Research Report

CLINT REACH, ALYSSA DEMUS, MICHELLE GRISÉ, KHRYSTYNA HOLYNSKA, CHRISTOPHER LYNCH, DARA MASSICOT, DAVID WOODWORTH

Russia's Evolution Toward a Unified Strategic Operation

The Influence of Geography and Conventional Capacity

For more information on this publication, visit **www.rand.org/t/RRA1233-8**.

Published by the RAND Corporation, Santa Monica, Calif.

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-1-9774-0935-5

About This Report

Russian planning for regional and large-scale war is trending toward a so-called unified strategic operation. This notional concept is an organizing construct for a future Russian force structure with increasing conventional capacity to engage critical targets at the regional and global levels. It includes a nonnuclear and nuclear component and involves the coordinated action of multiple joint strategic commands. The conventional tasks within a unified strategic operation likely are oriented toward the destruction (degradation) of the North Atlantic Treaty Organization (NATO) aerospace system and civilian infrastructure to terminate the conflict prior to nuclear escalation. The offensive tasks could include the following:

- strikes against NATO sea-launched cruise missile platforms
- suppression and destruction of NATO orbital satellites
- air and ground missile strikes against NATO air and missile defense and command and control systems
- disorganization of NATO command, control, communications, computers, intelligence, surveillance, and reconnaissance through the use of electronic warfare systems
- destruction or disruption of critically important NATO infrastructure through the use of air-launched cruise missiles, long-range aviation, frontal aviation, ground-based missile systems, and cyber weapons.

In this report, we examine why Russia is evolving toward a unified strategic operation and the capabilities related to the execution of these tasks. The primary research for this report was completed in January 2022, before Russia's invasion of Ukraine in February 2022. The few references to the war in Ukraine were added prior to publication.

The research reported here was completed in March 2022 and underwent security review with the sponsor and the Defense Office of Prepublication and Security Review before public release.

RAND National Security Research Division

This research was sponsored by the Russia Strategic Initiative, U.S. European Command, and conducted within the International Security and Defense Policy Center of the RAND National Security Research Division (NSRD), which operates the National Defense Research Institute (NDRI), a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise.

For more information on the RAND International Security and Defense Policy Center, see www.rand.org/nsrd/isdp or contact the director (contact information is provided on the webpage).

Acknowledgments

We are indebted to Mike Albertson and James Black for their constructive reviews that greatly improved the report.

Summary

Background and Purpose of This Report

Recent evidence suggests that Russian operational concept development is trending toward a *unified strategic operation*.[1] This future concept is intended to more effectively organize and allocate Russia's conventional strike and nonkinetic attack capacity as it increases over time. To understand why this trend is occurring, we examined the following questions:

- What are the key military problems that have influenced Russian operational concept development since the late Cold War?
- What is the unified strategic operation, and how does it fit in with this history?
- What are the key military tasks that are likely associated with this operation, and how is Russia developing its forces to carry out these tasks?

Findings

The Military Problem and Solutions

During the Cold War, the primary military challenge for the Soviets was rapidly defeating an economically, technologically, and demographically superior alliance that possessed nuclear weapons and a large amount of strategic depth. By the 1970s, the Soviet military leadership concluded that leading with nuclear weapons against a nuclear peer was a dubious approach to achieve desired political ends.[2] They arrived at deep ground operations to quickly sever the ability of the North Atlantic Treaty Organization (NATO) to escalate with theater nuclear weapons. The prevailing principle for the Soviets was that overwhelming mass and closure speed into the depths of the adversary were essential to the success of the rapid offensive.

The military problem and leading principles remain the same today for the Russian military. Russian operational thinking continues to emphasize that offensive actions must be conducted rapidly and throughout the entire depth of NATO to overwhelm its ability or willingness to continue the war. The critical question for Russian strategists over the past 30 years has centered on the means with which to conduct such actions in a theater that has grown increasingly disadvantageous for Russian operations. Notably, as NATO depth was expanding in the 2000s,

[1] The primary research for this report was completed in January 2022, before Russia's invasion of Ukraine in February 2022. The few references to the war in Ukraine were added prior to publication.

[2] Clint Reach, Alexis A. Blanc, and Edward Geist, *Russian Military Strategy: Organizing Operations for the Initial Period of War*, Santa Monica, Calif.: RAND Corporation, RR-A1233-1, 2022; L. I. Voloshin, "Teoriia glubokoi operatsii i tendentsii ee razvititiia," *Voennaia mysl'*, No. 8, 1978, p. 25.

Russia decreased its land forces to approximately 300,000 personnel.[3] The lack of large numbers of ready land forces relative to the size of the military theater has forced Russian operational planners to embrace a strike-centric approach to regional deterrence and warfighting.

However, Russia's lack of conventional strike capacity reduces flexibility in planning. For the first two decades of the post-Soviet era, the state of the Russian economy and armed forces dictated an approach that was reliant upon nuclear deterrence and retaliation. In the early 2010s, a prominent idea was to use Russia's limited conventional long-range strike assets to target energy and electricity supplies and other critical infrastructure—that is, a *countervalue campaign*, in modern Russian parlance. At that time, nonstrategic nuclear weapons were still the leading edge of a "counterforce" campaign to destroy NATO military infrastructure related to the aerospace attack deep into Russia. Despite the modernization of the armed forces since 2011, Russia's nonstrategic nuclear weapons remain the primary instrument of regional deterrence. Leading Russian military experts consider long-range conventional strike assets auxiliary tools in regional and large-scale war scenarios.[4]

This is not the desired end state for Russia's strategy to counter NATO. Employing nuclear weapons against a nuclear peer remains a dubious approach to achieving political ends through military force, thereby undermining Russian deterrence. Russia eventually wants to build sufficient conventional offensive capacity to conduct deep conventional strikes and electronic attacks to neutralize NATO's conduct of noncontact warfare and to make the war untenable through the destruction of military-industrial and other civilian infrastructure. The operational challenge for Russia is how to best coordinate dual-use and other assets from across all of Russia's military districts to engage regional and global targets.

The Unified Strategic Operation

Looking ahead to the 2030s and beyond, the notional unified strategic operation concept is designed to coordinate Russia's increasing nonnuclear strike and electronic attack assets to engage NATO targets at the regional and global levels while retaining sufficient capacity to escalate to nuclear use. This single concept would merge two developing operations—the general-purpose forces operation (GPFO) and the strategic deterrence forces operation (SDFO). The GPFO likely is intended to isolate a conflict at the local level with exclusively conventional weapons, deterring external intervention through the threat of long-range precision strike and nonstrategic nuclear weapons against military targets and civilian infrastructure—that is, something akin to the ongoing Russian invasion of Ukraine, which has been ground-centric and in which long-range precision munitions did not play a leading role in the initial period of war.

---

[3] Viktor Khudoleev, "Voiska s velikoi istoriei," *Krasnaya Zvezda*, 2015.

[4] A. A. Protasov, S. V. Kreidin, and Iu. A. Kublo, "Aktual'nye aspekty razvitiia silovykh instrumentov i kontseptsii strategicheskogo sderzhivaniia," *Vestnik Akademii voennykh nauk*, Vol. 3, No. 76, 2021, pp. 44–45.

Russian formations equipped with missiles with ranges of more than 500 km make up Russia's strategic deterrence forces.[5] The SDFO, therefore, is tailored to inflict increasing levels of nuclear and conventional damage against critical NATO targets in a regional or large-scale war.[6] It is defined as

> a prospective type of strategic action of the Armed Forces using strategic strike weapons with conventional payloads, as well as a strictly limited number of strategic nuclear strikes to inflict unacceptable damage on the aggressor and deter him from dangerous actions. It can be carried out by a small force to prevent and disrupt an imminent attack in the form of a demonstration of military power or with full-scale use of all means in the event of aggression. [SDFO] is being developed along the lines of the strategic operation of nuclear forces [SONF], but in other forms as appropriate means of combat are created. In the future, this operation could use both nuclear weapons with limited fall-out and conventional high-precision weapons on various platforms, as well as strategic reconnaissance-strike systems.[7]

Senior Russian officers and analysts have suggested that the SDFO relies primarily on nuclear weapons, whose role will decline over the next two decades as more long-range conventional weapon systems enter service.[8] In our view, the SDFO is the medium-term Russian solution to the conduct of regional war and the requirement that offensive actions must be conducted rapidly and throughout the entire depth of NATO to overwhelm its ability to continue the war.

As a merger of the two concepts, the unified strategic operation would not require a strict delineation of assets and tasks between local and regional war. Prior to the Syria conflict, the Russians apparently were thinking either about a local war along the periphery that did not involve the employment of long-range precision munitions or about a regional war in which nonstrategic nuclear weapons were the primary means to repel a NATO aerospace attack. The expected increase in conventional strike capacity is creating a new environment for Russian operational planning that must account for how to allocate and employ these and other weapons in an increasing number of conflict scenarios.

Key Military Tasks and Associated Capability Development

The key military tasks of the unified strategic operation are all related to engaging targets beyond the range of Russian ground forces and artillery. These tasks are long-range conventional

---

[5] Russia's strategic deterrence forces also include national air and missile defense assets, which we have examined in other studies but were beyond the scope of this report. See Ministry of Defense of the Russian Federation, "Strategicheskie sily sderzhivaniia," Voenno-entsiklopedicheskii slovar', Ministerstvo oborony RF, undated.

[6] Russia consolidated its strategic operation to destroy critically important targets with its strategic operation of nuclear forces. The new operation is alternatively referred to as the *strategic deterrence forces operation (SDFO*) and the *strategic offensive forces operation*.

[7] D. O. Rogozin, ed., *Voina i mir v terminakh i opredeleniiakh*, Moscow: Veche, 2017, p. 155.

