venezuela/.
[33] Ibid.
[34] Tucker, "Russia Is Perfecting."
[35] Valenta, "Russia's Military Should Leave."
[36] Yoni Kazeem, "Russia Is Targeting African Politics and Elections With Misinformation Campaigns On Social Media," *Quartz*, October 31, 2019, https://qz.com/africa/1739308/facebook-bans-russia-accounts-interfering-in-african-elections/; Paul Goble, "Moscow Exporting 'Political Technologists' Beyond Africa to Europe," *Eurasia Daily Monitor*, September 19, 2019.
[37] Jason Burke and Luke Harding, "Documents Suggest Russian Plan To Sway South Africa Election," *Guardian*, May 8, 2019, https://www.theguardian.com/world/2019/may/08/documents-suggest-russian-plan-to-sway-south-africa-election; Carol Castiel, "Mozambique Elections Analysis/Russia in Africa," Voice of America, October 18, 2019, https://www.voanews.com/episode/mozambique-elections-analysisrussia-africa-4050191.
[38] Tucker, "Russia Is Perfecting"; Dvornikov, "Shtaby Dlia Novykh Voin."
[39] Ibid.

asserted that these exercises showed that “Iran cannot be isolated.”[40] Others cited the same goal as in Venezuela, warning Washington away from attacking Iran.[41] In November 2019, the South African, Russian, and Chinese navies conducted joint exercises off South Africa’s coast “to ensure safety of shipping and maritime economic activity.”[42] Similarly, Egyptian paratroopers have participated in annual joint exercises with Russian and other foreign troops in Russia and Egypt since 2017.[43] Russia also directly projects power to Africa. Tu-160 strategic nuclear-capable bombers and their support aircraft flew to South Africa in October 2019, signaling a diplomatic deployment that resembled the deployment of bombers in 2018 to Venezuela.”[44]

Objectives

This multidimensional strategy possesses several visible objectives. Successful operations show foreign leaders in these regions as well as all the great powers that Russia is a global power that must be reckoned with. These operations scratch Moscow’s permanent itch or obsession with status that requires it to persuade its domestic audience of its acknowledged greatness in world affairs. Economically, apart from trade and investment deals that secure needed resources, the economic and military operations overseas generate leverage over key economic and political sectors abroad. Third, Moscow seeks diplomatic support in the UN and globally from targeted governments and regional security organizations (e.g., the Organizations of African States) on issues now occupying the global agenda. Fourth, these operations directly enrich or have the possibility of enriching the state and oligarchs like Yevgeny Prigozhin, Konstantin Malofeev, and others. Fifth, successful power projection operations not only distance the area targeted from the United States and the West, but they also cause problems for Western governments. As one member of the panel reviewing these papers reported, Foreign Minister Lavrov reportedly boasted that Russian operations in Africa certainly “stepped on France’s toes” in Africa.

Finally, and most importantly from an operational standpoint, successful power projection operations permit the acquisition of naval and air bases, port visits, or logistic centers. Not only do those gains facilitate the long-range strike targeting missions against the North Atlantic Treaty Organization (NATO) allies that predominate in Russian strategy, but they also could help solve a problem for the Russian navy. The navy largely runs on diesel fuel which Russia has had trouble acquiring after it invaded Ukraine, its previous source. To

[40] “China, Russia and Iran Begin Joint Naval Drills,” Al Jazeera, December 27, 2019, https://www.aljazeera.com/news/2019/12/china-russia-iran-joint-naval-drills-191227183505159.html.

[41] “Iranian Admiral Reveals,” Sputnik.

[42] “Exercise Mosi Will See Chinese, Russian and South African Navies Work Together,” defenceWeb, October 21, 2019, https://www.defenceweb.co.za/featured/exercise-mosi-will-see-chinese-russian-and-south-african-navies-work-together/.

[43] “Egyptian Paratroopers To Conduct Military Exercise In Russia Next Week,” Egypt Independent, September 9, 2017, https://www.egyptindependent.com/egyptian-paratroopers-conduct-military-exercise-russia-next-week/; “Egypt To Host Joint Drills Of Russian, Egyptian Paratroopers In 2018-MoD,” Sputnik, January 6, 2018, https://sputniknews.com/world/201801061060553794-russia-egypt-drills/; “Egypt Forces Embark On Joint Military Drills With Russia, Belarus,” Ahram Online, August 20, 2019, http://english.ahram.org.eg/NewsContent/1/64/344060/Egypt/Politics-/Egypt-forces-embark-on-joint-military-drills-with-.aspx.

[44] David Cenciotti, “Russian Air Force Tu-160 Strategic Bombers To Make Unprecedented Visit To South Africa,” Aviationist, October 21, 2019, https://theaviationist.com/2019/10/21/russian-air-force-tu-160-strategic-bombers-to-make-unprecedented-visit-to-south-africa/.

the degree that it can acquire stocks of this or other compatible fuels for its ships, it can deploy ships far abroad and to some degree shift the burden of providing for them to the host country.[45]

Doctrine

Gerasimov and other military leaders have openly discussed a strategy of limited foreign operations.[46] Gerasimov highlighted the growing number of actors participating in military actions, including quasi-states, and the use of informational, economic, diplomatic, and military measures in these conflicts whose essence involves using "the protest potential of the fifth column."[47] Since, in his view, Russia's enemies use these wars as well as high-tech operations against Russia, the Russian military must be "ready to conduct new-type wars and armed conflicts, using 'classical' and 'asymmetric' methods of operation."[48] He cites Syria's lessons as the basis for this strategy of limited actions using self-sufficient troops.

Gerasimov further asserted that this strategy consists of planning and coordinating (under Russian command) military and nonmilitary operations of combined Russian and non-Russian professional and otherwise militarized forces, including in humanitarian and post-conflict stabilization operations.[49] Gerasimov also emphasized the increasing role of unmanned- aerial vehicles (UAVs) and counter-UAV electronic operations and the role of information operations in achieving superiority in these scenarios.[50] Moreover, he reiterated that because information transcends national borders, it can underpin covert, remote operations, directly destabilizing a country's internal security.[51]

In 2018, Colonel-General Aleksandr Dvornikov, commander of the Southern Military District, anticipated Gerasimov's ideas. Dvornikov discerns a universal trend towards integrated "camouflaged" forces:

> Such groups are being created on the basis of local resources on the principle of opposition, national, and confessional divisions, by means of organizing irregular troops and popular militias in units that are capable of coalescing into larger-scale formations with the support and under the leadership of the Special Operations Forces and private military companies of other states. This also involves the armed forces of the host-nations, foreign Air Force, Navy and other groupings of troops (forces), civil and nongovernmental organizations, that are all brought together for the purpose of performing tasks in the strategic or operational directions in a unified information-intelligence space.[52]

Moscow also learned here the need and art of creating flexible command and control groupings to conduct integrated strategic-political operations there. Consequently, according to Dvornikov:

[45] Petersen, *Strategic Deterrence.*

[46] Gerasimov, "Razvitie Voyennoi Strategii."

[47] Ibid.

[48] Ibid.

[49] Ibid.

[50] Ibid.

[51] Ibid.

[52] Dvornikov, "Shtaby Dlia Novykh Voin."

> Effectively, we are talking about fragmented irregular armed formations. However, when they are united under the command of the RF AF troops grouping commander, and when acting under a single concept, they acquired a new status, so now they can be called an "integrated grouping" in the full sense of the word.[53]

Gerasimov and Dvornikov's writings outline this emerging trend. Russia can exploit significant sociopolitical, ethnic, or religious cleavages and conduct this form of warfare anywhere it wants. By trial and error, Russia fashioned a way to project its influence and power abroad and will continue experimenting with these forces and tactics. Russian military writing is integrating new forces and concepts into Russia's overall thinking about contemporary war and strategy. Accumulating tensions in ostensibly peripheral areas like Africa, the Middle East, and Latin America have historically helped precipitate crises in more central areas—sometimes even triggering major wars. Without learning political, military, or combined means of meeting these challenges, they will not only become local "forever wars" but will grow into larger, longer, and more violent conflagrations in Europe and Asia.

Dr. Stephen Blank is an internationally-known expert on Russia and the former Soviet Union, who comes to AFPC from the US Army War College where he spent the last 24 years, 1989-2013 as a professor of National Security Studies at the Strategic Studies Institute of the US Army War College in Carlisle Barracks, PA.

[53] Ibid.

The Broader Challenge of Russian Electronic Warfare Capabilities

BY ANDREAS TURUNEN

Introduction

The United States and its allies in Europe employ technologically sophisticated armed forces, which are considered superior to near-peer adversaries such as Russia, especially in a conventional confrontation. This situation has led Russia to increase efforts to find ways to exploit weaknesses and shortcomings in U.S. force posture as part of a wider strategy to gain regional influence at the expense of the United States and its allies. Potential vulnerabilities in the U.S. approach stem from a dependence on technological advantage, as well as from a reliance on the unobstructed flows of information required to achieve information dominance in the battlespace. In order to challenge Western military superiority in Europe, Russia must find creative and effective ways to hinder and deny the functionality of the military information systems required for the United States and its allies to maintain their dominant position across every domain of military interaction.

This recognition has driven a logical conclusion in Russian strategic planning, namely the development, deployment, and use of electronic warfare (EW) capabilities that can be applied not only in conventional scenarios but also within gray zone and hybrid approaches. An important aspect of the Russian way of electronic warfare is the notion of EW capabilities as a force multiplier that can be integrated into every possible scenario and situation, both offensively and defensively. Russian EW assets are present in every domain including land, sea, air, space, and cyber and can be used simultaneously. In recent years, the EW formations in Russia have gained an equal status with combined arms, communications, and aerospace defense formations. For greater effect, EW capabilities can also be used in combination with kinetic, non-kinetic, conventional, and gray zone activities to extend the number of attack vectors and focus the effects on vulnerable centers of gravity. For the United States and its allies in Europe, Russia's increased EW capabilities carry substantial and perhaps even decisive risks, especially in scenarios which allow the elements of surprise, initiative, and deniability to be utilized to undermine the strength of Western powers.

The successful application of EW capabilities includes the degradation of combat capabilities, denial of movement (including reinforcement efforts), disruption of information and data flows, obstruction of support elements such as logistics, and disabling the effective use of C5ISR systems. In addition to conventional warfare, EW systems can be used to target the infrastructure of states hosting U.S. troops. Hence, for the United States and its allies, the primary recommendations for countermeasures include a greater emphasis on electronic warfare in operational and strategic planning, as well as a further increase in training for scenarios involving degraded or denied operational information environments.

The Way of Russian Electronic Warfare

From the period of the Russian Empire to present day

Russia has strong traditions in the field of electronic warfare and holds that its first implementation dates as far back as the blockade of Port Arthur during the 1904-05 Russo-Japanese War, where the Russian Imperial Navy successfully jammed Japanese radio communications to disrupt artillery correction for battleships.[1] Four decades later, the development of maneuver warfare in the Second World War significantly highlighted the role of communications in a gradually accelerating tempo of operations. Based on the lessons learned from that war, Soviet military theorists recognized the importance of functioning communications in "operational level troop control"; loss of communications leads rapidly to loss of organization, leading to a risk of defeat.[2] For this reason, the Soviets developed a Radio-Electronic Combat (REC) doctrine to merge their electronic warfare capabilities into an integrated discipline.[3] The integration of EW doctrine aligned with broader lines of Soviet strategic culture, including concealment and deception. Subsequently, the way electronic warfare capabilities were regarded during the Soviet period was inherited into the Russian view of electronic warfare in which EW acts as an integrated discipline in every category of combat activity.

Throughout the Cold War, Soviet EW capabilities evolved at a considerable pace. However, after the collapse of the Soviet Union, the domestic industry responsible for developing electronic warfare capabilities also stagnated. Procurement from the electronic warfare industry decreased significantly, which affected the resources available for research and development (R&D).[4] After nearly two decades, the modernization of the Russian armed forces that began in the mid-2000s revitalized the electronic warfare industry. Significant resources were directed into R&D, while inventories were modernized.[5] The consequences of almost a decade of rapid

[1] Jonas Kjellén, *Russian Electronic Warfare: The role of Electronic Warfare in the Russian Armed Forces* (Stockholm, Sweden: FOI, September 2018), 19, https://www.foi.se/rest-api/report/FOI-R--4625--SE.

[2] U.S. Department of the Army, *Field Manual No. 100-2-1, Soviet Army: Operations and Tactics* (Washington, DC: Department of the Army, July 1984), 15-1, https://fas.org/irp/doddir/army/fm100-2-1.pdf.

[3] Ibid.

[4] Andrew Radin et al., *The Future of the Russian Military: Russia's Ground Combat Capabilities and Implications for U.S.-Russia Competition* (Santa Monica, CA: RAND Corporation, 2019), 187, https://www.rand.org/pubs/research_reports/RR3099.html.

[5] Ibid., 188.

development and modernization were clearly visible in the conflicts in eastern Ukraine and Syria.