[8] A. E. Sterlin, A. A. Protasov, and S. V. Kreidin, "Sovremennye transformatsii kontseptsii i silovykh instrumentov strategicheskogo sderzhivaniia," *Voennaia mysl'*, Vol. 8, 2019.

strikes against critical military and civilian targets; electronic warfare (EW) to disrupt command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR); counterspace actions; and cyberattacks against critical infrastructure.[9] In Chapters 3 through 6 of this report, we examine Russia's capability development in each of these task areas. Chapter 3 details Russia's likely capacity constraints in long-range munitions and platforms. The analysis shows why leading Russian military experts are skeptical of Russia's ability to conduct conventional theater strikes for a sustained period and why they continue to emphasize the role of nonstrategic nuclear weapons at the regional level. Chapters 4 and 5 identify Russian strengths and weaknesses in EW and counterspace. While Russia likely has some ability to disrupt NATO C4ISR at the regional level, our preliminary investigation raises questions about the extent to which Russia could generate sufficient EW and counterspace effects to compensate for platform and munitions limitations in long-range theater strike. On Russian cyber weapons (discussed in Chapter 6), real-world evidence suggests that there could be a consequential threat to critical civilian infrastructure in both Europe and the United States in the event of a crisis or conflict. Understanding lasting effects (impacts) of such attacks on both warfighting and societies requires further study.

[9] Russia's ground forces, in addition to participating in the execution of several such tasks, could seize and hold territory commensurate with their numbers and logistics capacity.

Contents

Figures and Tables

Figures

Tables

1. Introduction

Background

Russian military thought since the early 1990s has been focused on the proliferation and employment of conventional long-range precision munitions.[10] The capability to inflict damage throughout the entire depth of the theater of war has had implications for military strategy, deterrence, and conflict escalation. If the North Atlantic Treaty Organization (NATO) could launch attacks against Russian territory at the outset of a war, how could Russia respond? It was not obvious that deep conventional strikes against a Russian military-industrial site or reserve forces would credibly justify Russian nuclear retaliation against a nuclear peer. Until the early 2010s, Russia did not possess a credible long-range conventional response. Russian force structure development since that time has been oriented in part toward resolving this escalation dilemma.[11]

Russia wants to establish a credible intermediate (regional) level of conventional force to deter conflict or, in crisis, conduct preemptive, destructive operations at ranges beyond that of artillery to eliminate both the aerospace threat and the infrastructure required to sustain NATO societies supporting the war. There are offensive and defensive elements, but Russian emphasis is on offense and destruction. One Russian strategist captured the destructive mindset:

> At more-serious stages of conflict escalation, but still within the pre-nuclear stage, remote civilian infrastructure facilities can be targeted in order to minimize the loss of civilians and inflict tangible economic damage on the aggressor, for example, by taking down power plants (except nuclear) that provide energy to megacities.[12]

The military capabilities that correspond to this regional level of warfare are found in four areas. The first is Russia's own version of long-range precision strike, which includes a triad of air, sea, and land-based cruise, ballistic, and hypersonic missiles, as well as manned and unmanned delivery platforms and intelligence, surveillance, and reconnaissance (ISR). The second consists of national air defenses and means of electronic attack to degrade command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). The third centers on weapons to disrupt space-based communications. The final area includes

---

[10] Alexey Arbatov, ed., *Kontrol' nad vooruzheniiami v novykh voenno-politicheskikh i tekhnologicheskikh usloviiakh*, Moscow: IMEMO RAN, 2020a, p. 36.

[11] Anya Loukianova Fink and Olga Oliker, "Russia's Nuclear Weapons in a Multipolar World: Guarantors of Sovereignty, Great Power Status & More," *Daedalus*, Vol. 149, No. 2, Spring 2020; Kristin Ven Bruusgaard, "Russian Nuclear Strategy and Conventional Inferiority," *Journal of Strategic Studies*, Vol. 44, No. 1, 2021.

[12] A. A. Kokoshin, "Strategicheskoe iadernoe i neiadernoe sderzhivanie: prioritety sovremennoi epokhi," *Vestnik Rossiiskoi akademii nauk*, Vol. 84, No. 3, 2014, p. 202.

cyber weapons to target military and civilian infrastructure that is critical for warfighting and domestic stability.[13]

In the post–Cold War era, Russia has sought to develop operational concepts for regional and large-scale war to organize and employ a joint force equipped with the above capabilities. Up to 2008, Russia had relied on Soviet-era operational concepts—separate strategic operations to achieve dominance on the ground, in the air, and at sea in support of a single objective. A strategic operation of nuclear forces (SONF) was a last resort if conventional operations failed to ensure the viability of the Russian state. These distinct lines of effort did not correspond to the changes that had taken place in technology and modern warfare throughout the 1990s and early 2000s. As General-Lieutenant Valerii Makhnin explained in 2019,

> The intensification of the processes of confrontation between combat systems of various levels, the use of high-precision weapons, unmanned aerial vehicles and robotic systems, as well as weapons based on new physical principles, [has led] not only to an increase in the combat capabilities of the [Russian] armed forces, but also has influenced the transition to new forms of their use. For example, there is the general-purpose forces operation [GPFO] and a strategic deterrence forces operation [SDFO] with a space and anti-space operation.[14]

Prior to 2008, Russia had not formally developed an operation to coordinate the employment of a force grouping equipped with air, land, and sea-based long-range precision weapons. Key outstanding questions were what to target and what was required in munitions, platforms, and ISR.[15] An additional challenge was how best to allocate dual-use Russian long-range strike assets. Furthermore, NATO's reliance on the collection and transfer of digital information elevated the importance of coordinating the actions of kinetic, cyber, and electronic warfare (EW) and counterspace against NATO C4ISR and civilian assets well beyond the tactical depth.[16] Relatedly, separate strategic operations did not correspond to the joint and simultaneous character of future war with NATO in the European theater of war and into the continental United States. Up to around 2004, for example, Russia thought about offensive aerospace

---

[13] V. M. Burenok, R. A. Durnev, and K. Iu. Kriukov, "Sukhoputnye voiny budushchego: opyt futurologicheskogo analiza," *Innovatika i ekspertiza*, Vol. 2, No. 27, 2019, p. 240; R. A. Durnev and E. V. Sviridok, "Sistema strategicheskogo neiadernogo sderzhivaniia: ekspertnyi podkhod k obosnovaniiu," *Vooruzhenie i ekonomika*, Vol. 3, No. 57, 2021, p. 16.

[14] V. L. Makhnin, "Voina kak sotsial'no-politicheskoe iavlenie: ot bipolarnosti do tranzitarnosti," *Vestnik Akademii voennykh nauk*, Vol. 3, No. 68, 2019, p. 47. See also V. B. Zarudnitskii, "Kharakter i soderzhanie voennykh konfliktov v sovremennykh usloviiakh i obozrimoi perspective," *Voennaia mysl'*, No. 1, 2021b, p. 43.

[15] For a discussion of the challenges related to matching precision strike technology to an operational concept, see U.S. Congress, Office of Technology Assessment, *New Technology for NATO: Implementing Follow-On Forces Attack*, Washington, D.C.: U.S. Government Printing Office, OTA-ISC-309, June 1987.

[16] Zarudnitskii, 2021b, p. 39.

operations and air defense operations as separate lines of effort in planning.[17] Over the course of the past two decades, Russia has been updating its operational concepts to adapt to changes in warfare.

In sum, Russia's evolution in operational concept development is derived from the need to coordinate and sequence the actions of increasingly diverse and destructive offensive and defensive forces under a single plan to destroy NATO's long-range precision strike system and ability to sustain a war as an alliance, while retaining the ability to cross the nuclear threshold (see Chapter 2).[18] There is also the requirement of incorporating long-range strike assets into the conduct of local or expeditionary wars near Russia's periphery. As General-Major Andrei Sterlin—a department head within the Main Operations Directorate of the Russian General Staff, which is responsible for operational concept development—and coauthors from the 27th Central Scientific Research Institute of the Russian Ministry of Defense wrote in 2019,

> In the future, we must assume that the lines between SDFO and the GPFO will merge into a *unified strategic operation.* The prerequisites for this are already being seen from the perspective of trends in updating the Russian concept of strategic deterrence, de-escalation, and suppression of military threats. The strategic offensive forces represented by the strategic nonnuclear forces [i.e., assets able to engage targets beyond 500 km] are already integrated into the traditional sphere of general-purpose forces in terms of fighting local wars. Thus, the clear separation of strategic deterrence forces [SDF] and general-purpose forces, between the SDFO and the GPFO[,] is collapsing. This portends further integrative associations in the direction of a single strategic operation.[19]

As alluded to by Sterlin and colleagues, one of the most important issues influencing Russian operational concept development is the means that Russia has at its disposal to execute key military tasks at all levels of war—local, regional, and global.

Russian Preparations for an Expanded War

As stated above, a future NATO-Russia war may expand beyond military targets. Energy supply facilities and other critical infrastructure to sustain a war and national economies would be at risk for both sides from the outset of the conflict.[20] This is a factor in Russia's operational

---

[17] G. P. Kupriianov, "Osnovnye tendentsii razvitiia form i sposobov vooruzhennoi bor'by v vozdushno-kosmicheskoi sfere i ikh vliianie na razvitie teorii strategii operativnogo iskusstva VS RF," *Vestnik Akademii voennykh nauk*, Vol. 2, No. 7, 2004, pp. 50–51. Chapter 2 has more discussion of this topic.

[18] There is not an official Ministry of Defense definition of the unified strategic operation. This is our assessment based on the evidence presented in Chapter 2.

[19] A. E. Sterlin, A. A. Protasov, and S. V. Kreidin, "Sovremennye transformatsii kontseptsii i silovykh instrumentov strategicheskogo sderzhivaniia," *Voennaia mysl'*, Vol. 8, 2019, p. 16, emphasis in original.