Russian EW capabilities today

Despite significant developments in Russian electronic warfare capabilities during the last decade, Soviet tradition is still strongly present in modern Russian EW doctrine. The difference, however, is in the definition of radio-electronic combat, which has broadened concurrently with the overall development of operational art. Radio-electronic combat doctrine consists of four subcategories: Electronic attack, electronic protection, countermeasures against technical reconnaissance, and radio-electronic information support measures.[6] By definition, electronic attack and protection are almost identical to Soviet radio-electronic doctrine. Unlike in the West, Russian electronic warfare practitioners also count the use of conventional force against an adversary's radiofrequency systems as a form of an electronic attack (for example anti-radiation missiles). The modern Russian definition of electronic attack also considers possible cyber operations within the EMS-framework. The next 5 to 20 years are likely to see continuing convergence between the EMS and cyberspace, creating new vectors for attacking systems via the linkages between different warfighting domains—in other words, delivering weaponized effects via different domains of interaction, such as a virus against a networked system via radiofrequencies.[7]

The Russian armed forces possess a wide array of EW means intended to cover the entire operable electromagnetic spectrum for all physical domains of warfare (land, sea, submarine, air, and space). The variety of EW systems is tailored to support a wide selection of needs, from tactical and operational to the strategic level. At the strategic level, electronic warfare capabilities are in general targeted against the North Atlantic Treaty Organization's (NATO) C4ISR systems and global communications networks. The main component of this strategic-level electronic attack capability (strategic radio jamming system) is the Murmansk-BN system which operates in high frequency (HF) range and is designed to jam intertheater communications.[8] Murmansk-BN stations are also a vital part of the armed forces' rapidly increasing capabilities in the Far North, emphasizing the strategic importance of the Arctic in the Russian strategic mindset.[9] Below the so-called "strategic umbrella," EW equipment and formations are currently being integrated into increasingly lower-level organizational structures. With the 2008 military reform, maneuver brigades were restructured to include an organic EW component, such that electronic warfare is always present in the Russian Ground Forces' operational execution, and can be seen as a full combat support branch along with more traditional

[6] Kjellén*, Russian Electronic Warfare*, 22.

[7] Joseph Trevithick, "Ukrainian Officer Details Russian Electronic Warfare Tactics Including Radio 'Virus,'" *The Drive*, October 30, 2019. https://www.thedrive.com/the-war-zone/30741/ukrainian-officer-details-russian-electronic-warfare-tactics-including-radio-virus.

[8] Roger N. McDermott*, Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum* (Tallinn, Estonia: ICDS, September 2017), 15, https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf.

[9] Atley Staalesen, "Russia says its radio-electronic shield now covers the Arctic," Barents Observer, May 21, 2019, https://thebarentsobserver.com/en/arctic-security/2019/05/russia-says-its-radio-electronic-shield-now-covers-arctic.

branches such as logistics, indirect fires, et cetera.[10] This state of affairs significantly differs from Western operational art, where electronic warfare support usually originates from specialized units that are subordinated to the force structure conducting the operations. Accordingly, the Russian approach prioritizes EW support to a much greater degree than its Western counterparts.

Russia's ongoing military operations in eastern Ukraine and Syria provide a laboratory for testing new capabilities and technologies in real-life operational scenarios. Operations there also provide an opportunity for Russia's potential adversaries to observe trends in how Russia conducts electronic warfare. In this context, Syria and eastern Ukraine differ significantly in terms of operational environment. In Syria, the Russian Armed Forces have been mainly testing aerial effect electronic equipment such as unmanned aerial vehicle (UAV) jamming systems, SIGINT collection capabilities, and countermeasures against intelligence, surveillance, and reconnaissance.[11] In eastern Ukraine, the focus has been more on supporting ground operations and testing new methods for combining information, cyber, and EW measures. A major trend in the conduct of electronic warfare operations in eastern Ukraine has been target designation for indirect fires by UAV-based signals intelligence, which has tested the Ukrainian armed forces' capability to control their electronic emissions and therefore to protect themselves from Russian electronic reconnaissance.

By observing Russia's ongoing electronic warfare actions in Syria and Ukraine, Western militaries can obtain insight into the quality of the opposing electronic measures they would face in a potential conflict with Russia. Secondly, in a conflict, Russia would presumably use both nonconventional (e.g., applying electronic warfare measures against civilian infrastructure or using intelligence acquired through electronic means for targeting civilian devices) and conventional electronic warfare creatively, simultaneously, and with a considerable level of flexibility. Based on its record in Syria and Ukraine, Russia would also fail to discriminate between civilian and military targets, especially in terms of infrastructure and logistics—in the electronic as well as the physical domain, where Russia has demonstrated an understanding of the war-winning value of targeting civilians and humanitarian facilities.

Russian EW Challenging U.S. Regional Advantages

Russia's strategic methodology

The Russian armed forces' desire and motivation to invest heavily in electronic warfare capabilities stems from Russia's relative weakness compared to the armies of the United States and the NATO-allied countries. The Russian armed forces are less technologically advanced, especially in the fields of sensors and C4ISR, and therefore are unable to challenge U.S. forces in Europe, or the NATO allies, in technologically symmetric clashes. Second, although Russia's armed forces are considerable in size, they would still have difficulty sustaining a regional-level conflict in the European theater without the eventual use of

[10] Kjellén, *Russian Electronic Warfare*, 83.

[11] Anna Varfolomeeva, "Signaling strength: Russia's real Syria success is electronic warfare against the US," Defense Post, May 1, 2018, https://thedefensepost.com/2018/05/01/russia-syria-electronic-warfare/.

nuclear weapons.[12] In terms of electronic warfare capabilities, Russia, therefore, strives to render the technological gap less relevant through electronic means while exploiting the vulnerabilities of U.S. and NATO assets by fully controlling the electromagnetic spectrum.

Russia's approach is based on a combination of creativity, deception, "un-restrictedness," shock-effect, and flexibility. In this context, EW is well suited due to its potential application across all domains of military interaction. In conventional and hybrid-like scenarios, electronic warfare presents a meaningful challenge against more traditional force compositions, as it can be used as an instrument to achieve combinational effects such as psychological targeting via EW assets.[13] Compared with NATO and U.S. forces in Europe, the Russian armed forces also enjoy more freedom in the range of situations where they can conduct electronic warfare missions during or before conflict and are also more flexible in achieving their strategic objectives without the same normative constraints. Even with this emphasis on EW, Western analysts should avoid overemphasizing hybrid-like scenarios or neglecting Russia's steadily increased capability to conduct large-scale conventional operations by "traditional" means.[14]

Main Western vulnerabilities

When addressing the threat that Russian EW poses, it is vital to recognize the most vulnerable BLUEFOR systems and the ways these vulnerabilities can be exploited. In hybrid-like scenarios, EW measures can be directed against vital functions of civilian society, meaning that protective measures and contingency plans are not only the concern of armed forces. Modern-day societies are dependent on the EMS in a number of ways; for example, jamming radio communications may cause severe damage to aviation and maritime traffic flows. Radio systems used by air traffic control (ATC) and maritime vessel management (VTS) are not designed to operate in a hostile environment, where communications are completely or even partially jammed, and even low-level interference might paralyze them, restricting traffic flows.

Evidence from the conflict in eastern Ukraine suggests that Russia has also used its EW capabilities to wage information warfare against the civilian population by suppressing cellular communications and afterwards creating false mobile base stations using the UAV-mounted Leer-3 EW system. The so-called IMSI-catching method forces targeted devices to connect with a false base station, enabling propaganda broadcasting directly to personal devices.[15] The effectiveness of the information campaign is likely to increase when IMSI-catching is combined with other information warfare tools such as social media influencing. Importantly, such hybrid EW-scenarios are likely to include attempts at deniability, causing difficulties in attribution.

[12] Fredrik Westerlund et al., *Russian Military Capability in a Ten-Year Perspective – 2019* (Stockholm, Sweden: FOI, December 2019), 65-67, https://www.foi.se/rest-api/report/FOI-R--4758--SE.

[13] Yuriy Danyk et al., "Hybrid War: high-tech, Information and Cyber Conflicts", *Connections* 16, no. 2 (Spring 2017): 12-13, https://www.jstor.org/stable/pdf/26326478.pdf?refreqid=excelsior%3Ab736cfdd0a5b24ff6a9531bb5be6881c.

[14] Westerlund et al., *Russian Military Capability*, 65-67.

[15] Yuri Lapaiev, "Russian Electronic Warfare in Donbas: Training or Preparation for a Wider Attack?" *Eurasia Daily Monitor* 17 no. 34 (March 2020), https://jamestown.org/program/russian-electronic-warfare-in-donbas-training-or-preparation-for-a-wider-attack/.

In more conventional and "traditional" warfare scenarios, the proportion and intensity of Russian EW measures are likely to be substantially greater. The technological gap between the West and Russia forces the Russian side to target the adversary's systems across the electromagnetic spectrum in order to effectively decrease its combat potential. On the tactical and operational levels, U.S./allied communications and radar systems would encounter jamming measures seeking to complicate command and control functions, the targeting cycle, and effective use of fires. At the strategic level, intelligence gathering sensors would be undermined through a combination of EW capabilities and physical *maskirovka* actions such as camouflaging and smoke screening. The aim of such measures is to create multilayer protection against sensors operating in different parts of the electromagnetic spectrum (e.g., ELINT, COMINT, IMINT). Interfering with navigational systems is also likely to occur, as observed during recent military exercises in the Arctic.[16] However, GPS jamming itself is mainly a defensive and self-protective measure to mitigate the threat of standoff weapons reliant on satellite guidance.

Threats against U.S. interests

The primary threat in the evolution and application of electronic warfare measures in the Russian armed forces is their ability to contribute to the defeat of U.S. and European NATO allies in a conventional confrontation in the European theater. If Russian military decisionmakers are able to exploit a potential window of opportunity, be successful in long-term preparations, and achieve escalation dominance in the early hours of a potential conflict, Russia could gain both territorial and military advantage, which would transform into political gain. Electronic warfare can play a role both before and during the initial phase of conflict.

1. **Long-term preparations** in the gray-zone stages of (or alternatives to) conflict could include applying low-intensity electronic warfare measures to both gauge the capabilities, resilience, and reactions of adversaries and to exercise interference with logistics and infrastructure in order to hamper movement of reinforcements and supplies in the pre-conflict situation.[17]

2. **Escalation dominance** is achievable with the assistance of electronic warfare capabilities by distorting, jamming, denying, and eliminating key C4ISR systems, equipment, and vehicles in order to paralyze decisionmaking, hinder intelligence processes, and seize key moments in the very first stages of overt hostilities.

The rapid advance of the Russian armed forces' electronic warfare capabilities also lowers the threshold for Russia to challenge the United States and its allies in the European theater militarily. Hence, for the United States, the maintenance of credible deterrence requires prioritizing means of countering the Russian electronic warfare threat in order to avoid the risk of defeat—and indeed to reduce the risk of armed conflict overall. Doing so requires maintaining clear superiority in capabilities including EW-resistant communications, electronic warfare platforms such as the

[16] Thomas Nilsen, "Russian military officials arrive in Oslo as Norway puts GPS jamming facts on the table," Barents Observer, March 4, 2019, https://thebarentsobserver.com/en/security/2019/03/russian-military-officials-arrive-oslo-norway-provides-facts-gps-jamming.
[17] Keir Giles, "Missiles Are Not The Only Threat" FOI, n.d.

EA-18G Growler, and both manned and unmanned systems capable of operating in electronically denied environments without continuous datalink connection to ground stations and satellites.

Finally, the Russian way of electronic warfare has the potential to be imitated by U.S. adversaries outside of Europe. In the Indo-Pacific region, China has an interest in obtaining technological capabilities that threaten U.S. dominance in the Pacific region. In the next 10 years, the possible proliferation of Russian EW-exports, combined with access to commercial dual-use products such as drone technology may see other potential adversaries, including smaller state actors such as Iran, Syria, and North Korea but also non-state actors such as militant organizations and state-supported proxy forces, follow Russia's lead. Russia has already deployed Krasukha-4 systems in Syria, which have been suspected of engaging in GPS spoofing activities.[18] According to Russian state media, this system has also been exported abroad.[19] The expansion of Russian electronic warfare capabilities beyond Europe raises the cost of deterrence for the United States due to the increased potential for U.S. adversaries to exploit vulnerabilities stemming from the U.S. overreliance on technological superiority.

Ways to overcome the Russian EW challenge

A vital first step in countering the Russian EW challenge is the acceptance that Western forces do not enjoy unchallenged control of the electromagnetic spectrum. Unlike in recent asymmetric conflicts against non-state actors, Russia as a near-peer adversary has developed its EW capabilities that deliberately aim to exploit NATO's dependence on high-end technology. Russia uses EW as a force-multiplier to add delays to the system-oriented command and control cycle of U.S. and NATO forces, causing friction and potentially significant levels of confusion during operations. In the European theater, the electromagnetic spectrum is highly likely to be contested by Russia. Although the term anti-access area denial (A2/AD) is controversial, it can be applied, for instance, to describe the difficulties facing the Baltic states in terms of electronic warfare. As EW equipment operates within the electromagnetic sphere, it is subjected to the limits of geography as well as to the laws of physics. Forward operating areas in the European theater are located in close proximity to the territory of the Russian Federation and can be targeted by Russia from all the domains of combat (ground, air, sea, submarine, and space) at any time.

Operating in this environment challenges Western militaries to act in a number of ways. First, they must recognize that they will be operating in a highly challenged electromagnetic environment. Second, strategic prioritization and well-written doctrines and manuals alone are not sufficient for tackling the challenges stemming from electronic warfare. Routine, systematic efforts must be conducted to prepare troops for operating under electronic attack in multiple domains, potentially simultaneously. Each soldier must be trained to identify the indicators of an

[18] C4ADS, *Above Us Only Stars* (Washington, DC: C4ADS, 2019), 48, https://static1.squarespace.com/static/566ef8b-4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf.

[19] "Foreign Buyers interested in Russia's Krasukha electronic warfare systems – company," TASS, August 26 2015, https://tass.com/russia/816597.

electronic attack and react in an appropriate manner. Third, the persistent condition of a challenging EW environment has to be embedded in the conduct of operational planning. Operational situations involving electronic warfare can be mathematically and physically modeled, allowing chokepoints and critical points of failure to be recognized, leading to more efficient planning. Finally, countering the Russian EW threat requires a high level of adaptation in many fields of the Western way of warfare and therefore increased awareness of the challenges .

Recommendations

Based on this assessment, the United States and its NATO allies should:

1. **Those NATO partners and allies that have not already done so should recognize the significance of the threat stemming from the capability and advancement of the Russian Armed Forces' electronic warfare measures.** Recognition of the threat implies prioritization of awareness regarding electromagnetic conditions in operational planning to ensure operability in electronically denied environments and situations. Training for troops to conduct combat actions without wireless communications, positioning systems, and integrated electronic field services must be incorporated in every stage of initial training and skill maintenance across all branches of service. Formations must be able to conduct successful combat operations without reliance on sea, air, and land-based support due to the threat of electronic interference. Operations in asymmetric and non-linear hostile environments where the full range of electronic warfare measures is applied should also be exercised.

2. **Recognition of both the significance and the consequences of Russian electronic warfare capabilities must continue in the long-term strategic planning of the United States and its allies.** Technology development strategies must prioritize ways to minimize the effects of hostile electronic actions while maximizing the effectivity of counter-electronic warfare systems and measures. Confidence in the United States' enduring technological advantage must be challenged in strategic thinking, leading to the identification of operational gaps and elimination of vulnerabilities. Awareness concerning the significance of Russian electronic warfare should also be expanded beyond the European theatre to other strategic directions in order to prepare for the proliferation of Russia's effective electronic warfare capabilities to countries regarded as strategic opponents, including China.

Conclusion

Russian electronic warfare capabilities are a continuously evolving challenge that can only be countered by investment and institutional change. Years of Western emphasis on counter-insurgency and combat operations against non-peer adversaries created an embedded sense of security and superiority in the conduct of operations. Despite recent efforts to challenge this complacency, refocusing on countering threats from peer and near-peer rivals, including EW, still requires time and sustained effort. For the United States and NATO member states, the moment of action is now in order to sustain deterrence in the European theater. Russia will continue to develop and enhance its electronic warfare capabilities while finding new vulnerabilities and attack vectors utilizing the full spectrum of electromagnetic means across the domains of military interaction. Lack of a meaningful response by Russia's adversaries carries within it the risk of defeat and hence risks emboldening Russia to even more assertive interventions in Europe.

Andreas Turunen is a research analyst at Conflict Studies Research Centre specialized in Russian defence analysis, hybrid warfare, and strategic communication.

From Leaflets to “Likes”: The Digitalization and Rising Prominence of Psychological Operations in Russia’s Military

BY JOE CHERAVITCH

Introduction

Russia’s employment of information warfare aimed at the West continues to punctuate headlines surrounding elections, the Ukraine conflict, and a host of other international issues. Russia’s military intelligence agency, the GRU (*Glavnoe razvedevatel’noe upravlenie,* or Main Intelligence Directorate), is often at the forefront. “Information confrontation (*informatsionnoe protivoborstvo*),” the overarching concept that guides many Russian digital campaigns, is bifurcated into a technical aspect, like the malware that facilitates hacking, as well as a psychological one, which involves everything from artillery shells that explode into leaflets to websites to influence the Russian diaspora.[1] The focus on “effective” propaganda during Defense Minister Sergey Shoygu’s 2017 rollout of the information operations force exemplifies the mounting importance of psychological operations to Russian strategy. Nonetheless, international observers have paid more attention to the technical capabilities than to the psychological operations (PSYOP) that constitute half of the equation behind Russian information campaigns.

[1] Most Russian military publications on information confrontation discuss the inseparability of technical from psychological aspects of electronic warfare, computer network operations, intelligence activities, psychological warfare, and military deception (*maskirovka*)—all of which mutually reinforce one another. See: A.N. Limno and M.F. Krysanov, “Informatsionnoe protivoborstvo i maskirovka voysk,” *Voennaya mysl’*, no. 5, (2003). One of the most authoritative figures within the GRU to write about information confrontation is Vyacheslav Kondrashov, a former deputy chief, who in 2016 published an article titled “information confrontation in the cybernetic space.” See: Vyacheslav Viktorovich Kondrashov, “Informatsionnoe protivoborstvo v kiberneticheskom prostranstve,” Nauchno-issledovatel’skiy tsentr problem bezopastnosti, August 22, 2016.

Russia's military has long used psychological warfare to undermine conventionally superior enemies. According to a 2006 publication on information confrontation, General Aleksandr Suvorov, perhaps Russia's most renowned military commander, used PSYOP to influence Piedmontese soldiers to surrender to his Austro-Russian force during a campaign against Revolutionary France.[2] Over a century later, Russian military intelligence used covert media and frontline leaflets to attempt to pry Slavic nationalities from the Central Powers during World War I.[3] The Red Army's special propaganda department during World War II used leaflets, radio, and loudspeakers to call on Axis soldiers, particularly non-German ones, to lay down their arms and join their respective national fronts in liberating the workers of Eastern and Central Europe from fascism.[4]

History looms large over the GRU's approach to contemporary information confrontation. A GRU manual on psychological warfare published in 1999, for example, highlights the Soviet Union's annexation of eastern Poland in 1939 as an example of the efficacy of using national, religious, and ethnic differences to divide an enemy country.[5] Wartime themes emerge in current GRU influence operations like the Victory for Peace campaign, an early 2015 effort to promote pro-Soviet and Russian narratives of World War II, through social media and a GRU-run online news network.[6]

Post-Soviet Development

But GRU PSYOP officers in the post-Soviet period also turned to other states when studying psychological warfare, leading to their growing perception that Western operations posed a serious threat.[7,8] The vast resources behind NATO's information warfare apparatus, according to one officer, generated a "strong envy" among Russian counterparts.[9] Nonetheless, other military authors saw an asymmetric route to overcoming Western predominance in the "information space" through the internet, such as the ability of proxies supporting former Yugoslav president Slobodan-Milošević during

[2] L.V. Vorontsova and D.B. Frolov, *Istoriya i sovremennost' informatsionnovo protivoborstva*, Goryachaya-liniya, 2006, 22.
[3] In August 1915, for example, the Main Directorate of the Russian General Staff established the "Nord-Sud" telegraph agency to broadcast propaganda to several Balkan countries, with an emphasis on Romania. See: A.B. Atashov, *Propaganda na Russkom fronte v gody pervoy mirovoy voyny*, Spetskniga, 2012, 50-1.
[4] The memoirs of M.I. Burtsev, a special propaganda commander from 1939 through World War II, serve as a thorough primary account of psychological operations conducted by the Red Army at the time. See: M.I. Burtsev, *Prozrenie*, Voenizdat (1981).
[5] The author adds, "Addressing the mass consciousness of such groups, especially if they are harassed by the government, is very productive." Vladimir Gavrilovich Krysko, *Sekrety psikhologicheskoy voyny*, Minsk, 1999. The textbook was featured in a 2017 article published in *The Moscow Times*. See: Alexey Kovalev and Matthew Bodner, "The Secrets of Russia's Propaganda War, Revealed," *Moscow Times*, March 1, 2017.
[6] Renee Diresta and Shelby Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019* (Stanford, CA: Stanford Internet Observatory, 2019), 43-51.
[7] After Soviet collapse, special propaganda was rebranded the Center for Foreign Military Information and Communication and directly subordinated to the GRU. See: "Osobiy front", *Argumenty vremeni*, January 10, 2018. These units eventually adopted symbols that featured a five-pointed carnation per a ministry of defense decree in 2005, which is a symbol unmistakably associated with Russian military intelligence. See: "Ofitisal'no. Prikazy i direktivy ministra oborony RF," *Rossiyskoe voennoe obozrenie*, no. 001 (2006): 77-80.
[8] Kapitan Valentina Makarenkova, "Epokha bol'shoy nelyubvi," *Ural'skie voenniye vesti*, no. 95 (2001); Evgeniy Yurchevskiy, "Versiya. Sleduyushchiy – Iran?" *Na strazhe Rodiny*, no. 137-8 (2003).
[9] Vladimir Akhmadullin, "Amerikanskie psikhobortsy," *Nezavisimoe voennoe obozrenie*, no. 029, (2004): 7; Makarenkova, "Epokha bol'shoy nelyubvi"; Yurchevskiy, "Versiya. Sleduyushchiy – Iran?"

the war in Kosovo to appeal to internet users while disabling enemy messaging through cyberattacks.[10] A 2007 article coauthored by a senior GRU PSYOP commander elaborated:

> [T]he development of the internet is accompanied by an increasingly widespread use of the opportunities it provides for the implementation of information warfare, a growth in scale and complexity of its participants' actions, which are performed by both state and individual groups.[11]

The disappointment by many Russian officers in the inability to respond to perceived information operations conducted by Western mass media and governments during the Georgian War in 2008 further underscored the importance of digital influence operations in modern conflict. As cybersecurity analyst Emilio Iasiello asserted, Georgia won the information war in 2008 in part because it sought private public relations expertise and reported Russian airstrikes on civilian targets, allowing Georgia to win over the hearts and minds of the international community, despite Russia's dominance in the physical battlespace.[12] As one Russian defense pundit described shortly after the conflict, the Russian military failed to make use of the internet to build public support for its military operations, as the North Atlantic Treaty Organization (NATO) did with its public webpages established shortly after the onset of their operations in Afghanistan, partly due to a "famine" of qualified personnel.[13] An official with the GRU's PSYOP faculty at the Ministry of Defense's Military University, for example, saw a need to further digitalize its curriculum after the Georgian War.[14] Its alumni demonstrated at least a nascent capability to conduct internet-based influence operations by the onset of the Ukraine crisis, including efforts to mobilize pro-Russian communities in Ukraine through disinformation on social media, such as using fake profiles on Facebook to pit pro-Russian Ukrainians against protestors by portraying the latter as *zapadentsy* (Westerners), and issuing physical threats over the internet to pro-Russian figures in southeast Ukraine to legitimize official claims that radical Ukrainian nationalists were encouraging violence in the region.[15] At the same time, sources confirmed to Russian state press outlets that the military sought to build an information operations branch that would integrate the diverse elements of modern information confrontation. As a Russian military expert explained, the psychological aspect was no less important than the technical means of modern warfare:

> Psychological warfare technologies can inflict no less damage to an adversary than means of armed attack, and informational weapons built on the basis of

[10] Yu.O. Yashchenko, "Internet i informatsionnoe protivoborstvo," *Voennaya mysl'*, no. 3 (2003).

[11] A. Kostyukhin, G. Gorbunov, and A. Sazhin, "V planakh komandovaniya vs S.Sh.A," *Zarubezhnoe voennoe obozrenie*, no. 5 (2007).

[12] Emilio J. Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," *Parameters*, no. 2 (2017): 53-4.

[13] Vladimir Shcherbakov, "Spetspropaganda otsidelas' v kustakh", *Nezavisimoe voennoe obozrenie*, No. 29 (2008).

[14] S.A. Cheshuin, "Osobennosti sovremennovo informatsionnovo protivoborstva i ikh uchyot pri podgotovke spetsialistov zarubezhnoy voennoy informatsii v Voennom universitete." The article as of February 2020 is available here: https://pandia.ru/text/77/194/29043.php. Although this version is anonymous, the author maintains a copy attributed to S.A. Cheshuin. The main training pipeline for GRU PSYOP officers is the Faculty of Foreign Military Information at the Defense Ministry's Military University in Moscow. According to a description on a regional website, the faculty exclusively sends graduates to the GRU: http://moscow-russia.ru/voennyy-universitet-ministerstva-oborony/.

[15] Ellen Nakashima, "Inside a Russian disinformation campaign in Ukraine in 2014," *Washington Post*, December 25, 2017.

> psychological influence technologies have much greater destructive, penetrating, and selective capability.[16]

In January 2015, an ostensibly pro-ISIS hacking outfit named CyberCaliphate posted allegedly sensitive information exfiltrated from U.S. Central Command networks.[17] Months later, the group would claim responsibility for temporarily disabling France's TV5 Le Monde's channels in a far more sophisticated attack. Investigators quickly deduced that the actors behind that attack, however, were probably Russian because the Arabic messaging used as part of the operation was riddled with mistakes and the malware being circulated strongly resembled that of an intrusion set previously linked to hackers backed by Moscow.[18] In late 2018, the United Kingdom's National Cyber Security Center publicly attributed CyberCaliphate to the GRU.[19] The campaign marked an unprecedented interaction between the GRU's technical cyber activities and its psychological operations, with units from both ends of the information confrontation spectrum supporting the effort.[20] The following year, Chief of the General Staff General Valeriy Gerasimov revealed that officers participating in a large-scale exercise established information confrontation groups for the first time.[21] GRU influence campaigns aimed at Ukraine exhibited what that integration of cyber and psychological capabilities meant for operations. They combined cyberattacks and influence efforts conducted by proxies like Cyber Berkut along with electronic warfare platforms and cell phone-site simulators to demoralize Ukrainian soldiers and citizens through SMS messages that typically emphasize the supposed futility in fighting for the Ukrainian government or attempt to provoke unrest by forwarding disinformation about drafts for military service.[22] Throughout the Ukraine conflict, the importance of the psychological aspect of information confrontation continued to gain traction in defense circles. For instance, a Russian professor presenting on the "transformation of information wars" at Russia's 2018 Armiya conference asserted that Russia faced a new era in propaganda:

> [W]e are witnessing the erasure of the borders between 'military propaganda' and information manipulation without a military-political and even political focus.
>
> [. . .]
>
> Propaganda of the past was not a dialogue. Now, a constant dialog is implied, and this requires a completely different form of propaganda during peacetime.[23]

[16] "V vooruzhennykh silakh sozdayut voyska informatsionnykh operatsiy," *Nezavisimoe voennoe obozrenie*, no. 16 (2014).