[20] A. A. Kokoshin, Iu. N. Baluevskii, V. I. Esin, and A. V. Shliakhturov, *Voprosy eskalatsii i deescalatsii krizisnykh situatsii, vooruzhennykh konfliktov, i voin*, Moscow: LENAND, 2021, pp. 60–65; Vladimir Slipchenko and Makhmut Gareev, *Future War*, translation, Ft. Leavenworth, Kan.: Foreign Military Studies Office, 2007, p. 25.

concept development, both from a defensive and an offensive perspective. Russia must commit resources to the protection of critical political, military-industrial, and population centers. (Russia deployed the first S-500 surface-to-air missile [SAM] system to protect Moscow and the "Central Industrial Region."[21]) Offensively, Russia could attempt to mass long-range conventional strikes exclusively against the military assets most directly related to that threat—e.g., air and naval bases, strike platforms, and ISR platforms. However, as Russian officers acknowledge, and as we show in this report, this is probably not a viable strategy for Russia as of 2021 because of the number and location of NATO targets and Russian conventional capacity constraints.[22]

Therefore, Russia is gravitating toward courses of action, under a single operational concept, that are more preemptively violent, expansive, and civilian-focused than some in the West have contemplated.[23] Russian operational planning for future war and the geographical distance between the main forces suggest that a limited war with NATO in a small region in Eastern Europe is improbable. If the war remains a symmetrical, conventional military-to-military fight over a sustained period, the result, because of the large power disparity between the two sides, could be the loss of Russia's defense capability and a breakdown of the Russian state.[24] Unwilling to wait for that outcome, Russia has oriented its operational thinking toward asymmetric employment of kinetic and nonkinetic means against key military and civilian targets in Europe and the United States. The idea is to inflict sufficient damage with all available conventional means (under the nuclear shadow) to compel the West to cease military actions or to fight a conventional war that is much less reliant on the advanced technology that supports noncontact warfare.[25]

Purpose, Organization, and Scope of This Report

We examine Russia's evolution toward a unified strategic operation and associated capability development. To do this, we explore the following questions:

- What are the key military problems that have influenced Russian operational concept development since the late Cold War?

---

[21] "Istochnik: pervaia brigada S-500 zashchitit nebo Moskvy i Tsentral'nogo promyshlennogo raiona RF," TASS, October 12, 2021.

[22] R. A. Durnev, K. Iu. Kriukov, and F. M. Deduhenko, "Preduprezhdenie tekhnogennykh katostrof, provotsiruemykh protivnikom v khode voennykh deistvii," *Voennaia mysl'*, No. 10, 2019a, p. 42.

[23] V. V. Gerasimov, S. F. Rudskoi, V. V. Trushin, and S. P. Belokon', *Osnovy pobedy v boiu*, General'nyi shtab Vooruzhennykh sil Rossiiskoi Federatsii, 2018, p. 6.

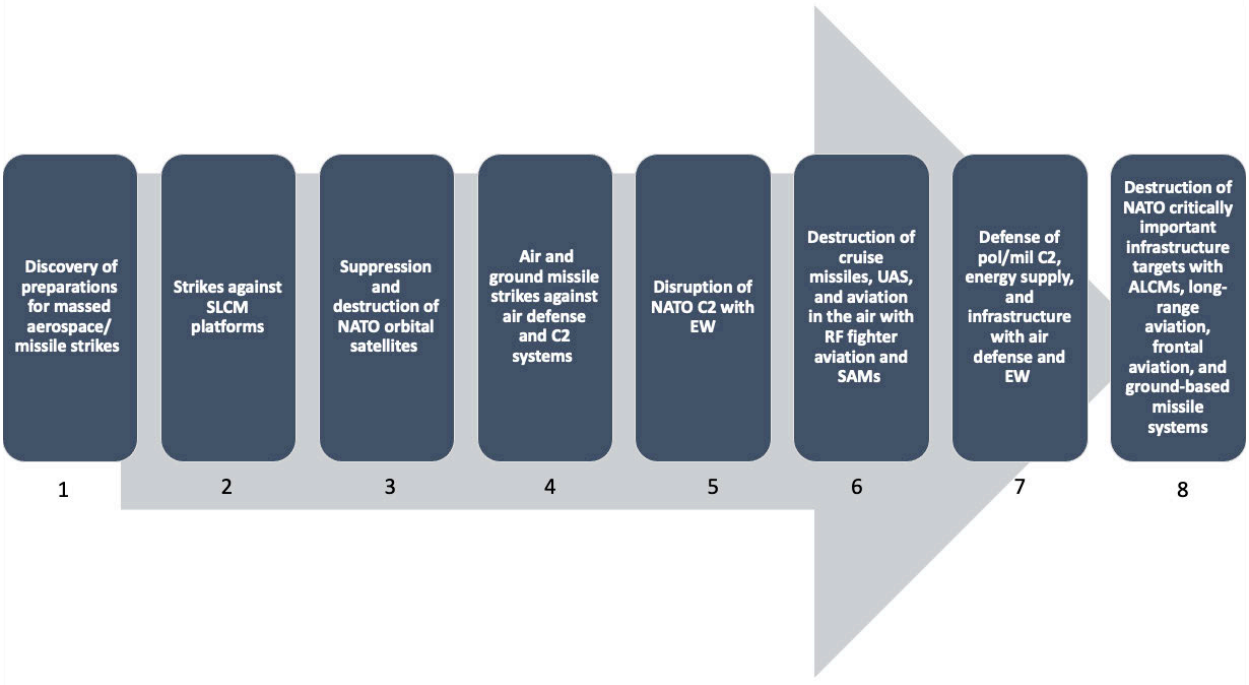
[24] Clint Reach, Alyssa Demus, Eugeniu Han, Bilyana Lilly, Krystyna Marcinek, and Yuliya Shokh, *Russian Military Forecasting and Analysis: The Military-Political Situation and Military Potential in Strategic Planning*, Santa Monica, Calif.: RAND Corporation, RR-A198-4, 2022.

[25] Michael Kofman, Anya Fink, and Jeffrey Edmonds, *Russian Strategy for Escalation Management: Evolution of Key Concepts*, Arlington, Va.: CNA, DRM-2019-U-022455-1Rev, April 2020.

- What is the unified strategic operation, and how does it fit in with this history?
- What are the key military tasks that may be associated with this operation, and how is Russia developing its forces to carry out these tasks?

Chapter 2 presents a brief history of Russia's operational concept development to the present. The General Staff is dealing not only with a qualitatively different military adversary but with an armed force that is far removed from what Soviet planners had at their disposal. The chapter shows how these and other factors are driving operational innovation. In the remainder of the report, we examine Russia's transition to build a "new-type" military that can execute the offensive tasks associated with a future unified strategic operation concentrated in the European theater.[26] Some of the possible tasks to accomplish this mission are shown in Figure 1.1.

Figure 1.1. Notional Sequence of Russian Nonnuclear Actions in Future War in 2030s



SOURCE: Features information from V. M. Burenok, "Razvitie sistemy vooruzheniia i novyi oblik vooruzhennykh sil RF," *Zaschita i bezopasnost'*, No. 2, 2009, p. 15.
NOTE: ALCM = air-launched cruise missiles; C2 = command and control; pol/mil = political and military; RF = Russian Federation; SLCM = submarine-launched cruise missile; UAS = unmanned aerial systems.

We consolidated some of these tasks according to the assets used to execute them. In Chapter 3, we consider Russian theater conventional strike capabilities (Tasks 2, 4, and 8). In Chapter 4, we examine Russia's employment of EW to disable or degrade C4ISR linkages related to the conduct of a massed aerospace attack. Chapter 5 explores Russia's capability and concept

[26] Timothy Thomas, "The Evolving Nature of Russia's Way of War," *Military Review*, July–August 2017, p. 39.

development to exploit NATO reliance on space-based assets in warfighting, and Chapter 6 focuses on Russia's use of cyber weapons to attack critical infrastructure.

Russian operational concepts take shape against Russia's perception of future war. To put our analysis into that context, we draw on three NATO-Russia war scenarios from Russian military literature since 2008. The primary source is a 2008 article by Colonel Arkadii Borzov, then a professor at the Academy of Military Sciences. Borzov analyzed NATO exercises from the early 2000s and speculated on a possible NATO force package to attack Russia that NATO built up prior to the attack.[27] He depicted the Russian forces arrayed in four *fronts*—northern (fronts 1 and 2) and southern—which roughly correspond to present-day joint strategic commands (JSCs) North, West, and South. (See Chapter 2 for a discussion of fronts and JSCs.) General-Major Vasilii Burenok, the current president of the Russian Academy of Military and Artillery Sciences, and Konstantin Sivkov, who served for 12 years within the Russian General Staff, also offered versions of expected NATO force buildup and actions against Russia that generally align with Borzov's analysis.[28] Table 1.1 summarizes the information from Borzov's article, and the table note provides additional information from the other sources.

Table 1.1. Russian Assessment of NATO Force Package and Actions in Future War

Direction[a]	NATO Forces	Operational-Tactical Actions
Arctic	12–16 strategic bombers, 240–320 ALCMs	"Strategic strikes" against Kola Peninsula and surrounding Moscow region
Northwest strategic direction	20 strategic bombers, 3 carrier strike groups, 1 regional strike group, up to 1,500 tactical and naval aircraft, 46 SLCM-capable platforms, airborne warning and control system, 4 Army tactical missile system battalions, 270 nuclear-capable platforms	Strikes against JSC West, JSC South targets, and forces in Belarus
Karelian operational direction	190 tactical aviation, 120 naval aviation, 70 UAS, 220 cruise missiles	Strikes against JSC North targets
Baltic operational direction	150 tactical aircraft, 20–40 UAS, 20–40 operational-tactical missiles	Strikes against JSC West, including Kaliningrad, and forces in Belarus
Western strategic direction	1,140 tactical and naval aviation, 650 UAS, 80–100 operational-tactical missiles, 750 cruise missiles	Strikes against JSC West, JSC South targets, and forces in Belarus

[27] Arkadii Borzov, "Vchera – Iugoslaviia. A kto zavtra?" *Vozdushno-kosmicheskaia sfera*, No. 3, 2008, pp. 38–44.