[17] Brian Fung and Andrea Peterson, "The CENTCOM 'Hack' That Wasn't," *Washington Post*, January 12, 2015.

[18] John Lichfield, "TV5Monde Hack: 'Jihadist' Cyber Attack on French TV Station Could Have Russian Link," *Independent*, June 10, 2015; Bill Chappell, "French TV Network Hacked By 'Cyber Caliphate' Group," NPR, April 9, 2015.

[19] Kim Sengupta, "Russian Spy Agency GRU Responsible for International Cyberwar, UK Government Says," *Independent*, October 4, 2018.

[20] Anton Troianovski and Ellen Nakashima, "How Russia's military intelligence agency became the covert muscle in Putin's duels with the West," *Washington Post*, December 28, 2018.

[21] "Na ucheniyakh 'Kavkaz-2016' vpervye otrabotali 'informatsionnoe protivoborstvo'," RIA Novosti, September 14, 2016.

[22] Troianvoski and Nakashima, "How Russia's military…" (20); Ukrainian sources claim that other GRU units equipped with electronic warfare equipment are responsible for SMS messages along the front, such as the 2140th Psychological Operations Detachment. See: "Stali izvestny dannye o voyskakh 'psikhov' Rossii," Tribun, February 6, 2018.

[23] Dmitriy Gennadievich Evstaf'ev, "Transformatsiya informatsionnykh voyn: ot klassicheskoy propagandy k infor-

Strengths and Weaknesses

Perhaps the greatest strength held by the GRU's information confrontation apparatus is its ability to combine electronic warfare, cyber, and psychological operations. Not all of these operations require advanced technology. The GRU's PSYOPs units have kept a foothold in conducting the kind of tactical, low-tech operations involving face-to-face communication and loudspeakers, mostly a product of the Soviet-Afghan War and refined during the Chechen Wars.[24]

These experiences probably served as the foundation for frontline information confrontation in Syria, which Russia's ground force-commander argued allowed Russian forces to "shake the situation from the inside within a matter of days."[25] But the GRU's flexibility extends beyond the ability to switch between digital and physical propaganda; Russian military intelligence is unfettered by either domestic or international legal constraints, affording personnel free rein to go after whichever targets with any digital means they please. For good reason, the liberal democratic states comprising NATO lack a similar freedom when conducting information operations, which are subject to a litany of legal and bureaucratic considerations.

But the GRU's information confrontation machine faces significant obstacles in its bid to match the West in covert digital warfare. Most significantly, it very likely lacks the resources and human capital to build and expand relevant units. According to a 2017 survey published by a Russian cybersecurity firm on states' cyber-capabilities, Russia ranked only fifth among leading states in resourcing cyber-forces, far behind China and the United States.[26] Pay and retention are probably at least partly responsible for staffing issues,[27] and PSYOP units likely face the same challenges from corruption that affect the broader Russian military.[28] These deficiencies probably play a large part in the operational

matsionno-sotsial'noy dekonstruktsii na baze integrirovannykh kommunikatsiy," Konferentsiya *'psikhologicheskaya oborona'*, August 23, 2018, 20.

[24] For a comprehensive account of special propaganda operations during the Soviet-Afghan War, see: Nikolay Pikov, Afganskie zapiski spetspropagandista, *Desyatka*, 2007.

[25] Aleksandr Dvornikov, "Shtaby dlya novykh voyn," *Voenno-promyshlenniy kur'er*, July 24, 2018.

[26] Mariya Kolomychenko, "V internet vveli kibervoyska," *Kommersant*, January 10, 2017. Though the firm's survey was reported by several Russian media outlets, its methodology was largely unexplained and opaque. The report as of February 2020 is available here: "Kibervoyni 2017: Balans sil v mire," Zecurion, January 2017, https://www.zecurion.ru/upload/iblock/cb8/cyberarmy_research_2017_fin.pdf.

[27] A current opening for a position in the GRU's Far East PSYOP unit, for example, involving "computer" and "translation" work requires intermediate English skills and offers a salary significantly less than the regional average. Additionally, the vacancy as of mid-February 2020 had been viewed over 1,200 times with no responses: "Vakansiya № 440887," Centr Zanyatosti Naseleniya, http://employmentcenter.ru/vacancy/?action=read3&id=440887. According to Ukrainian sources and resumes of former personnel, Unit 03134 is the Center for Foreign Military Information and Communications for the Far East Military District: "Stali izvestni dannie o voiskax "psihov" Rossii," Tribun, February 6, 2018, https://tribun.com.ua/47273; "Rukovoditel podradeleniya," Superjob, https://habarovsk.superjob.ru/resume/rukovoditel-podrazdeleniya-8060291.html. As of early 2020, the average salary in Khabarovsk is close to 50 thousand rubles, or $787: "Srednyaya zarplata v Khabarovske v 2020 godu," BANKIROS, September 1, 2019, https://bankiros.ru/wiki/term/srednaa-zarplata-v-habarovske.

[28] In 2015, the commander of a different probable PSYOP unit based in Chita faced up to four years in prison for granting financial bonuses to his subordinates and pocketing their money. The commander fell under a protected veteran status based on his service in Chechnya and Georgia-Abkhazia. Additionally, a former colleague defended the officer's conduct as a necessity to meet demands in a period of meager funding, such as using bonuses to finance construction projects ordered by more senior commanders. See: "Eks-komandira sekretnoy voinskoy chasti Chity budut sudit' za

errors committed by GRU specialists—most notably mistranslations that lead to their attribution during false-flag operations and which perhaps limit the impact of narratives promoted through social media.[29]

Whatever their shortcomings, GRU PSYOP units are likely to remain at the forefront of Moscow's efforts to digitally undermine its perceived adversaries. While their covert messaging—belied by linguistic troubles and possibly an unfamiliarity with the platforms used to promote it—may fall flat in many cases, the cyberattacks used to support them certainly present significant threats to targeted networks. Nevertheless, as demonstrated by a recent (unattributed) disinformation operation in Ukraine that played on local coronavirus fears to incite rioting, information operations can have significant physical consequences even in the absence of cyberattacks.[30]

Moreover, the GRU is one actor among many that support Russia's foreign policy and military objectives through covert digital influence. Although they seemingly lack the ability to conduct sophisticated cyber operations, online "trolls," including those that operate under Russian oligarch Yevgeniy Prigozhin, have demonstrated effectiveness in reaching target audiences through an approach rooted in marketing rather than military strategy.[31] While the GRU takes a longer-term approach to its digital propaganda, such as laundering lengthy narratives through social media proxies and accounts, Prigozhin's enterprise relies more heavily on memes to aggravate targeted populations to quick action. As the Russian revolutionary Georgiy Plekhanov described, "A propagandist presents many ideas to one of a few persons; the agitator presents only one or a few ideas, but he presents them to a mass of people."[32] The prospect that Russian military intelligence extensively collaborates with a security-service outsider like Prigozhin is dubious, but a de facto and tacit division of labor between their digital propaganda apparatuses certainly allows Moscow to simultaneously approach a given target audience with multiple techniques.

prisvoenie premiy podchinyonnykh," *Chita.ru*, September 9, 2015. Several months earlier, the same commander was brought to a regional military court for allegedly sowing marital discord through false information on social media: A. A. Ryabkov, "Postanovlenie № 1-91/2015 ot 26 avgusta 2015 г. po delu № 1-91/2015," Sudebnie i normativnie akti RF, https://sudact.ru/regular/doc/v6vMa7eMdb6P/.

[29] Possibly the most notable case of this outside of the 2016 effort to influence the U.S. presidential election is the poor Arabic used by CyberCaliphate in the wake of the cyberattack on France's TV5 Le Monde. See: "Russian hackers likely behind 'IS group cyber attack' on French TV network," France 24, June 10, 2015, https://www.france24.com/en/20150610-france-cyberattack-tv5-television-network-russia-hackers. For instance, an article on U.S.-Russia relations published in late 2019 on a GRU-sponsored news portal was rife with grammatical errors and was largely ignored by social media users, while similar errors undermined narratives related to the Syrian conflict on a different page. See: Diresta and Grossman, *Potemkin Pages & Personas,* 29, 39.

[30] According to press reports, on February 20, in response to rumors circulated on social media and text messages, residents of Novi Sanzhary, Ukraine, blocked roadways and threw stones at buses they believed were carrying coronavirus-positive patients that had arrived in their town. The unrest necessitated intervention by Ukraine's national guard and riot police, which resulted in nine injured officers and 24 arrests. Ukrainian intelligence claimed that unidentified actors, outside of Ukraine, sent a fake email ostensibly created by Ukraine's health ministry claiming that there were five Ukrainians who had contracted coronavirus, which combined with social media rumormongering to give Ukrainians the notion that people arriving in Novi Sanzhary were infected. See: Christopher Miller, "A Viral Email About Coronavirus Had People Smashing Buses And Blocking Hospitals," BuzzFeed News, February 20, 2020.

[31] Kelsey Sutton, "Russian Trolls Used 'Digital Marketing Best Practices' to Sow Discord, Senate Reports Find," *Adweek*, December 17, 2018.

[32] Peter Kenez, *The Birth of the Propaganda State: Soviet methods of mass mobilization, 1917-1929* (New York: Cambridge University Press, 1985), 7.

Conclusion

Just as leaflets were used to attempt to divide enemy coalitions along ethnic, religious, and social differences in the past, modern GRU operators apply those techniques to undermine NATO and its partners through social media and cyberattacks. These techniques were most recently demonstrated in the spate of cyberattacks against Georgia in late 2019, which, according to U.S. Secretary of State Mike Pompeo, aimed to "sow division, create insecurity, and undermine democratic institutions."[33] Information confrontation, in this sense, represents digital echoes of techniques forged through some of the worst conflicts in human history. It falls on the shoulders of analysts and experts to bridge the vast differences between Western and Russian approaches to digital conflict, differences rooted in historical experiences and contemporary realities, in order to equip decisionmakers with a better understanding of the actors behind these furtive campaigns that are almost as certain to occur as the elections, military exercises, and regional conflicts they seek to impact.

Joe Cheravitch is a Russian information operations analyst in the cybersecurity industry. Cheravitch worked as a government and defense analyst focusing on international cyber-warfare and influence operations since 2014.

[33] Dan Lamothe, "U.S. joins other nations in accusing Russia of cyber attack in Republic of Georgia," *Washington Post*, February 20, 2020.

Section 2: Capabilities

Strategic Deterrence, Critical Infrastructure, and the Aspiration-Modernization Gap in the Russian Navy

BY MICHAEL B. PETERSEN

Introduction

How capable is the Russian Federation Navy (RFN) of inflicting significant damage against U.S. and European critical infrastructure? Historically, the navy's wartime missions focused on ensuring a second nuclear strike capability and defense of Russia's maritime approaches. Over the last decade, however, the RFN has accrued a new counter-infrastructure mission designed to control conflict escalation or force an adversary to sue for peace. Most commonly, this mission involves attacks utilizing non-strategic nuclear or conventional means. Indeed, the RFN's doctrinal statements place a high priority on the ability to carry out such attacks. However, despite massive investment, the navy has important limitations on its ability to do so. Its decade-long modernization has given it the ability to target critical infrastructure locally and regionally, but it has struggled to build a fleet to fulfill its more ambitious objectives farther afield, especially against the United States. Russia is closing this aspiration-modernization gap, but challenges will persist, especially in the near term.