[28] Burenok, 2009; Konstantin Sivkov, "Nebesnye bastiony," *Voenno-promyshlennyi kur'er (VPK)*, February 18, 2019.

Direction[a]	NATO Forces	Operational-Tactical Actions
NATO naval forces in western Mediterranean	32 combat vessels, 200 cruise missiles	Strikes against naval and air targets and JSC South
Southwestern strategic direction	260 tactical aviation, 20–30 UAS, 200–220 cruise missiles	Strikes against JSC South

SOURCE: Features information from Borzov, 2008.
NOTES: Burenok, 2009, depicts a similar scenario, albeit in less detail. Burenok estimated a duration of active combat from 60 to 190 days. The duration in Borzov, 2008, appears to be approximately 14 days (following force buildup). In 2019, Sivkov predicted that, in a similar scenario to that in Borzov, 2008, and Burenok, 2009, combat activities could last 60 days or more depending on NATO's ability to continue launching offensive air operations.
[a] The forces listed within an "operational direction" seem to be included in those listed for the "strategic direction," although the numbers do not always add up.

To be sure, Russian threat forecasts from the mid-2010s included several different scenarios, such as crises in the Baltics, Belarus, Ukraine, and the southern Caucasus.[29] A war between Russia and NATO might result in part from NATO's belief that it needs to respond to a crisis with a military force buildup to deter Russian actions. From there, assuming that the conflict could not be isolated along Russia's periphery, it would initially center on Russia's ability to disrupt NATO's force generation and conduct of long-range precision strike in the initial period of war. The geographic disposition of main forces demands it.

Because we examine a notional concept for Russia—the unified strategic operation—some speculation is involved. At the same time, the objectives and tasks in this report are drawn from years of following Russian military literature and capability development. Since the early 2000s, the Chiefs of the General Staff and other senior officers have emphasized the criticality of using all available means to disrupt NATO's ability to execute conventional long-range strike. In 2019, the Chief of the General Staff, General Valerii Gerasimov, discussed the idea of preemptively attacking areas where NATO cruise missiles could be launched,[30] and he has repeatedly described EW as a priority in force development to challenge advanced militaries.[31] The head of the Russian General Staff Academy (and former Chief of the Main Operations Directorate) has pointed to NATO's ever growing reliance on space and the need for Russia to target that dependency.[32] Recent actions have shown Russia's ability and willingness to conduct cyber

[29] Clint Reach, *Russian Military Forecasting Translation Volume: 1999–2018*, Santa Monica, Calif.: RAND Corporation, RR-A198-5, 2022, pp. 71–73.

[30] Valerii V. Gerasimov, "Vektory v razvitii voennoi strategii," *Krasnaia zvezda*, March 4, 2019.

[31] Valerii V. Gerasimov, "Sovremennye voiny i aktual'nye voprosy oborony strany," *Vestnik Akademii voennykh nauk*, Vol. 2, No. 59, 2017b, p. 12; Valerii V. Gerasimov, "Vliianie sovremennogo kharaktera vooruzhennoi bor'by na napravlennost' stroitel'stva i razvitiia vooruzhennykh sil Rossiiskoi Federatsii. Prioritetnye zadachi voennoi nauki v obespecheniia oborony strany," *Vestnik Akademii voennykh nauk*, Vol. 2, No. 63, 2018, p. 19; Gerasimov, 2019.

[32] Zarudnitskii, 2021b, p. 41.

operations in both Europe and the United States. Russia, at least until around 2020, did have a strategic operation to destroy critically important targets (SODCIT) (see Task 8 in Figure 1.1).[33] Finally, General-Major Burenok, the author of the 2009 article that we reference for the possible tasks of a future unified strategic operation, is one of the most authoritative Russian officers on weapons development, which, up to 2021, has closely followed the tasks shown in Figure 1.1.[34]

A Note on Sources

The most important source for this report was a 2019 article, cited above, discussing the latest trends in Russian operational concept development.[35] The article was published in the Russian General Staff journal, *Military Thought* [*Voennaia mysl* in Russian], by General-Major Sterlin, Andrei Protasov, and Sergei Kreidin. As mentioned earlier, at the time the article was published, Sterlin was a department head in the Main Operations Directorate of the General Staff.[36] Sterlin is a major thinker and actor within the Russian military. He regularly represents the Russian General Staff in international delegations on arms control and strategic security dialogues with the United States. Protasov was the head of the 27th Central Scientific Research Institute of the Ministry of Defense, where Kreiden works as a senior researcher.[37] Over the course of two decades, Protasov and Kreidin have promoted ideas on strategic deterrence, regional war, nonstrategic nuclear weapons, and strategic nonnuclear weapons that were repeated in the 2019 article. The addition of Sterlin's imprimatur gave authority to these ideas.[38]

Sterlin is also directly or indirectly associated with other Russian thinkers whose work was influential for this report. Aleksandr Khriapin, for example, was a coauthor with Sterlin in an explanatory article in 2020 after the Russian government published the "Principles of State Policy of the Russian Federation on Nuclear Deterrence."[39] Khriapin is a senior researcher at the

---

[33] Michael Kofman, Anya Fink, Dmitry Gorenburg, Mary Chesnut, Jeffrey Edmonds, and Julian Waller, *Russian Military Strategy: Core Tenets and Operational Concepts*, Arlington, Va.: CNA, August 2021, pp. 68–72.

[34] Andrew Radin, Lynn E. Davis, Edward Geist, Eugeniu Han, Dara Massicot, Matthew Povlock, Clint Reach, Scott Boston, Samuel Charap, William Mackenzie, Katya Migacheva, Trevor Johnston, and Austin Long, *The Future of the Russian Military: Russia's Ground Combat Capabilities and Implications for U.S.-Russia Competition*, Santa Monica, Calif.: RAND Corporation, RR-3099-A, 2019.

[35] Sterlin, Protasov, and Kreidin, 2019.

[36] One of the primary tasks of the Main Operations Directorate is strategic and operational planning for the employment of the Russian armed forces.

[37] For a longer discussion of the history and role of the Russian military science system, including its individual research institutes, see Clint Reach, Vikram Kilambi, and Mark Cozad, *Russian Assessments and Applications of the Correlation of Forces and Means*, Santa Monica, Calif.: RAND Corporation, RR-4235-OSD, 2020, pp. 4–7.

[38] It is important to note that what Sterlin et al. discuss in the article is not official military doctrine; it is the authors' view on where they think Russian operational concept development is going according to current trends.

[39] A. Sterlin and A. Khriapin, "Ob osnovakh gosudarstvennoi politiki Rossiiskoi Federatsii v oblasti iadernogo sderzhivaniia," *Flag rodiny*, August 14, 2020; President of Russia, "Ob osnovakh gosudarstvennoi politiki Rossiiskoi Federatsii v oblasti iadernogo sderzhivaniia," decree, No. 355, June 2, 2020.

Center for Military-Strategic Studies of the Military Academy of the General Staff and has written about strategic deterrence and the employment of nuclear weapons since the 1990s. In their 2019 article, Sterlin, Protasov, and Kreidin describe the work of General-Major Burenok and Iurii Pechatnov, titled *Strategic Deterrence*, as a prevailing view on the topic in Russian strategic thought. Thus, Protasov, Kreidin, Khriapin, Burenok, and Pechatnov, along with Sterlin, form an authoritative cadre of Russian thinkers whose work is relevant to ongoing military debates on Russian operational concept development.

A final important source for this study was the late General-Colonel Andrian Danilevich. Danilevich served from 1964 to 1990 on the Soviet General Staff in the Main Operations Directorate. He led a collective effort in the 1970s to develop the *Strategy of Deep Operations*.[40] In 1992, Danilevich wrote an important piece—the only publicly available article he wrote that we are aware of—on the future employment of Russia's "strategic nonnuclear forces"; that is, long-range precision munitions. His argument was as follows. First, the territorial division of forces in the post–Cold War era would dictate engaging targets at long range. Second, critical military and civilian targets were ubiquitous in the European theater, which would create steep quantitative requirements for munitions. Third, because of the munitions requirement and Russian resource limitations to acquire them, Russia should employ these weapons against an adversary's military-economic potential (e.g., energy supplies, such as oil and electricity). Curiously, Danilevich is not cited in contemporary Russian literature on strategic deterrence or operational concepts. But the issues he raised in 1992 about conventional long-range munitions have been discussed in Russian military writing for the past three decades, including in the works of the leading officers and experts mentioned above.

[40] This work remains classified or inaccessible to non-Russian analysts.

2. Russia's Evolution Toward a Unified Strategic Operation

Introduction

NATO is an alliance with a massive amount of military and economic potential protected by thousands of kilometers of strategic depth. It also possesses the conventional and nuclear capability to generate decisive military effects in future war. The central military problem for the Soviets and Russians, therefore, has been how to conduct offensive operations rapidly and throughout the entire depth of NATO to overwhelm its ability or willingness to continue the war.[41]

Since World War II, there have been four eras of Russian operational concept development in pursuit of a solution to this military problem. Each of these eras has been influenced by technological, economic, and geopolitical factors. The first era—1945 to 1976—was defined by strategic and theater nuclear weapons, which could rapidly and perhaps decisively alter the correlation of forces in favor of the preemptive aggressor. The second era—1976 to 1991—was one of strategic nuclear parity.[42] During this time, operational thinking about conventional war returned when leading Soviet strategists realized that preemptive nuclear escalation was likely not a viable strategy against a nuclear peer. The third era—1991 to 2011—was one of economic upheaval for Russia, territorial changes in favor of NATO, a rapid reduction in Russia's conventional capability, and the employment of long-range precision weapons on the battlefield. The fourth era—2011 to the 2030s—is still underway and includes important features of the previous era. The most important characteristic of the fourth era, from the standpoint of overcoming NATO's strategic depth, is the ongoing development of Russia's ability to engage targets at the regional level (beyond 500 km from Russian forces, roughly speaking) with nonnuclear weapons.

This chapter, and the remainder of this report, is focused on this fourth era of Russian operational concept and capability development. However, the second and third eras remain relevant, and we will highlight the most-salient factors from these periods in the opening sections of this chapter. We will show how Russia is in the midst of a transition away from nuclear dependence toward nonnuclear means, such as cruise and ballistic missiles, EW, counterspace, and cyber weapons, to engage targets at long range. Russia's operational concept innovation is

[41] We explained the reasons for the Soviet and Russian preference for offensive, destructive operations in a previous study (Reach, Blanc, and Geist, 2022).

[42] Russian President Mikhail Gorbachev took the Soviet military in a different direction from 1985 to 1991. A defensive approach was adopted, and forward forces were moved to the rear. This was an aberration in the post–World War II era, when the Soviets and Russians by and large were thinking about how to structure and employ forces to destroy the adversary in offensive operations throughout the depth of the theater.

centered on coordinating and employing these disparate capabilities from across Russia's military districts while retaining the ability to cross the nuclear threshold with dual-use platforms. According to leading Russian military strategists, as of 2021, Russia is still reliant on nonstrategic nuclear weapons as the primary tool for regional deterrence and warfighting. The transition to the fourth era of operational concept development, which aspires to a *unified strategic operation* weighted more heavily toward nonnuclear capabilities, remains incomplete.

Overcoming NATO's Strategic Depth: 1976–1984

Up to the mid-1970s, the Soviets were primarily focused on how to decisively employ nuclear weapons against NATO.[43] As the reality of strategic nuclear parity was absorbed by Soviet military planners, new approaches were considered, most notably by Chief of the General Staff Nikolai Ogarkov (1976–1984). Ogarkov and senior advisers brought new concepts to the General Staff that were more focused on fighting and winning the conventional war rapidly and decisively. The employment of nuclear weapons was always an element of Soviet military planning, but the General Staff considered whether it might be possible to conduct conventional operations to put NATO in a position where theater nuclear employment was either not possible or not desirable.

To do this, Soviet planners wanted to conduct rapid, conventional ground and strike operations "to the beaches at the western edge of [Europe]."[44] If the Soviets did not detect NATO preparations for nuclear escalation, the plan was to use conventional means exclusively.[45] One of the key Soviet theoreticians behind the scenes was General-Colonel Andrian Danilevich, who, around 1977, oversaw the development of the three-volume *Strategy of Deep Operations* while serving in the Main Operations Directorate of the Soviet General Staff.[46] In a review of the development of deep operations up to 1978, one contemporary described the leading trends in operational thinking at that time:

> [T]he main condition for a successful offensive without the use of nuclear weapons is the creation of superiority over the enemy in tanks, artillery, and aviation in the directions of the main strikes. The choice of the direction of the main attack should ensure the successful penetration of the tactical defense zone, the movement of forces in a short time to the areas where the enemy's most important objects (nuclear attack weapons, command posts, airfields, etc.) are

---

[43] David M. Glantz, *The Military Strategy of the Soviet Union: A History*, Abingdon, United Kingdom: Frank Cass, 1992, p. 192; V. A. Zolotarev, ed., *Istoriia voennoi strategii Rossii*, Moscow: Kuchkovo Pole/Poligrafresursy, 2000, pp. 461–465.

[44] John Hines, Ellis M. Mishulovich, and John F. Shull, *Soviet Intentions 1965–1985:* Vol. II, *Soviet Post-Cold War Testimonial Evidence*, McLean, Va.: BDM Federal, Inc., September 22, 1995, p. 7. The quote is as recorded by Hines from an interview with General-Lieutenant Gelii Batenin.

[45] Hines, Mishulovich, and Shull, 1995, p. 7.

[46] As mentioned previously, as far as we know, this work remains classified or at least is inaccessible to non-Russian analysts.

> located, to the flank and rear of the main grouping to defeat the enemy. [T]he operational formation of military units can include the same elements as in an offensive with the use of nuclear weapons, but it is necessary to create a stronger first echelon, and the second echelons and reserves can be somewhat closer to the first, which will ensure their faster introduction into battle and will reduce the depth of the operational formation. [At] the very beginning of the operation, it is necessary to disable the enemy's nuclear attack weapons, aviation, suppress his reserves, disrupt command and control, and, during the offensive, continuously build up strikes by introducing second echelons and reserves into battle.[47]

The military historian David Glantz describes the objective of deep operations within a larger theater strategic operation as being "aimed at disrupting the link between conventional hostilities and their escalation towards a global nuclear war."[48]

To carry out this vision, Ogarkov first needed to update operational concepts. Up to the second half of the 1970s, there was not a fully developed, unified strategic plan for the employment of the armed forces.[49] Strategic operations apparently were defined by individual tasks and loosely connected. Ogarkov was envisioning a complex of coordinated actions of multiple fronts and fleets at the outset of the war that were highly mobile and capable of strikes at longer ranges within the construct of a single strategic operation. He described the rationale for a new strategic operational concept, which he called a *large-scale operation in the theater of military operations*, this way:

> At the present time the combat capabilities of troops, aviation, and navies, their maneuverability, and the long range of their munitions has drastically increased [since World War II]. Timelines for concentrating strike groupings and replenishing them have been reduced. The conditions and methods for executing operational and strategic tasks with large, joint formations have changed. Additionally, supreme military command can directly and decisively influence the course and outcome of the war. As a result, previous forms of employing large, joint formations have become obsolete in modern conditions. The primary operation is no longer the *front* operation or even the multi-*front* operation, but it is rather a modern, large-scale *operation in the theater of military operations*.[50]

Three elements distinguished Ogarkov's theater strategic operation: There would be coordinated conventional strikes from the outset of the war throughout the entire depth of the continent; the scope covered the entire theater of military operations; and there would be a combination of offensive and defensive actions, but the focus would be on the offense.[51] To execute, the Soviets

---

[47] L. I. Voloshin, "Teoriia glubokoi operatsii i tendentsii ee razvititiia," *Voennaia mysl'*, No. 8, 1978, p. 25.

[48] David M. Glantz, "Inheriting Ogarkov: Soviet and Russian Views of the Changing Nature of War," remarks translated into Russian by Centre for Analysis of Strategies and Technologies, March 13, 2015.

[49] Iu. N. Baluevskii, *General'nyi shtab Rossoiskoi armii: istoriya i sovremennost'*, Akademicheskii Proekt, 2006, p. 307.

[50] N. V. Ogarkov, *Istoriia uchit bditel'nosti*, Voenizdat, Moscow, 1985, p. 47, emphasis in original.

[51] Zolotarev, 2000, p. 469.

required higher readiness of first- and second-echelon forces, and actions of ground, air, naval, airborne, and missile forces would need to be coordinated to (1) inflict widespread damage on critical military and economic targets to disable NATO's response and (2) support the rapid seizure of broad swaths of territory by land forces in a very short time (weeks).[52] Another objective was to take out smaller member-states of the coalition as rapidly as possible.[53] As noted by Ogarkov, the simultaneous or closely sequenced actions of multiple fronts and fleets was a necessity to achieve the desired aims. Table 2.1 presents the primary characteristics of the strategic operation in the continental theater of military operations (which we also refer to as a *theater strategic operation* for shorthand).

Table 2.1. Strategic Operation in a Continental Theater of Military Operations, 1977–1984

Category	Details
Front	1,000–1,500 km
Depth	90–1,200 km
Duration	30–35 days
Tempo	20 km per day
Operations	• Massed missile/fire strikes throughout theater • Initial front offensive (10–12 days) • Sequential front offensive (20 days) • Partial defense • Air • Air defense • Airborne • Naval • Reserve deployment
Order of battle	• 2–5 fronts • 2–5 air armies • 1–2 fleets • Airborne division

SOURCES: Features information from N. V. Ogarkov, "Doklad nachal'nika Shtaba rukovodstva—nachal'nika General'nogo shtabe Vooruzhennykh Sil SSSR Marshala Sovetskogo Soiuza Ogarkova N.V.," in *Materialy rasbora operativno-strategicheskogo komandno-ucheniia 'Zapad-77'*, Moscow: Ministerstvo oborony SSSR, 1977; Zolotarev, 2000, p. 470.

The idea of a lightning blow against such a massive military alliance as NATO, which had enormous depth back to the U.S. heartland, was ambitious. The Soviet strategist Aleksandr Svechin cautioned against such overreach in the 1920s.[54] Svechin believed that a quick war

[52] "Strategic Operations in a Continental Theater of Strategic Military Action," *Journal of Slavic Military Studies*, Vol. 2, No. 2, 1989, p. 173.

[53] David M. Glantz, *Soviet Military Operational Art: In Pursuit of Deep Battle*, Abingdon, United Kingdom: Frank Cass, 1991, p. 221.

[54] Aleksandr A. Svechin, *Strategy*, 2nd ed., trans. Kent Lee, ed., Minneapolis, Minn.: East View Publications, 1991.

between great powers was unlikely given each side's material resources to weather a blow and continue fighting. The result, in Svechin's view, would instead be a protracted war with enormous losses on both sides. Svechin, therefore, rejected an expensive peacetime force buildup to execute decisive offensive operations in the initial period of war—exactly what Ogarkov was proposing.

At the same time, the theater strategic operation with conventional forces demonstrates the complexity of planning a war against a large, nuclear alliance. When the defending side has nuclear weapons, the political rationale of the attacker can quickly be rendered moot if the adversary cannot be defeated quickly and conflict escalation ensues. Thus, if a conventional war is to be won, there is a temptation to try and win it quickly to put the opposing side in a position in which capitulation looks more appealing than nuclear escalation. The economic and military challenge is to build up and coordinate sufficient offensive capacity to decisively overwhelm such a powerful adversary with a large amount of strategic depth. Nevertheless, Ogarkov designed a ground-centric operation that called on as many as five fronts to execute rapid ground operations to the depths of Western Europe.