Destruction of Critical Infrastructure: Increasing Centrality in Russian Naval Thought

In Russian thinking, strategic deterrence operations are executed in peacetime and wartime, and they feature what western strategists might define as conflict dissuasion and escalation control.[1] Military forces achieve these missions through pre-conflict

[1] See Anya Loukianova Fink, "The Evolving Concept of Russian Strategic Deterrence: Risks and Responses," *Arms Control Today* 46, no. 6 (July/August 2017): 14-20; Kristin ven Bruusgaard, "Russian Strategic Deterrence," *Survival* 58, no. 4 (August/September 2016).

signaling and by inflicting specifically assigned damage criteria in local, regional, and strategic conflicts. In regional and strategic conflicts—wars against the North Atlantic Treaty Organization (NATO) in particular—this criteria is met in part via attacks against an adversary's critical infrastructure. These operations perform the vital function of military signaling during what Russian thinkers term the "period of threat," and then apply measured force against strategic targets during the ensuing "initial period of war." Thereafter, these operations also provide a means of escalation management.[2]

The importance of critical infrastructure attacks in Russian military analysis has been increasing for at least a decade. For example, in their 2009 survey of post-Cold War conflict dynamics, Colonels A.V. Serzhantov and A.P. Martoflyak wrote that modern war "focuses its main efforts on key government and military control systems, military infrastructure, the economy, and sources of livelihood that, if destroyed, put the state's existence on the line." Attacks on "critically vital targets," according to the authors, would compel an adversary into ending the conflict.[3]

Naval thinkers have likewise been considering this approach for years. In 2007, Admiral Vladimir Masorin, then commander-in-chief of the Russian Navy, wrote that modern economies' dependence on energy and transportation systems "makes it possible to regard elements of those systems as the *key objects* for influencing the economies of potential adversaries." Destruction of these key objects, Masorin held, leveraged a strategic vulnerability and meant that adversaries could be more easily deterred or compelled to end a conflict on terms favorable to Russia.[4]

Over the following decade, these considerations became embedded in Russia's thinking about its navy. A 2016 *Military Thought* article argued that in addition to its more traditional missions, the RFN now had a "qualitatively different task," to "crush the adversary's military economic potential by directly impacting their vital centers from the sea using conventional sea-based long-range high-precision weapons." The navy was ideal for this task because it could, according to the authors, deploy anywhere in the world "to attack the adversary's critically important ground-based facilities without violating, until a certain moment, its national sovereignty."[5]

With the rise of Russia's precision strike capabilities, the Ministry of Defense (MOD) and RFN have embraced these ideas as well. According to the MOD, one of the critical

[2] For a full treatment of Russia's philosophy on strategic warfighting and damage criteria at various levels of conflict, see Dave Johnson, Russia's Conventional *Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds* (Livermore, CA: Lawrence Livermore National Laboratory Center for Global Security Research, 2018), https://cgsr.llnl.gov/con- tent/assets/docs/Precision-Strike-Capabilities-report-v3-7.pdf. The Russian phrase for attacks against critical infrastructure is "strategicheskaya operatsiya po porazheniyu kriticheski vazhnykh obyektov" (strategic operation to destroy critically important objects). The phrase "strategicheskaya operatsiya" (strategic operation] has a specific definition in the Russian military lexicon and denotes joint force strikes that are coordinated and connected by purpose, place, task, and time. See Military Encyclopedia of the Russian Ministry of Defense, http://encyclopdia.mil.ru/encyclopedia/dictionary/details.htm?id=10378@morfDictio- nary.

[3] A.V. Serzhantov and A.P. Martoflyak, "Modern Military Conflicts," *Military Thought* 2 (2009): 94. Emphasis in original.

[4] Vladimir Masorin, "Naval Doctrine as a Component Part of the Russian Federation Military Doctrine," *Military Thought* 2 (2007). Emphasis in original.

[5] O.V. Alyoshin, A.N. Popov, and V.V. Puchnin, "The Naval Might of Russia in Today's Geopolitical Situation," *Military Thought* 25, no. 3 (2016): 17.

wartime tasks for the RFN is to "destroy enemy land-based facilities at long distances."[6] The RFN's 2017 *Fundamentals of the State Policy of the Russian Federation in the Field of Naval Operations for the Period Until 2030* is more expansive, noting:

> [The navy possesses] strategic nuclear and conventional naval forces and the ability to implement its combat potential in virtually any area of the World Ocean; and the ability to deploy naval expeditionary groups in a short period of time into the areas of conflict and remain in these areas for an extended period of time without violating the sovereignty of other states; as well as a high level of readiness for actions, including strikes on critically important enemy targets.[7]

Specifically, the Fundamentals note that "destruction of the enemy's military and economic potential by striking its vital facilities from the sea" can enhance deterrence and provide a measure of escalation control through the use of precision-guided munitions. This is the official enshrinement of what the Fundamentals deem to be a "qualitatively new objective" for the RFN.[8]

New Ships for a New Objective?

Has the RFN's intensive modernization under President Vladimir Putin provided it with the capacity to sustainably and credibly provide signaling in a threatened period of military conflict, as well as counter-critical infrastructure missions during the initial period of war and beyond? Results are decidedly mixed. While Kalibr cruise missiles, the key weapons in the RFN's precision strike complex, have proven to be quite capable, production of new platforms to deliver those missiles has been problematic. Russia has been reasonably successful with smaller, less complex platforms, but measured against its own expectations for modernizing the force with larger, more complex platforms, it has struggled. As a result, the Russian navy has developed a force that allows it to use its smaller platforms to credibly threaten counter-critical infrastructure operations locally and regionally, but it has failed to develop the sustainable global capability to which its guiding doctrinal statements aspire.

New ship construction is emblematic of this dynamic. The RFN generally envisioned new Admiral Gorshkov-class frigates, the most sophisticated class of Russian surface warships constructed since the Cold War, as the foundation of a revived Russian surface fleet.[9] The lead ship was laid down in 2006, but problems plagued it for over a decade, and it was only accepted for service in July 2018.[10] A second Admiral Gorshkov-class frigate was laid

[6] "Missions," Russian Federation Ministry of Defense, https://eng.mil.ru/en/structure/forces/navy/mission.htm.

[7] Anna Davis, trans., *Fundamentals of the State Policy of the Russian Federation in the Field of Naval Operations for the Period Until 2030* (Newport, RI: Russia Maritime Studies Institute, 2017), 11, https://dnnlgwick.blob.core.windows.net/portals/0/NWCDepartments/Russia%20Maritime%20Studies%20Institute/RMSI_RusNavyFundamentalsENG_FINAL%20(1).pdf?sr=b&si=DNNFileManagerPolicy&sig=fjFDEgWhpd1ING%2FnmGQXqaH5%2FDEujDU76EnksAB%2B1A0%3D.

[8] Ibid., 12.

[9] "Fregat proyekta 22350 'Admiral Gorshkov' vyshel na ispytaniya v Beloye more," RIA Novosti, September 22, 2015, https://ria.ru/20150922/1273336488.html.

[10] Ilya Kramnik, "Noveyshiye fregaty okazalis' slishkom slozhnymi i dorogimi," *Izvestia*, September 15, 2011, https://iz.ru/news/500810; Paul Schwartz, *Admiral Gorshkov Frigate Reveals Serious Shortcomings in Russia's Naval Modernization Program* (Washington, DC: CSIS, 2016), https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/160310_Schwartz_AdmiralGorshkov_Web.pdf.

down in 2009 and may join the fleet in early 2020.[11] While the navy expects to eventually receive six of these ships, it has produced exactly two of them in fourteen years.[12] The problems with the Admiral Gorshkovs became so acute that the RFN ordered a smaller substitute frigate with reduced capabilities. In 2010 and 2011, the MOD signed contracts for the delivery of six Admiral Grigorovich-class frigates, three of which the RFN accepted for service.[13] While these frigates come equipped with some of Russia's most advanced naval combat systems, they lack the survivability, range, and magazine depth that would allow them to execute sustained global deterrence and combat missions.[14]

Since the start of its 2014 war with Ukraine, Russia has struggled to complete orders for all of its new surface combatants. Prior to the war, all maritime gas turbine engines were manufactured by Zorya-Mashprojekt in Ukraine, which subsequently canceled production. Russia was unable to equip any of the remaining frigates it had ordered, and gas turbine engines were unavailable for a planned 3400-ton Derzky-class "super-corvette." Moscow then sold the three incomplete Grigorovich frigates that had begun construction (but lacked engines) to India.[15] The Russian company NPO Saturn claims that it has begun small batch production of gas turbine engines, but the first serially produced engines, originally scheduled for delivery in 2019, have still not arrived as of early 2020.[16]

The failure to procure new frigates in significant numbers drove the RFN into fielding higher numbers of smaller (800-1500 ton) corvettes and patrol vessels designed for littoral and near-sea operations. The RFN has accepted eight Kalibr-armed Buyan-M-class corvettes, and another four are under construction. In addition, the lead ship of a new the Karakurt-class corvette was commissioned at the end of December 2018 (two are currently in service), and the RFN expects to receive 18 of the vessels.[17] The navy has also commissioned two 1500-ton Bykov-class patrol ships since December 2018, with both serving in the Black Sea Fleet.[18]

All of these smaller vessels utilize marine diesel engines for their propulsion. But EU sanctions against Russia in 2014 cut off the supply of these engines, and Russia's domestic diesel industry has been unable to ramp up to meet the increased demand. According to an industry source, Russian diesel engines "have a huge import dependency due to an array of foreign-made components," so the industry has had to start almost from scratch.[19]

[11] "'Admiral flota Kasatonov' poobeshchali peredat' VMF v pervom kvartale 2020 goda," Flotprom, February 17, 2020, http://flotprom.ru/2020/Испытания17/.

[12] "Russian Navy to Lay Keels for other Two Gorshkov-Class Frigates in 2020, Insiders Say," Mil.Today, February 6, 2020, http://mil.today/2020/Industry2/.

[13] Office of Naval Intelligence, *The Russian Navy: A Historic Transition* (Suitland, MD: Office of Naval Intelligence, 2015), 22.

[14] For a good, short summary of the Grigorovich FFG's capabilities, see "Project 11356 Admiral Grigorovich Class Frigates," Naval Technology, https://www.naval-technology.com/projects/project-11356-admiral-grigorovich-class-frigates/.

[15] "OSK poluchila den'gi po kontraktu s Indiyey na pestroyku fregatov proyekta 11356 – Rakhmanov," Interfax, September 24, 2019, https://militarynews.ru/story.asp.?rid=1&nid=518002&lang=RU.

[16] "Russia Starts Serial Production of Marine Gas Turbine Engines," Naval Today, January 16, 2018, https://navaltoday.com/2018/01/16/russia-starts-serial-production-of-marine-gas-turbine-engines/; "Russian Navy to Get First Serial Home-Made Gas Turbines in 2019," Mil.Today, May 23, 2018, http://mil.today/2018/Industry12/.

[17] "Russia Commissions Lead Karakurt-Class Corvette Mytishchi," Naval Today, December 12, 2018, https://navaltoday.com/2018/12/18/russia-commissions-lead-karakurt-class-corvette-mytishchi/.

[18] "Den'gi na flot byli. Ikh dazhe potratili," *Voyennoye Obozreniye*, April 5, 2019, https://topwar.ru/156426-na-samom-dele-dengi-na-flot-byli-ih-dazhe-potratili.html.

[19] "Experts: Russian Naval Ships to Change D49 Engines for D500," Mil.Today, November 28, 2018, http://mil.to-

Moscow purchased a small number of diesel engines from China, but these substitute engines either consistently broke in testing or would not fit inside the engineering spaces of the smaller Russian vessels.[20]

Despite these challenges, smaller surface combatant and diesel submarine construction has been adequate to meet the potential demands of local and regional counter-critical infrastructure missions. Alongside smaller corvettes and patrol vessels, construction of new Kalibr-equipped diesel submarines has been relatively successful, and several have joined the fleet recently. These Project 636.3 Kilo-class diesel submarines have been a mainstay for several years.[21] They are capable platforms, but like small surface combatants, are range, speed, and firepower limited, particularly if called upon to credibly sustain the threat of global counter-infrastructure operations.

The maritime requirements of counter-critical infrastructure operations directed against the United States, combined with Russia's lack of overseas maritime infrastructure, mean that the Russian navy must rely on large, complex, covert, survivable platforms with more firepower and extended endurance, especially nuclear-powered guided-missile submarines (SSGNs). These submarines are capable of long deployments at sea, holding the mainland United States at risk without surfacing or returning to port for three or even four months, and their covert capabilities render them more difficult to track and target.

Russia's newest operational SSGN is the now-famous Yasen-class SSGN *Severodvinsk*. Construction on *Severodvinsk* began in late 1993, but with the country in the throes of economic collapse, work virtually ground to a halt while most of the country's existing submarine fleet spent the decade rusting at the pier. In 2014, the *Severodvinsk* was finally commissioned and began operational deployments.[22] Its sister submarine, the modernized Yasen-M class SSGN *Kazan,* was laid down in 2009. Sea trials in 2018 identified major problems with *Kazan's* "auxiliary systems," and according to a Defense Ministry source, the submarine may not be available until 2021.[23]

day/2018/Navy28/; "'Ot remonta dvigateley k seriynomu proizvodstvu': Kingiseppskiy mashnostroitel'nyy zavod kak mnonoprofil'noye predpriyatiye," Flotprom, February 13, 2020, https://flotprom.ru/2020.Оборонка76/.

[20] Maxim Klimov, "Ob ekstrennyih merah po razresheniyu kriticheskih problem nashego nadvodnogo korablestroeniya," Novosti VPK, November 16, 2018, https://vpk.name/news/235005_ob_ekstrennyih_merah_po_razresheniyu_kriticheskih_problem__nashego_nadvodnogo_korablestroeniya.html; "Newest Russian Border Patrol Vessel Sidelined by Chinese-Made Engine Problems," Defence Blog, September 4, 2018, https://defence-blog.com/news/newest-russian-border-patrol-vessel-sidelined-by-chinese-made-engine-problems.html; Stepan Kotcherga, "Russian Navy Brand New Corvette Towed Through Dardanelles. Something Wrong?" Maritime Bulletin, November 6, 2018, https://maritimebulletin.net/2018/11/06/russian-navy-brand-new-corvette-towed-through-dardanelles-something-wrong/.

[21] "First Project 636.3 Submarine Enters Service with Russia's Pacific Fleet," TASS, November 25, 2019, https://tass.com/defense/1092443.

[22] Office of Naval Intelligence, *The Russian Navy: A Historic Transition*, 18; Maxim Klimov, "APKR 'Severodvinsk' sdan VMF s kriticheskimi dlya boyesposobnosti nedodelkami," *Voyennoye Obozreniye*, May 19, 2019, https://topwar.ru/157559-apkr-severodvinsk-proekt-885-jasen-sdan-vmf-s-kriticheskimi-dlja-ego-boesposobnosti-nedodelkami-protivotorpednoj-zaschity-podlodok-vmf-rf-net.html.