The Soviet operational development at that time had a dual effect. First, senior Western military commanders believed that Soviet execution of operational concepts would create serious problems for NATO. According to a 1987 report by the congressional Office of Technology Assessment,

> On several occasions, NATO's Supreme Allied Commander Europe (SACEUR), General Bernard W. Rogers, has warned that were the Warsaw Pact to attack NATO, it would only be a few days before he would have to ask NATO political leaders for permission to use nuclear weapons. . . . Some analysts believe that the Soviets might overrun NATO so quickly that NATO would not have time to decide to use its theater nuclear weapons [exactly Ogarkov's plan]. Only strategic nuclear weapons would be left.[55]

The second effect was the pursuit by NATO of its own operational counteractions based on new technology of the time. NATO's ability to employ conventional long-range munitions against Soviet second-echelon forces created new problems for Soviet planners to contemplate.

Ogarkov apparently never fully consolidated Soviet concepts into the single theater strategic operation. He was dismissed in 1984, and later Russian references show that the Soviets and Russians retained multiple operational concepts for large-scale war. Gorbachev eventually took the Soviet Union and the military in an entirely different direction based on his perception of the unsustainability of the Soviet approach to military and domestic policy. In the late Cold War period, the Soviets adopted a defensive doctrine that was followed by force reductions and a shift away from an offensive force posture. The tack to defense proved to be short-lived, however. By the 2010s, the Russians had returned to some of the leading principles of the theater strategic

[55] U.S. Congress, Office of Technology Assessment, 1987, p. 15.

operation, albeit within a very different geopolitical environment, theater force posture, and overall force structure.[56]

Overcoming NATO's Strategic Depth: 1991–2011

The collapse of the Soviet Union and the geographic and economic fallout were the defining moments of this era from a military perspective. The reduction of borders back to the Russian Federation drastically increased the amount of territory that Russia's land forces would have to cover to "close quickly with the enemy."[57] Moreover, the Russian economy would not be able to support the amount of ground forces needed to rapidly seize and control NATO territory. Helpfully for the Russians, in the first two decades of the post–Cold War period, NATO was itself engaged in a massive military drawdown in response to the geopolitical environment of the time. The last U.S. tank departed Europe in 2013.

At the same time, there were significant changes in the way the West was preparing to wage modern war. The employment of conventional precision-guided munitions (PGMs) was reducing the role of land forces and providing new ways to engage critical targets beyond the tactical depth without a large ground force or nuclear weapons. Even prior to the U.S.-led intervention in the Persian Gulf War in 1991, the Soviets were grappling with how technological developments might affect the theater strategic operation.[58] The forecasted proliferation of long-range PGMs created challenges for the first and second echelons. A concentrated first echelon could be vulnerable to preemptive conventional attack. If the second echelon were close to the first, it too could be targeted early in the conflict, leaving the first echelon more exposed over time. (This was precisely NATO's thinking in the development of the "follow-on forces attack.") In other words, the linear echelonment of the past would likely need to be replaced with new forms of deployment and maneuver.

In 1991, Glantz summarized the Soviet view on technology and future war:

> Today, armed with new weaponry, the defender [NATO] can strike at the enemy [the Soviet Union] at long range, and at a time of his own choosing before the enemy deploys for attack. . . . In these circumstances . . . the ability of the attacker [the Soviet Union] to close quickly with the enemy has become more important, because by closing rapidly the attacker can deprive [NATO] of its ability to employ high precision weapons to their fullest effect. This altered relationship has also placed greater premium on an attacker conducting rapid initial maneuver to intersperse his forces among those of the defender so as to

[56] Jacob W. Kipp, "The Evolution of Soviet Operational Art: The Significance of 'Strategic Defense' and 'Premeditated Defense' in the Conduct of Theatre-Strategic Operations," *Journal of Soviet Military Studies*, Vol. 4, No. 4, December 1991.

[57] Glantz, 1991, pp. 254–255.

[58] U.S. Congress, Office of Technology Assessment, 1987, pp. 105–108; Barry D. Watts, *Six Decades of Guided Munitions and Battle Networks: Progress and Prospects*, Washington, D.C.: Center for Strategic and Budgetary Assessments, March 2007, pp. 28–30.

> ensure that combat remains fragmented. Fragmented combat, characterized by forces striving to achieve point or area objectives rather than securing lines (linear battle), also hinders employment of high precision and tactical nuclear weapons. This is, in essence, analogous to the Soviet anti-nuclear techniques of the 1970s, only now writ large.[59]

All of these changes—economic, geographic, technological—meant that Russian operational concepts would have to evolve. The theater strategic operation could no longer be the primary planning construct for regional war; there would not be enough ready ground forces to move all the way to central, southern, and western Europe, where NATO's greatest military potential outside the United States resided. The Russians nevertheless did not waiver from the principle that offensive actions needed to be conducted throughout the depth of the theater. But there were serious questions regarding the means with which this principle could be matched with an operational plan.

From Ground-Centric to Strike-Centric: The Role of Nonstrategic Nuclear and Strategic Nonnuclear Weapons

Prominent Russian strategists were adamant that defense alone would not be suitable against an adversary with significant long-range strike capability. For one, NATO might execute conventional strikes not exclusively on first or second echelons but also on the military-economic potential of the country (which remains an enduring concern for the Russians). In 1994, A. P. Bondarenko, N. I. Turko, and S. I. Fedorchenko, all Russian colonels at the time, examined how strategic operations would need to evolve given the ongoing changes in modern warfare. They concluded that the protection of Russian military-economic potential in the interior of the country would have to be done through the coordinated *offensive* actions of a joint force to destroy the aerospace enemy at the point of departure, deep within its territory.[60]

General-Colonel Danilevich argued for a somewhat different approach based on the same offensive principles. In 1992, he considered whether Russia might be able to carry out symmetric, conventional strikes against NATO air bases and other military infrastructure.[61] He doubted that Russia, for the foreseeable future, would have the munitions capacity to directly attack traditional military targets—e.g., air bases and naval platforms—with long-range precision munitions. Instead, he proposed a "countervalue campaign" designed to inflict damage on NATO's own military-economic potential, which included oil refining infrastructure, warehouses and terminals of oil products, and electric power enterprises.[62]

---

[59] Glantz, 1991, pp. 254–255.

[60] A. P. Bondarenko, N. I. Turko, and S. I. Fedorchenko, "Evolutsiia form strategicheskikh deistvii v bor'be s vozdushno-kosmicheskim protivnikom," *Voennaia mysl'*, 1994, p. 23. Clearly, Russian air defenses would have a large role to play in the defense of the Russian interior.

[61] A. A. Danilevich and O. P. Shunin, "O neiadernykh silakh sderzhivaniia," *Voennaia mysl*, No. 1, 1992, p. 49.

[62] Danilevich and Shunin, 1992, p. 52.

Notable in Danilevich's analysis was the explicit rejection of a massive ground operation into the depths of the European continent to rapidly destroy NATO's ability to launch a conventional aerospace attack. Russian force structure was moving in the opposite direction, downsizing considerably, a trend that would continue for the next two decades.[63] Danilevich was adapting to a new theater force laydown and technological developments: "[D]eep fire strikes using high-precision weapons, especially in conditions when the opposing sides are territorially divided will form the basis of operations in conventional war."[64] Deep operations to quickly disrupt NATO were evolving from linear and ground-centric toward a nonlinear, strike-centric approach.

Danilevich was looking to a reality that would not exist for Russia for another 25 years. And, even then, it would exist only at a nascent phase. The idea of Russia targeting military or civilian targets in central and western Europe with long-range precision munitions remained mostly hypothetical until the mid-2010s. This meant that other solutions would have to fill the gap until Russian force structure caught up with the theory. Several other Russian analysts, who appear to remain influential today given their ties to General-Major Sterlin, repeatedly connected Russian conventional strike inferiority to preemptive nuclear escalation in regional war.[65]

In the late 1990s, Colonel Khriapin, as a coauthor, focused on the relatively new (for Russia) role for nuclear weapons at the regional level in response to a conventional attack.[66] The authors noted that strategic stability at the regional level could be maintained by "nonstrategic nuclear forces equipped with operational-tactical (tactical) nuclear weapons [see Table 2.2], together with the general-purpose forces and, if necessary, the air-based component of the strategic nuclear forces."[67] They further argued, "The presence of nonstrategic nuclear weapons in Russia's nuclear forces makes it possible to compensate for the imbalance of general-purpose forces, and their use in the course of hostilities completely negates the enemy's superiority in certain strategic (operational) areas."[68]

---

[63] According to the Russian Ground Force Commander, in 2015, there were 209,400 personnel in the Russian Ground Forces. By 2020, they planned to increase that number to 300,000 (Viktor Khudoleev, "Voiska s velikoi istoriei," *Krasnaya Zvezda*, 2015).

[64] Danilevich and Shunin, 1992, p. 48.

[65] Protasov and Kreiden coauthored the 2019 piece with Sterlin, and Khriapin was a coauthor with Sterlin in an explanatory article in 2020 after the Russian government published "Principles of State Policy of the Russian Federation on Nuclear Deterrence" (see Sterlin and Khriapin, 2020; President of Russia, 2020).

[66] V. A. Ivasik, A. S. Pis'iaukov, and A. L. Khriapin, "Iadernoe oruzhie i voennaia bezopasnost' Rossii," *Voennaia mysl'*, No. 4, 1999, p. 72.

[67] Ivasik, Pis'iaukov, and Khriapin, 1999, p. 72.

[68] Ivasik, Pis'iaukov, and Khriapin, 1999, p. 72.

Table 2.2. Russian Categorization of Nuclear Weapons

Categorization	Weapons
Strategic nuclear weapons	• ICBMs • SLBMs • ALCMs (Tu-95 and Tu-160)
Operational-strategic (theater) nuclear weapons	• ALCMs (Tu-22) • SLCMs (submarine and surface)
Operational-tactical (tactical) nuclear weapons	• Gravity bombs • SRBMs and artillery rounds • SAMs and ABMs • Nuclear mines and torpedos

SOURCES: Features information from V. I. Levshin, A. V. Nedelin, and M. E. Sosnovskii, "O primenenii iadernogo oruzhiia dlia deeskalatsii voennykh deistvii," *Voennaia mysl'*, No. 3, 1999, pp. 34–35; NATO, *The Secretary General's Annual Report*, Brussels, 2020, p. 32.
NOTE: ABM = antiballistic missile; ICBM = intercontinental ballistic missile; SLBM = submarine-launched ballistic missile; SRBM = short-range ballistic missile.

That same year, Lieutenant Colonel Kreidin weighed in on the issue of regional deterrence. Kreidin began by stating that the relevance of regional deterrence was the result of "the crisis state of the domestic economy and general-purpose forces, whose ability to repel large-scale aggression has significantly decreased in recent years."[69] One of the issues that Kreidin raised was how the development of U.S. conventional strike capability could threaten Russia's ability to launch tactical nuclear weapons. (This was NATO essentially turning the tables on the Russians by presenting them with the same dilemma that General Bernard Rogers faced in the 1980s.) Therefore, Kreidin left open the door for the use of *strategic* nuclear weapons in limited numbers, even at the regional level.[70] This reference to strategic nuclear weapons probably coincides with the reference immediately above to the air-based component of the strategic nuclear forces being employed in a regional war.[71] Another important argument was that nuclear weapons at the regional level should primarily target military infrastructure of the aggressor.[72] Whereas Russian strategic nuclear strikes would be massed against countervalue targets in the United States, regional nuclear weapons should be allocated for counterforce missions in limited numbers.

Although these authors were writing at a time of great economic upheaval in Russia, the discourse on the relationship between conventional capacity and operational planning for regional and large-scale war has not changed significantly among authoritative Russian sources since the late 1990s. Writing in 2011, Burenok and Pechatnov echoed the remarks of Khriapin

[69] S. V. Kreidin, "Global'noe i regional'noe iadernoe sderzhivanie: k sisteme printsipov i kriteriev," *Voennaia mysl'*, No. 4, 1999, p. 74.

[70] Kreidin, 1999, p. 74.

[71] Ivasik, Pis'iaukov, and Khriapin, 1999, p. 72.

[72] Kreidin, 1999, p. 75.

and Kreidin above. In their work on strategic deterrence, they reached two important conclusions. First, the Russian general-purpose forces were not sufficiently manned and equipped to respond to conventional aggression from NATO.[73] As a result, strategic and nonstrategic nuclear weapons were the foundation of Russian deterrence and, presumably, regional and global warfighting.[74] Second, nonstrategic nuclear weapons would be the primary tool in a regional conventional war that was threatening the existence of the Russian state. These weapons were most appropriate for counterforce missions (agreeing with Kreidin), and strategic nonnuclear weapons at that time and for the foreseeable future were an auxiliary tool best employed against the military-economic potential of the adversary (agreeing with Danilevich).

Strategic Operation to Destroy Critically Important Targets

The operational result of such ideas appears to have been SODCIT.[75] The Russians officially adopted this operation around 2008, likely in preparation for a growing but still small number of long-range conventional weapons. Because Russia retained SONF, and drawing on the discussion immediately above, we can infer that SODCIT was a conventionally focused operation for striking at depth against NATO civilian and military infrastructure. In our view, this was a component of Russian planning for future regional or large-scale war into the 2010s and 2020s. Prior to 2010, Russia simply did not have the long-range conventional means to warrant a dedicated strategic operation for their employment. As explained above, SONF was probably the most relevant operational concept for regional war during this era and into the next one.

Overcoming NATO's Strategic Depth: 2011 to the 2030s

The 2020 and 2027 State Armaments Programs are major efforts to invest the resources required to overhaul the Russian military and prepare it to deter and conduct modern warfare. Most relevant to this discussion have been Russian investments in a conventional theater strike complex, EW, counterspace, and cyber weapons.[76] These are the means with which Russia can threaten NATO at the regional and global levels without resorting to nuclear escalation, which is fraught with unpredictable and existential escalation risks. Developments in Russian strategic operations throughout the 2000s have in some ways related to how to most effectively and efficiently employ formations equipped with such weapons to counter NATO throughout its strategic depth.

---

[73] V. M. Burenok and Iu. A. Pechatnov, *Strategicheskoe sderzhivanie*, pre-publication copy, 2011, p. 101.

[74] Burenok and Pechatnov, 2011, pp. 101, 151–152.

[75] For more information on this operational concept, see Kofman et al., 2021; and Reach, Blanc, and Geist, 2022.

[76] Burenok, 2009. See the subsequent chapters in this report for discussions of these capability areas.

A notable trend has been the consolidation of operational concepts. The purpose of consolidation is to simplify operational planning and improve the speed at which heterogeneous forces can be coordinated and concentrated to deliver maximum destruction of the enemy in the shortest time possible. In the 1960s, the primary focus was on coordinating all elements of the nuclear triad to deliver decisive strikes against key enemy military-industrial, command and control (C2), and nuclear weapons facilities to set the stage for rapid ground operations deep into Western Europe. In the late 1970s and early 1980s, Ogarkov sought similar objectives, but primarily with conventional forces, with the leading role assigned to the land troops at breakthrough points in central Europe.

The post-Soviet period has seen a renewed consolidation of strategic operations to overcome NATO's strategic depth, with the specific aim of destroying NATO's aerospace attack system and critical civilian infrastructure to terminate the war on Russian terms.[77] In 2004, Russia generally retained the strategic operations from the late Soviet period, folding the operation to repel an aerospace attack into the strategic aerospace operation.[78] General-Lieutenant G. P. Kupriianov explained the reason for this consolidation, emphasizing the simultaneous need to both defend against the aerospace attack and launch offensive strikes against enemy assets involved in the attack. His discussion was focused on air and air defense, but it offers important insight into what has followed since the early 2000s:

> These [strategic air and air defense] operations were practiced, as a rule, in the same airspace, with practically the same forces and means, with largely similar goals and objectives. In the absence of a theater commander [apparently rejected after Ogarkov's departure], and due to technical issues, command and control until recently was carried out by multiple branches of the Armed Forces (Air Force and Air Defense Forces). Now this imbalance in the organizational plan has been partially eliminated by the merger of the Air Force and Air Defense Forces into a single branch of the Armed Forces [now the Aerospace Forces (VKS)]. In this regard, to simplify the planning, organization, and conduct of operations in the air domain, to reduce the number of operational documents being developed, and to make actions more dynamic, it is proposed to plan one air operation in the theater of operations instead of two (air and air defense).[79]

In 2013, Gerasimov questioned the need for multiple strategic operations and implied possible reduction in the future.[80] Some time prior to 2020, Russia again merged its strategic operations. It combined SODCIT and SONF, creating what some have referred to as the *strategic*

[77] Reach, Blanc, and Geist, 2022.

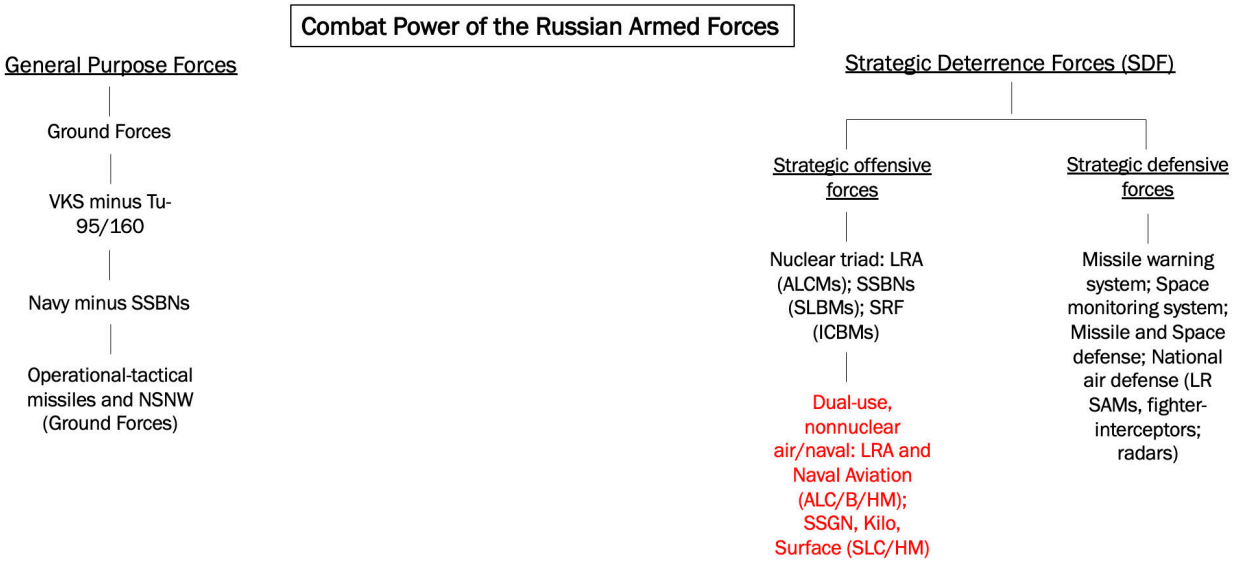
[78] An argument for consolidation of the operations can be found in Kupriianov, 2004, pp. 48–52.

[79] Kupriianov, 2004, p. 51.