[23] "Istochnik: v 2019 godu pervyy "Yasen'-M" ne zhdite," *Flotprom*, May 17, 2019, Flotprom, https://flotprom.ru/2019/Севмаш8/; Andrei Riskin, "Atomnaya submarina 'Yasen,'" *Nezavisimaya Gazeta*, May 20, 2019, http://www.ng.ru/armies/2019-05-20/100_jasen200519.html; "Glava OSK rasskazal o problemakh pri ispytaniyakh golovnogo 'Yasen-ya-M," *Flotprom*, May 17, 2019, https://flotprom.ru/2019/Севмаш7/.

Partly as an alternative to the shortcomings created by this excruciatingly inefficient program, the RFN approved modernization plans to equip legacy Oscar II and Akula-class submarines with Kalibr missiles, giving them true multimission capability with high-precision weapons.[24] Work on upgrading the first Oscar II began in 2013, but delivery has been delayed until at least 2021. As Russian critics have pointed out, the upgrade may take almost twice as long as it did to build the submarine.[25] In 2017, Deputy Defense Minister Yuri Borisov noted that work on three other Oscar IIs would be complete sometime between 2018 and 2025.[26] As of 2020, none of this work is done.[27]

The RFN's plans to conduct a similar "deep" modernization of Akula-class submarines emerged after the successful Kalibr cruise missile strikes into Syria in 2015.[28] These plans represented an expansion of a "medium" upgrade program initiated in 2011 that was by all accounts already failing.[29] However, despite recent progress, as of early 2020, no Akulas have completed deep modernization, and it is not yet clear when these refurbished vessels will be accepted for deployment.[30]

These "blue water" undersea platforms constitute the naval portion of Russia's potential global conventional strike capability. However, large platform modernization across the fleet has been protracted and shows few signs of improving in the short term. Indeed, the RFN's number of large oceangoing ships and submarines will remain low through at least 2025.

Implications

At first glance, as Russian observer Alexander Mozgovoy put it in 2017, "The results of naval shipbuilding as a whole don't impress."[31] Frigate production has been woeful. Early plans to build larger ships, such as destroyers and aircraft carriers, have been shelved for the time being. Modernization of legacy platforms moves at a snail's pace. In the submarine fleet, nuclear-powered boats with a conventional precision strike or non-strategic nuclear capability are similarly slow to join the force.

[24] "Future of Russian Navy Submarine Force within State Armaments Program 2025, Part I," Navy Recognition, July 19, 2017, http://www.navyrecognition.com/index.php/focus-analysis/naval-technology/5404-future-of-russian-navy-submarine-force-within-state-armaments-program-2025-part-1.html.

[25] "Russia's Pacific Fleet to get 4 Upgraded Nuclear Subs by 2021," TASS, February 6, 2018, www.tass.com/defense/988610.

[26] "Russian Submarines to be Equipped with Kalibr Missiles by 2025," TASS, June 3, 2017, www.tass.com/defense949667.

[27] "Chelyabinsk: 13-y God v Rezerve, 6-y v Zavode," Navy Korabel, February 25, 2020, www.navy-korabel.livejournal.com/230092.

[28] "Krylatyye rakety 'Kalibr' budut ustanavlivat'na podlodki proyekta 971," RIA Novosti, March 19, 2016, https://ria.ru/20160319/1392955574.html.

[29] "Modernizirovannaya Atomnaya Podvodnaya Lodka Proyekta 971M," www.bastion-opk.ru/971m-apl/; "Russia's Modernization of Soviet-era Vessels Facing Problems, Part 1," Navy Recognition, March 3, 2018, http://www.navyrecognition.com/index.php/focus-analysis/naval-technology/6006-russia-s-modernization-of-soviet-era-vessels-facing-problems-part-1.html.

[30] Alexei Ramm, Bogdan Stepova, "'Shchuka' v tigrovoy shkure: besshumnaya podlodka vozvrashchayetsya v story," *Izvestia*, February 3, 2020, https://iz.ru/964400/aleksei-ramm-bogdan-stepovoi/shchuka-v-tigrovoi-shkure-besshumnaia-podlodka-vozvrashchaetsia-v-stroi; "Vepr Submarine of Russian Northern Fleet Successfully Completes Sea Trials," Navy Recognition, April 1, 2020, https://www.navyrecognition.com/index.php/news/defence-news/2020/april-2020/8227-vepr-submarine-of-russian-northern-fleet-successfully-completes-sea-trials.html.

[31] Alexander Mozgovoy, "Zhdet li nas novaya Tsusima?" *Nezavisimaya Gazeta*, December 22, 2017, http://nvo.ng.ru/armament/2017-12-22/1_978_cusima.html.

Observers should not allow these shortcomings to obscure that, overall, the RFN's modernization program has drastically improved its capabilities and readiness, and the Russian fleet is more robust than it has been in at least three decades. In contrast to the situation with larger, blue-water surface combatant construction, new small surface combatant construction—less complex, single-mission ships that lack blue water capability—has been relatively successful despite serious problems. Currently, these vessels, equipped with modern Kalibr missiles, can credibly mount a sustainable threat to critical infrastructure across most of the European landmass and even against portions of Alaska.

However, since 1991, Russia has produced only one large combatant ship—the *Severodvinsk*—capable of evading enemy pursuit and credibly executing a counter-critical infrastructure mission against the continental United States. But the *Severodvinsk* cannot stay on station permanently. The RFN's ability to threaten U.S. critical infrastructure with precision kinetic attacks is therefore limited to the amount of time in a year that the *Severodvinsk* can sustain a patrol within range of the United States—probably no longer than two months. Furthermore, because the order of battle is limited to one, the RFN has no extra capacity if this submarine were to be disabled or destroyed in combat. Even if the follow-on submarine *Kazan* becomes operational in 2021, the Russian navy's ability to sustain a credible conventional and tactical nuclear deterrent against the United States will remain limited. In the short term, the RFN will be able to successfully execute strategic deterrence missions from the sea against European targets but will struggle to field the sustainable global conventional capabilities to which its guiding doctrinal statements aspire.

A policy aspiration-modernization gap has opened up for the RFN. Russia is likely to attempt to close this gap in two ways. The first is its continued construction of new global power projection platforms such as modernized Yasen-M and Laika-class nuclear-powered submarines, combined with efforts to field extended-range hypersonic anti-ship and land-attack cruise missiles. Modernization of legacy platforms may be limited. In the near term (1-5 years), the RFN will muddle through in a way that allows it to provide sustained deterrence missions against regional, mainland European adversaries. However, it will struggle to develop and upgrade more complex, larger platforms that allow it to sustain such missions globally. In the longer term (5-10 years), the RFN will begin achieving a more credible and sustainable long-term conventional and tactical nuclear deterrence presence as newer large platforms and extended-range precision strike systems slowly matriculate into the force.

In response, U.S. and allied militaries can pursue damage limitation strategies that account for this shift over time. The need in Europe is most urgent. Investments in distributed logistics and infrastructure upgrades, combined with modest upgrades to air defense capabilities, can provide resiliency and redundancy while taking advantage of the fact that Russia's small ships generate small salvos of long-range precision munitions.[32] European and U.S. militaries must also become comfortable working inside Russia's vaunted, but penetrable, anti-access bubble, where these smaller single-mission platforms are likely to

[32] It should be noted, however, that counter-infrastructure missions will be carried out by Russian joint forces, including long-range precision strikes from its air force.

operate.[33] This requires continued development of decentralized command and control concepts; improved counterintelligence, surveillance, and reconnaissance capabilities; and highly dispersed, mobile operations on land and at sea. In the longer term, as Russia grows its global capability, the United States will need to invest in improved undersea warfare technology, especially wide-area sonar search capabilities that can operate in the open ocean and along the U.S. littorals. Such capabilities can include both fixed systems as well as unmanned undersea vehicles.

Russian naval modernization is neither a spectacular success nor a desperate failure. The RFN has managed to develop in ways that allow it to credibly project power into critically vital areas among its European rivals. At the same time, it is on a long-term trajectory to expand its reach against the United States.

Michael B. Petersen is the director of the Russia Maritime Studies Institute and an associate professor at the United States Naval War College.

[33] Robert Dalsjö, Christofer Berglund, Michael Jonsson, *Bursting the Bubble, Russian A2/AD in the Baltic Sea Region: Capabilities, Countermeasures, and Implications* (Stockholm: Swedish Defense Research Agency, 2019).

Russian Unmanned Vehicle Developments: Syria and Beyond

BY SAMUEL BENDETT

Introduction

The Russian military modernization drive that began in 2011 has yielded major dividends. Key to this process has been the development and use of unmanned and autonomous military systems, or as the Russian military calls them, "robotic complexes" (*robotekhnicheskie kompleksy*-RTKs). The Russian government and military are discussing the use of RTK, and their statements and deliberations paint an overall picture of how Moscow is defining the concept of operations (CONOPs) and tactics, techniques, and procedures (TTPs) with respect to unmanned systems. Some of these CONOPS and TTPs are already tested in Syria, where the Russian military operates unmanned systems since 2015.

Russian leaders, the defense industry and the Ministry of Defense (MOD) institutions tasked with conceptualizing the future of war are envisioning the ever-increasing use of unmanned systems in combat. In 2017, Russian president Vladimir Putin noted that "autonomous robotized systems . . . are capable of changing the entire system of armaments for general-purpose forces."[1] In 2019, Putin remarked that "robotized systems and drones are being introduced actively and used in combat training, which enhances the capabilities of military units by several times."[2]

In 2016, Andrei Grigoryev, head of the Russian Advanced Research Foundation (Russia's DARPA equivalent founded in 2012)[3] noted that future wars will be waged by robots and drones: "I see more and more robotization taking place. [Future] combat will be a war of operators and vehicles—the soldier will gradually turn into an operator and move away from the battlefield."[4] According to Grigoryev, the future of war belongs to unmanned systems that are multifunctional and capable of operating in

[1] "Putin shares his view on what Russian Army needs most," TASS, January 28, 2017, https://tass.com/defense/927489.

[2] Ibid.

[3] Fond perspektivnikh issledovanii (ARF) official page, https://fpi.gov.ru/.

[4] "Advanced Research Foundation believes robots will lead the future wars (Fond perspektivnikh issledovanii shchitaet, shto voyni budushevo povedut roboti)," RIA Novosti, July 6, 2016, https://ria.ru/20160706/1459555281.html.

any environment—ground, air, above and below water, and in space—integrated into a common command and control structure.[5]

Key Unmanned Systems Development Milestones to 2020

Since 2009, the Russian military has shown flexibility in the development and expansion of its nascent aerial drone force. While the USSR built and used unmanned aerial vehicles (UAVs) for ISR (intelligence, surveillance, and reconnaissance), the period between the fall of the Soviet Union in 1991 and the beginning of a drone development and acquisition drive in 2011 is indicative of Russia prioritizing other military technology developments over unmanned military systems. The result was a "robotics gap" between Moscow and leading unmanned powers like the United States and Israel. Russia began 2011 with a relatively small number of military UAVs that were mostly short-range, small ISR drones for close support missions. Its domestic defense industry responded by designing light UAVs such as the Orlan-10 and Eleron, two workhorses in the MOD arsenal.[6] Lacking domestic expertise in developing more sophisticated UAVs, Moscow reached out to Israel and by 2011 acquired kits for assembling mid-range Zastava and MALE (Medium Altitude Long Endurance) Forpost UAVs at the UZGA defense enterprise (Ural Civil Aviation Works).[7] Fast forward to 2020, and Russia's UAV development and acquisition drive possibly made Moscow the second-largest military drone user in active combat, with over 2100 drones in service.[8]

The question is often asked why Russia still lacks a fully-functioning combat UAV (UCAV), especially given that states without a long history of aircraft manufacturing—like Iran or Turkey—are already operating many combat drone models. Russian military experts explain the problem as one of priorities—combat drones were not included in the MOD's earlier planning and implementation. They also describe problems of concentration and allocation of scientific, human, and financial resources.[9] To Russian analysts and commentators, "the creation of heavy drones capable of carrying serious weapons requires a huge technological leap—a technological 'abyss' exists between a lightweight 20-pound reconnaissance UAV and a combat drone weighing more than a ton."[10]

[5] Ibid.

[6] "'Orlan,' 'Eleron,' 'Tachion'" *Krasnaya Zvezda*, August 24, 2018, http://redstar.ru/ orlan-eleron-tahion/.

[7] "Russia purchased Israeli UAVs (Rossiya kupila bespilotniki u israilya)," RussianElectronics.ru, June 22, 2009, https://russianelectronics.ru/rossiya-kupila-bespilotniki-u-izrailya/

[8] "Russian Armed Forces development: 2012-2018," *Krasnaya Zvezda*, January 9, 2019, http://redstar.ru/vooru- zhy-onnye-sily-rf-razvitie-s-2012-po-2018-god/; Aleksandr Aleksandrov, "At the heart of state security (v osnovye bezopas-nost strani)," *Krasnaya Zvezda*, May 14, 2017, http://archive.redstar.ru/index.php/component/k2/ item/33144-v-os-nove-bezopasnosti-strany; Note: The United Statesis operating over 10,000 UAVs, see https://en.wiki- pedia.org/wiki/UAVs_in_the_U.S._military; Israeli UAVs active service, see https://www.jpost.com/Israel-News/How-Is- rael-be-came-a-leader-in-drone-technology-595209; China may operate more UAVs than Russia, yet it has a limited number in active combat with its allies, see https://taskandpurpose.com/news/china-drone-superower.

[9] Anton Lavrov, "Unmanned Race (Bespilotnaya gonka)," *Izvestia*, August 25, 2017, https://iz.ru/627546/anton-lavrov/rossiia-proigryvaet-bespilotnuiu-gonku.

[10] Ibid.

Source: Mike1979 Russia/WikiCommons (CC BY-SA 3.0)

Orlan-10 UAV

For the past twenty years, the Russian defense industry also lacked key expertise in developing modern UAV engines with a long resource life, a problem that persists today.[11] For example, the MOD did in fact task Russian developers with creating a long-range UAV—one project to build a high-altitude drone, "Altair/Altius," was undertaken in 2011 by the Simonov Design Bureau. As the work progressed, the bureau faced a number of difficulties, notably the absence of domestic UAV expertise, which Simonov thought could be contracted out once it had the funding. This lack of expertise led to cost delays and financial and delivery problems that threatened the implementation of the entire project.[12] As a result, the MOD intervened in 2017 and then in 2018, and the project was ultimately transferred to the UZGA, the only Russian defense company with experience building large UAVs that are operational today.[13]

When it comes to Russian unmanned ground vehicle (UGV) projects, many were self-initiated by the country's defense-industrial sector due to the lack of a comprehensive MOD RTK roadmap. In 2017, the MOD launched an annual initiative called "Robotization of the Armed Forces of Russia" in order to consolidate unmanned systems production and acquisition by developing common requirements and standards.[14] Today, the MOD robotization roadmap exists to guide the industry and military in developing, testing, and acquiring RTKs.[15] Despite the earlier lack of MOD attention, the domestic industry's accomplishments include the development of the demining Uran 6, Scarab, and Sphera platforms. Today, combat UGVs undergoing MOD testing and evaluation include the Platforma-M, Nerehta, Soratnik, Uran-9, Vihr, Marker, Kungas, and Shturm medium and heavy vehicles, to name a few.
At sea, Russia is looking to field unmanned underwater and surface vehicles (UUVs/USVs)

[11] Ibid.

[12] Mikhail Hodarenok, "Just a few more years: why Russian drones lag behind (Eshye neskolko let: pochemu otstaiyut rossiskiye droni)," Gazeta.ru, December 22, 2019, https://www.gazeta.ru/army/2019/12/22/12878396.shtml.

[13] Ibid.

[14] "II-ya Voenno-Nauchnaya Konferenciya I Vystavochnaya ekspozitsiya "Robotizatsiya Voorujonnyx Sil Rossiyskoy Federatsii," Patriot Ekspo, March 23, 2017, http://www.patriot-expo.ru/robotics/.

[15] "The target program for the creation of military robots adopted in Russia (Tselevaya programma po sozdanniyu voennikh robotov prinyata v Rossii)," RIA Novosti, December 4, 2014, https://ria.ru/20141204/1036508024.html.

that will give Russian vessels greater ISR range and capability, along with anti-submarine warfare, maritime border protection, demining, and even combat characteristics.[16] Rear Admiral Vladimir Tryapichnikov said in 2018 that the Russian navy will emphasize the development of unmanned technologies.[17] Just like with UAVs, the Russian navy managed to import Western equipment since 2008, as it began to explore the role of unmanned vehicles. Today, the MOD emphasizes domestic production in the government's import substitution drive as a response to Western sanctions. The navy also has potential plans to equip Russian ships with surface and subsurface unmanned complements, making each vessel a carrier and user of unmanned technology.[18]

Syria as Russia's Unmanned Military Lab

Since the start of the 2015 Russian intervention in Syria, the MOD has steadily increased its use of unmanned systems to assist its forces. The biggest emphasis has been on the use of unmanned aerial vehicles. Defense Minister Sergey Shoigu remarked in October 2017 that Russian UAVs were carrying out 24/7 monitoring and surveillance over Syria while conducting 16,000 missions—a 2.5-fold increase in comparison with 2015, with a total of 96,000 flight hours.[19] By July 2018, the number of UAV flight missions had climbed to over 23,000, with 140,000 flight hours.[20] Chief of the General Staff General Valery Gerasimov noted in late 2017 that Russian forces operated 60–70 UAVs on a daily basis, a major progress in drone use since 2012.[21] General Gerasimov elaborated that today's combat is "unthinkable without drones—they are used by gunners, scouts, pilots—everyone."[22]

Today's Russian UAV missions in Syria include aerial reconnaissance, providing target designation, controlling airstrikes, and adjusting artillery fire. UAVs are now a key part of what the MOD calls the reconnaissance fire and strike contours.[23] The reconnaissance-strike contour (RSC) was designed for the coordinated employment of high-precision, long-range weapons linked to real-time intelligence data and precise targeting provided to a command and control center.[24] The RSC was designed to function at operational depths

[16] Samuel Bendett, *The Rise of Russia's Hi-Tech Military* (Fletcher Security Review) (Medford, MA: Fletcher School at Tufts University, 2019), https://sites.tufts.edu/fletcherrussia/files/2019/06/The-Rise-of-Russia%E2%80%99s-Hi-Tech-Military-Samuel-Bendett.pdf.

[17] "Russian Navy to focus on unmanned warships," TASS, August 24, 2018, https://tass.com/defense/1018526.

[18] "7th Project 12700 trawler will be laid in St Petersburg in July (Sedmoy tralshchik proyekta 12700 zalozhat v Peterburgye v yulie)," TASS, April 10, 2019, https://tass.ru/ekonomika/6318333.

[19] "Russian drones conduct round-the-clock control in Syria, said Shoigu (Rossiiskie bespilotnikivedut kruglostochniy kontrol v Sirii, zayavil Shoigu)," RIA Novosti, October 27, 2017, https://ria. ru/20171027/1507669571.html.

[20] "Russian drones during the operation in Syria spent in the air more than 140 thousand hours (Rossiiskie bespilotniki vo vremya operatsii v Sirii proveli v vozdukhe boley 140 tisych' chasov)," Official website of the Russian MOD, July 6, 2018, http://syria.mil.ru/news/more.htm?id=12184627@egNews.

[21] "Chief of the General Staff of the Armed Forces of Russia Army General Valery Gerasimov: 'We have broken the spine of the shock forces of terrorism' (Nachalnik Genshtaba Vooruzhenikh sil' Rossii general armii Valeriy Gerasimov: «Mi perelomili khrebet udarnim silam terrorizma»)," *Komsomol'skaya Pravda*, December 26, 2017, https://www.kp.ru/daily/26775/3808693

[22] Ibid.

[23] Lester W. Grau and Charles K. Bartles, "The Russian Reconnaissance Fire Complex Comes of Age," Changing Character of War Centre, May 2018, http://www.ccw.ox.ac.uk/blog/2018/5/30/the-russian-reconnaissance-fire-complex-comes-of-age

[24] Ibid.

using surface-to-surface missile systems and aircraft-delivered “smart” munitions.[25] The reconnaissance-fire contour is the tactical equivalent that links intelligence data, precise targeting, a fire-direction center, and tactical artillery to destroy high-value targets in near real-time.[26] The MOD specifically noted that the use of UAVs together with aviation increased its ability to strike targets.[27]

Using UAVs in the complex Syrian environment came with many challenges, such as the dynamically changing ground conditions, the enemy’s use of persistent counter-UAV capabilities, as well as the need to share airspace with manned aircraft belonging to multiple combatants.[28] It should be also noted that Russia still relied on manned aviation in concert with UAVs, potentially putting pilots in danger of adversary anti-aircraft efforts. Russian forces in Syria also use UAVs for search and rescue, as well as electronic warfare and information warfare.[29]

When it comes to UGV use and testing in Syria, the Uran-6, Scarab, and Sphera demining vehicles were rated highly by Russian engineering forces, and the MOD plans to start acquisition of these vehicles.[30] However, these UGVs were designed to have the operator in close proximity. The situation surrounding vehicles built for operator remoteness in combat has proven more complicated. Russia’s Uran-9 combat UGV experienced several failures when tested in “near-combat conditions” in Syria—among them transportation, communication, firing, and issues with the operator’s situational awareness.[31] Russia also managed to test a UUV in Syria—in February 2018, the Russian Military-Industrial Commission announced that “Galtel” underwater “robotic complex” was tested.[32] The Galtel was engaged in the search for undersea unexploded ordnance and conducted sea-floor mapping and protection of the Tartus port area, where Russia has a naval base.[33]

[25] Ibid.

[26] Ibid.

[27] O. V. Milenin and A. A. Sinnikov, “O roli aviatsii vozdushno-kosmicheskikh sil v sovremennoi voine. Bespilotnye letatel’nye apparaty kak tendentsiia razvitiia voennoi aviatsii,” *Voennaia mysl’*, no.11 (November 2019): 50-57, https://dlib.eastview.com/browse/doc/55953437.

[28] Ibid.

[29] Ibid.

[30] Kelsey Atherton, “Russia orders a dozen new demining robots,” C4ISRNET, February 4, 2019, https://www.c4isrnet.com/unmanned/2019/02/04/russia-orders-a-dozen-new-demining-robots/.

[31] “Problematic issues of the development of military robotic systems (Problemniy voprosi razvitiya robototekhnicheskikh kompleksov voyennovo naznacheniya),” BMPD (blog), June 16, 2018, https://bmpd.livejournal. com/3239351.html; “‘Maddest’ Guest Blogger!” Mad Scientist Laboratory, September 10, 2018, https://madsciblog. tradoc.army.mil/tag/sam-bendett/.

[32] “Podvodniy robot «Galtel’» uspeshno vipolnil boevuyu zadachu v Sirii - chlen kollegii VPK,” Interfax-AVN, February 22, 2018, http://www.militarynews.ru/story.asp?rid=1&nid=474342.

[33] “Rossiiskii podvodniy robot vipolnil boevuyu zadachu v Sirii,” Rg.ru, February 22, 2018, https://rg. ru/2018/02/22/rossijskij-podvodnyj-robot-vypolnil-boevuiu-zadachu-v-sirii.html.

Source: Vitaly V. Kuzmin/WikiCommons (CC BY-SA 4.0)

Uran-9 unmanned combat ground vehicle

MOD Plans for Military Unmanned Systems

The Syrian experience has resulted in concrete MOD plans for the development of unmanned platforms and the conceptualization of how its forces will use such systems. First, the use of multiple ISR UAVs as part of the reconnaissance strike and reconnaissance fire contours convinced the MOD that it also needs unmanned aerial combat capabilities. These operational plans are no doubt influenced by the decades-long use of combat UAVs by the United States and Israel, as well as by relatively new users like Turkey.[34] This year and for the next several years, Russia will conduct testing and evaluation of an entire lineup of different classes of combat drones that have been in development from as early as 2010. They include the heavy Okhotnik combat UAV (UCAV); the mid-range Orion that was tested in Syria; the Forpost-R, a fully "Russian" drone made with domestic components that was originally assembled via Israeli license; the mid-range Korsar; the mid-range Orlan-30, an upgrade to the Orlan-10 workhorse; and the long-range Altius, to name a few.[35]

Some of these UAVs are several years away from potential acquisition by the armed forces, while others are graduating to final military testing and evaluation. The MOD has indicated that the Forpost-R and Orlan-30 could enter service in 2020.[36] In April 2020, MOD took

[34] Dylan Nicholson, "'Revolutionary' warfare or good marketing: Turkey's Syria drone strikes," *Defence Connect*, March 9, 2020, https://www.defenceconnect.com.au/strike-air-combat/5709-revolutionary-warfare-or-good-marketing-turkey-s-syria-drone-strikes.

[35] Samuel Bendett, "The Rise of Russia's Hi-Tech Military," *Fletcher Security Review* 6, no. 1 (Summer 2019), https://sites.tufts.edu/fletcherrussia/files/2019/06/The-Rise-of-Russia%E2%80%99s-Hi-Tech-Military-Samuel-Bendett.pdf.

[36] "Russian army to get Orlan-30 drone in 2020," *Army Recognition*, October 3, 2019, https://www.armyrecognition.com/weapons_defence_industry_military_technology_uk/russian_army_to_get_orlan-30_drone_in_2020.html; "The Ministry of Defense will receive ten new Forpost-R drones (Minoboroni poluchit desyat' novikh bespilotnikov "Forpost-R")," RIA Novosti, March 3, 2020, https://ria.ru/20200205/1564280927.html.

delivery of its first Orion UAVs, in order to conduct more testing and evaluation based on its recent Syria experience. The deployment of aerial combat drones in the long term will allow for the eventual retiring of outdated reconnaissance aircraft.[37] The MOD has also encouraged domestic industry to start developing a UAV swarm that could perform independent combat operations by penetrating enemy space and striking targets.[38]

Second, the Syrian UAV experience is resulting in structural change across the Ministry of Defense. The MOD currently organizes its drone fleet by companies that are divided into platoons based on the size and range of the UAVs they operate to more easily facilitate command and control as well as maintenance.[39] For example, some UAVs like the Orlan-10 will become part of Russian artillery brigades and artillery regiments.[40] Presently, there are 40 UAV companies and units formed across the country.[41] UAVs are incorporated into the Navy as ISR assets based on shore and on ships—every major Russian fleet now has units with Forpost and Orlan-10 drones.[42]

ISR UAVs are used regularly in military drills and exercises for aerial reconnaissance and intelligence gathering, as well as for electronic warfare and artillery fire correction.[43] They are also becoming an official part of motorized, artillery, infantry, and other units across the armed services.[44] Moreover, the MOD has found a new "home" for the UAVs: the General Staff's Directorate of UAV Construction and Development was transferred to the Air and Space Forces (*Voenno-kosmicheskie Sily*, VKS).[45] As the leading force in Syria, the VKS gained invaluable experience with manned and unmanned aviation that will now be officially codified across the MOD.

Third, the Russian military gained valuable lessons with UGV use in combat. The MOD has determined that for the next 10-15 years, unmanned ground military systems are not capable of fulfilling their assigned tasks in classical types of military operations—that is as part of the combat formations of combined arms units.[46] The Russian military will thus need to work through new concepts and tactics for using such combat robotics. Moreover, one-time and preferably stationary use of these UGVs would be more effective, using such unmanned platforms as "one-off" attack vehicles against adversary hard points and stationary targets, with maintenance and repair crews close by.[47]

[37] Ibid.

[38]"Within five years, a swarm of drones capable of independent solutions will be created in the Russian Federation (V RF v techeniye pyati let sozdadut "roy" bespilotnikov, sposobnikh k samostoyatel'nim resheniyam)," TASS, Septem- ber 28, 2017, https://tass.ru/armiya-i-opk/4592500.

[39] Ibid.; Grau and Bartles, "The Russian Reconnaissance Fire Complex."

[40] Ibid.

[41] "Russian Armed Forces development," RedStar.ru.

[42] "Russian naval aviation armed with drones," Navy Recognition, July 10, 2019, https://www.navyrecognition.com/index.php/focus-analysis/naval-technology/7274-russian-naval-aviation-armed-with-drones-part-1.html.

[43]"Voyennosluzhashchiye gornovo soyedineniye poluchili bolee 10 kompleksov s BLA," Official Ministry Of Defense web- site, January 2, 2019, https://function.mil.ru/news_page/country/more.htm?id=12210722@egNews.

[44] Ibid.

[45] "VKS will be involved in the development of drones for all military branches (Istochnik: VKS zaiymutsya razvitiyem bespilotnikov dlya vsekh rodov voysk)," Voennoe.rf, February 21, 2020, https://xn--b1aga5aadd.xn--p1ai/2020/%D0%91%D0%BF%D0%BB%D0%B02/.

[46] "Problematic issues," BMPD (blog).

[47] Ibid.

These and similar combat UGVs should be used with other military formations and "never on their own" because their breakdown would negatively impact the military mission.[48] Russian military officers and academics are conceptualizing that UGVs will face other UGVs in future combat because the "value of the robot is to replace a person and exceed soldier's capabilities."[49] Such deliberations point to the idea of an RTK as an expendable item on the battlefield, as well as a key transportation and logistical asset for the soldiers.[50]

To test out such concepts and theories, the MOD is supporting several flagship projects.[51] One key concept is the "Maker," which is in testing with the Advanced Research Foundation. The Maker serves as a test-bed for the development of "robotic combat-ready formations" or vehicle teams and swarms made up of ground and aerial vehicles as well as unmanned logistical and fuel systems.[52] This year, the MOD also announced that it will develop UGVs based on the Soratnik and Shturm concepts by taking over the vehicle development initiative from private enterprises as it begins to formulate a UGV concept of operations.[53] The Russian military is also developing Syria-based tactics and procedures for using RTKs in urban and coastal combat.[54]

Fourth, the Russian Navy's ongoing research and development points to ISR and situational awareness as the key criteria for unmanned maritime use. Syrian UAV workhorses like the Forpost have been tested as guidance mechanisms for the Kalibr cruise missiles and Yakhont anti-ship missiles.[55] Another workhorse—the Orlan-10 UAV—was tested as a ship-based ISR asset on frigates operating in the Mediterranean.[56] Development of UUVs as long-range ISR and combat assets is underway as well. Systems include the Klavesin, which can operate at up to 6000 meters below the surface;[57] the Surrogat, which can mimic a submarine signature;[58] and an anti-submarine UUV called "Cephalopod" that carries small torpedoes.[59]

[48] Ibid.

[49] "Teams of military robots will be created in Russia (V Rossii Sobralis' sozdat gruppirovki boyevikh robotov)," Vz.ru, November 23, 2019, https://vz.ru/news/2019/11/23/1009943.html.

[50] Aleksei Zakvasin and Elizaveta Komarova, "'In the line of fire': what tasks are assigned to combat robots of the Russian army («Na Linii ognya»: kakiye zadachi vozlozheni na boyevikh robotov rossiiskoy armii)," RT, November 28, 2019, https://russian.rt.com/russia/article/691199-kungas-boevye-roboty-minoborony.

[51] Dmitry Yurov, "Robots, lasers and other military 'gadgets' (Roboti, lazeri i drugiye «gadzheti» voyennovo naznacheniye)," Zvezdaweekly.ru, December 2, 2019, https://zvezdaweekly.ru/news/t/201911261055-EOcml.html.

[52] Ibid.

[53] "Commander of the Ground Forces spoke about the development of two combat robots (Glavkom Sukhoputnikh voysk rasskazal o razrabotkye dvukh boyevikh robotov)," RIA Novosti, December 24, 2019, https://ria.ru/20191224/1562799550.html.

[54] "Russia is developing concept for using robots in urban combat (Istochnik: v RF razrobatotaiyut taktiku primeneniye robotov v ulichnikh boyakh)," Ria.ru, November 24, 2019, https://ria.ru/20191124/1561522690.html.

[55] "Russian Navy to Use UAV for Cruise and Anti-ship Missile Targeting," Navy Recognition, August 21, 2018, https://www.navyrecognition.com/index.php/news/defence-news/2018/august-2018-navy-naval-defense-news/6439-russian-navy-to-use-uav-for-cruise-and-anti-ship-missile-targeting.html.

[56] Anton Valagin, "Video: Russian military is learning how to capture a UAV with a net (Video: rossiiskiye voyenniy nauchilis' lovit bespilotniki setyami)," Rg.ru, April 28, 2019, https://rg.ru/2019/04/28/reg-szfo/video-rossijskie-voennye-nauchilis-lovit-bespilotniki-setiami.html.

[57] Anna Yudina, "Gid po samim sekretnim podvodnim robotam Rossii," TASS, July 26, 2018, https://tass.ru/armiya-i-opk/5402375.

[58] Ibid.

[59] Kyle Mizokami, "Russia Working on New 'Cephalopod' Underwater Attack Drone," *Popular Mechanics*, July 30, 2018,

Finally, the MOD is considering a gradual shift from manual control over unmanned systems to a fully autonomous model, perhaps powered by limited AI (artificial intelligence) for better situational awareness in a fast-paced and fast-changing combat environment.[60] This goal remains aspirational as the current technology does not allow for this level of independence for unmanned vehicles. Thinking through future combat scenarios influenced by the Syrian experience, the MOD is proposing that AI should direct swarms of air, land, and sea-based unmanned and autonomous systems.[61] To get to the right solutions, the MOD has opened centers and institutions tasked with AI development and testing. They include the Advanced Research Foundation, where AI and swarming technologies are being developed, and the recently-launched ERA Technopolis.[62] As the Russian military is working to conceptualize AI use in its various weapons systems, its official position with respect to greater RTK autonomy is a "human-in-the-loop" approach (i.e., an operator who can make the key decisions with respect to using weapons on a drone).[63]

Conclusion

The Russian Federation has made major strides over the past decade in becoming one of the most active users and developers of unmanned military systems. Its involvement in Syria has been the single most defining experience for the MOD over the past 20 years. Its testing and use of RTKs are beginning to redefine how the Russian military fights today and tomorrow. Going forward, there are also significant challenges that will have to be overcome by the MOD. These include building up domestic drone development expertise; creating common RTK training, evaluation, and development standards; as well as building out combat logistics plans and scenarios such as RTK repair, resupply, and recovery. Finally, RTK costs will have to be balanced out along with costs for the development and acquisition of other military technologies. The domestic defense-industrial base's capacity to manufacture needed components also deserves attention as part of the import substitution drive that began in 2014.

The Russian MOD is working with multiple RTK projects. Some have seen active combat, others are starting to enter service, while others are years away as they undergo careful evaluation. Russia is determined to be one of the major trendsetting states that combines RTKs with other forces in current and future wars. This determination adds to the challenge that the United States and its allies in the North Atlantic Treaty

https://www.popularmechanics.com/military/navy-ships/a22593766/russia-working-on-new-cephalopod-underwater-attack-drone/.

[60] "In the future, Russian combat robots will be able to recognize and hit targets on their own (Rossiiskiye boyeviy roboti v budushem smogut sami raspoznavat i porazhat tseli)," TASS, February 5, 2019, https://tass.ru/armiya-i-opk/6081210.

[61] O. V. Milenin, A. A. Sinnikov, "O roli aviatsii vozdushno-kosmicheskikh sil v sovremennoi voine," 50-57.

[62] "Marker," Fond perspektvinyh issledovaniy, https://fpi.gov.ru/projects/fiziko-tekhnicheskie-issledovaniya/marker/; Fond perspektivnyh issledoviniy (2019, February 6). *Eksperimental'naya platforma "Marker"* [Video], Youtube, https://www.youtube.com/watch?v=HfYuDHphx1M&feature=emb_title; Kelsey D. Atherton, "Russian system uses infantry to spot for robots," C4ISRNET, March 3, 2019, https://www.c4isrnet.com/unmanned/2019/03/04/russias-new-robot-is-a-combat-platform-with-drone-scouts/.

[63] Russian Federation, "Examination of various dimensions of emerging technologies in the area of lethal autonomous weapons systems, in the context of the objectives and purposes of the Convention," CCW Group of Governmental Experts, November 10, 2017, https://admin.govexec.com/media/russia.pdf.

Organization (NATO) are already facing in trying to counter the effects of unmanned systems use among adversaries such as China and Iran. The United States needs to track the evolution of RTK development in Russia and other great powers because active unmanned and autonomous vehicle use by these countries is already redefining how modern combat is waged.

Samuel Bendett is an adviser with the CNA Russia Studies Program and an adjunct senior fellow with the Center for a New American Security.

About the Editor and Authors

Jeffrey Mankoff is senior fellow with the CSIS Russia and Eurasia Program. His areas of expertise include international security, Russian foreign policy, regional security in the Caucasus and Central Asia, ethnic conflict, and energy security. Before coming to CSIS, he served as an adviser on U.S.-Russia relations at the U.S. Department of State as a Council on Foreign Relations International Affairs Fellow. From 2008 to 2010, he was associate director of International Security Studies at Yale University and an adjunct fellow at the Council on Foreign Relations. He is the author of *Russian Foreign Policy: The Return of Great Power Politics* (Rowman & Littlefield, 2011). His forthcoming book, *Empires of Eurasia: How Imperial Legacies Shape International Security* (Yale, 2020), examines the impact of the imperial past on Chinese, Iranian, Russian, and Turkish politics and foreign policy.

Dr. Mankoff has also taught courses on international security, Russia, and Central Asia at Columbia, George Washington, Georgetown, and Yale Universities, and held academic fellowships at Harvard, Moscow State, and Yale. He holds dual BAs in international studies and Russian from the University of Oklahoma and an MA, MPhil, and PhD in diplomatic history from Yale.

***

Samuel Bendett is an adviser with CNA's Adversary Analysis Group, where he is a member of the Russia Studies Program. He is a member of CNA's Center for Autonomy and Artificial Intelligence. He is also an adjunct senior fellow at the Center for a New American Security. His work involves research on the Russian defense and technology developments, such as unmanned military systems and artificial intelligence. Samuel holds a master's degree in security studies from Tufts University's Fletcher School of Law and Diplomacy.

Dr. Stephen J. Blank is senior fellow at FPRI's Eurasia Program. He has published over 900 articles and monographs on Soviet/Russian, U.S., Asian, and European military and foreign policies, testified frequently before Congress on Russia, China, and Central Asia, consulted for the Central Intelligence Agency, major think tanks and foundations, chaired major international conferences in the United States and in Florence; Prague; and London, and has been a commentator on foreign affairs in the media in the United States and abroad. He has also advised major corporations on investing in Russia and is a consultant for the Gerson Lehrmann Group. He has published or edited 15 books, most recently *Russo-Chinese Energy Relations: Politics in Command* (London: Global Markets Briefing, 2006).

Joe Cheravitch has worked as an analyst focusing on international cyberwarfare and influence operations since 2014. Cheravitch previously served in the U.S. Army as a psychological operations specialist, deploying to Afghanistan in 2010 and Iraq a year later. He holds a master's degree from Georgetown University's Edmund A. Walsh School of Foreign Service.

Michael B. Petersen is the director of the Russia Maritime Studies Institute and an associate professor at the United States Naval War College. His current work focuses on high-technology joint warfare. Previously, he worked in the Defense Intelligence Agency and on the National Security Council. He holds a PhD from the University of Maryland, College Park, and has published books, articles, and essays on joint warfare, military intelligence, and strategic weapons history.

Andreas Turunen is a research analyst at CSRC specializing in strategic analysis of Russian defense and contemporary security issues. His main skills and areas of responsibility are open-source analytics, hybrid warfare, and interpretation of phenomena associated with Russia's strategic framework. In addition to his work with CSRC, Andreas has given expert commentary for the media on topics related to Russian security and he lectures about the topics of his expertise. He is also a Springer author (cyber power) on information warfare network theory.

COVER PHOTO MLADEN ANTONOV/AFP VIA GETTY IMAGES

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**