[80] Valerii V. Gerasimov, "Osnovnye tendentsii razvitiia form i sposobov primeneniia Vooruzhennykh sil, aktual'nye zadachi voennoi nauki po ikh soversheniiu," *Vestnik Akademii voennykh nauk*, Vol. 1, No. 42, 2013, p. 27.

offensive forces operation. We think that it is officially called the *strategic deterrence forces operation* (see Figure 2.1 for a depiction of Russia's SDF and general-purpose forces).[81]

Figure 2.1. Russia's General-Purpose and Strategic Deterrence Forces



SOURCE: Adapted from Ministry of Defense of the Russian Federation ("Strategicheskie sily sderzhivaniia," Voenno-entsiklopedicheskii slovar', Ministerstvo oborony RF, undated).
NOTES: ALC/B/HM = air-launched cruise/ballistic/hypersonic missiles; ALHM = air-launched hypersonic missile; LRA = Long-Range Aviation; LR SAM = long-range SAM; NSNW = nonstrategic nuclear weapons; SLC/HM = sea-launched cruise/hypersonic missile; SRF = Strategic Rocket Forces; SSBN = ballistic missile submarine; SSGN = multipurpose guided missile submarine. The Iskander operational-tactical missile system—with a 500-km range—is typically categorized strictly as a warfighting tool, as opposed to a component of deterrence forces with a different mission and target set. As longer-range ground-based systems come online, this is likely to change.

The reported reason for this marriage of operations was to simplify planning and the allocation of strategic nonnuclear and nuclear weapons in response to U.S. operational concepts:

> [The development of various U.S. concepts, such as Conventional Prompt Global Strike,] is one of the reasons behind the transformation of a strategic operation to destroy critically important targets and the strategic operation of nuclear forces into a new form of employing the Russian Armed Forces—a strategic offensive forces operation—which will ensure efficient allocation of enemy targets between [Russia's] nuclear forces and forces equipped with strategic nonnuclear weapons. This will facilitate joint planning and employment of nuclear and

[81] A definition of *operation of strategic deterrence forces* (SDFO) captures the blending of nonnuclear and nuclear strikes into a single operation. See the definition a few pages below.

> strategic nonnuclear forces in a coordinated plan under the Supreme Commander-in-Chief and under direct control of the Russian General Staff.[82]

The "allocation of enemy targets" and the platforms and munitions required to engage them will be a key theme of the next chapter. It is one of the most important tasks driving evolution in Russian operational art in the third and fourth eras. Russian strategists have grappled for three decades with how to organize and employ task forces equipped with long-range precision munitions while retaining the ability to cross the nuclear threshold with some of the same delivery platforms (e.g., the Tu-95 strategic bomber) and reserved dual-use munitions.[83]

In 2019, General-Major Sterlin suggested that further consolidation was in the offing. He described winnowing the operational concepts to two—a GPFO and an SDFO.[84] Russia's general-purpose forces, depicted in Figure 2.1, have been defined as

> a component of the Russian Armed Forces intended for warfighting with conventional weapons as well as for war with the use of tactical nuclear weapons in conjunction with the Strategic Nuclear Forces in nuclear war. General-purpose forces include Ground Forces, the Aerospace Forces, the Navy (excluding sea-based strategic nuclear forces), and forces that are outside the service branches and combat arms. . . . They are most often employed in local wars and military conflicts.[85]

According to this definition of Russia's general-purpose forces, the most likely purpose of a GPFO is to isolate a local conflict along Russia's periphery with conventional forces while deterring external intervention with nuclear operational-tactical missiles.[86] The SDFO, which we describe later in this chapter, is likely a phased employment of Russia's most destructive weapons throughout the theater of war, which would comprise all of Europe and the continental United States. Roughly speaking, the GPFO and the SDFO appear to be intended for local war and regional or large-scale war, respectively. They are the result of a clear delineation between

---

[82] V. G. Ivanov, A. Iu. Savitskii, and S. G. Makarov, "Vliianie voin i vooruzhennykh konfliktov na sistemu sviazi voennogo naznacheniia," *Radiolokatsiia, navigatsiia, sviaz': Sbornik trudov XXVI Mezhdunarodnoi nauchno-tekhnicheskoi konferentsii*, Voronezhskii gosudarstvennoi universitet / Sozvezdie Contsern, 2020, p. 248. The strategic offensive forces operation appeared in Russian military literature in 2017 (A. V. Vitko, "Chernomorskii flot: faktor rasshireniia boevykh vozmozhnostei v zone otvetstvennosti," *Voennaia mysl'*, No. 7, 2017, p. 20).

[83] Burenok and Pechatnov, 2011.

[84] Sterlin, Protasov, and Kreidin, 2019, p. 16. See also Makhnin, 2019, p. 47, which is referenced in Chapter 1 of this report.

[85] D. O. Rogozin, ed., "Operatsiia strategicheskikh sil sderzhivaniia," *Voina i mir v opredeleniiakh*, Book 1, Moscow: Veche, 2017, p. 236.

[86] For discussions of possible limits of advance of Russian Ground Forces along Russia's periphery, see Ben Connable, Abby Doll, Alyssa Demus, Dara Massicot, Clint Reach, Anthony Atler, William Mackenzie, Matthew Povlock, and Lauren Skrabala, *Russia's Limit of Advance: Analysis of Russian Ground Force Deployment Capabilities and Limitations*, Santa Monica, Calif.: RAND Corporation, RR-2563-A, 2020; and Alex Vershinin, "Feeding the Bear: A Closer Look at Russian Army Logistics and the Fait Accompli," *War on the Rocks*, November 23, 2021.

warfighting close to Russia's border and deterrence forces that can range sensitive targets at thousands of kilometers.

This delineation is collapsing for Russia because of the current geographic disposition of opposing forces and the expanding role of conventional PGMs and their delivery platforms across the spectrum of conflict escalation. As a result, Russia may eventually coalesce around a *unified strategic operation* that could entail the

> integrated employment of all available forces and means to destroy the enemy, which makes it possible to achieve fires superiority. Comprehensive destruction of the enemy [will be] realized by the advanced planning of all types of effects, which ensures a gradual transition from strategic deterrence measures to direct fires destruction.[87]

If the Russians previously considered long-range bombers and conventional air-launched cruise missiles (CALCMs) primarily as tools of deterrence, then they could be designated and allocated to conduct a single mission to attack military-economic or civilian targets in a NATO country, for example. As the numbers of munitions increase in the Russian inventory, the potential ways to employ these assets have expanded (see Figure 2.2). But because, for example, strategic bombers have both a conventional and a nuclear mission, and because the platforms and munitions are still relatively limited for Russia, careful planning is required to properly allocate their use (see Chapter 3).

Considering the ongoing force structure expansion in strike platforms and munitions, Russia is in a transition to a spectrum of conflict that can be broken down into three phases (see Figure 2.3). These phases may be interconnected within a future unified strategic operation, although there could be some overlap between them depending on circumstances.[88] The first phase is the conventional struggle for fires superiority—that is, the conventional counterforce phase. The Russians want to achieve fires superiority by destroying or degrading NATO's ability to launch and sustain long-range conventional strikes. In this phase, Russia would likely concentrate on key military targets, such as C4ISR infrastructure and naval and air bases or platforms. We base this conclusion on the prominence of Russian military discourse on "functional destruction," as opposed to prioritization of adversary forward forces.[89] Russian air defenses and EW will attempt to attrit aircraft and missiles, but the Russians consider offensive destruction of military assets related to the NATO aerospace attack as most consequential.

---

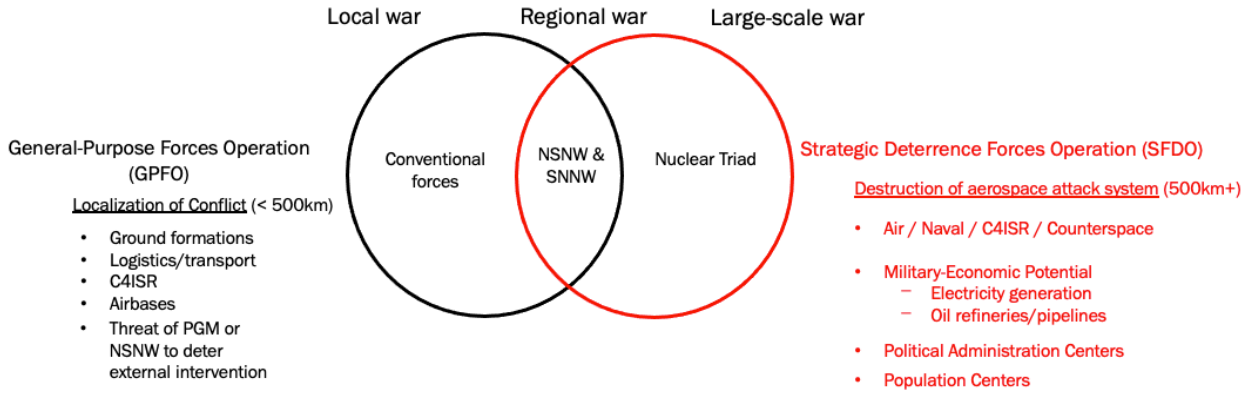
[87] V. B. Zarudnitskii, "Faktory dostizheniia pobedy v voennykh konfliktakh budushchego," *Voennaia mysl'*, No. 8, 2021a, p. 44. For a discussion of fires superiority (*ognevoe prevoshodstvo*) at the tactical level, see I. A. Buval'tsev, O. A. Abdrashitov, and A. V. Garvard, "Razvitie taktiki v sovremennykh usloviiakh," *Voennaia mysl'*, No. 10, 2021, p. 35.

[88] We did not draw our conclusion from Slipchenko's work, but he did suggest conflict phases along these lines in the early 2000s. See Jānis Bērziņš, "The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria," *Journal of Slavic Military Studies*, Vol. 33, No. 3, 2020, p. 364.

[89] Reach et al., 2022.

The second phase is the conventional destruction of NATO's military-economic potential and other critical civilian infrastructure. In this phase, the focus will be on creating "cascading effects" that are highly disruptive to modern life in states participating in the war (e.g., the infrastructure required to supply a large city with fresh water or energy). The final phase, albeit undesirable because of NATO's ability to respond in kind or escalate, is the preemptive employment of nonstrategic nuclear weapons against primarily military but also hard civilian targets followed by the use of strategic nuclear weapons against cities, military-industrial centers, and administrative-political infrastructure.[90]

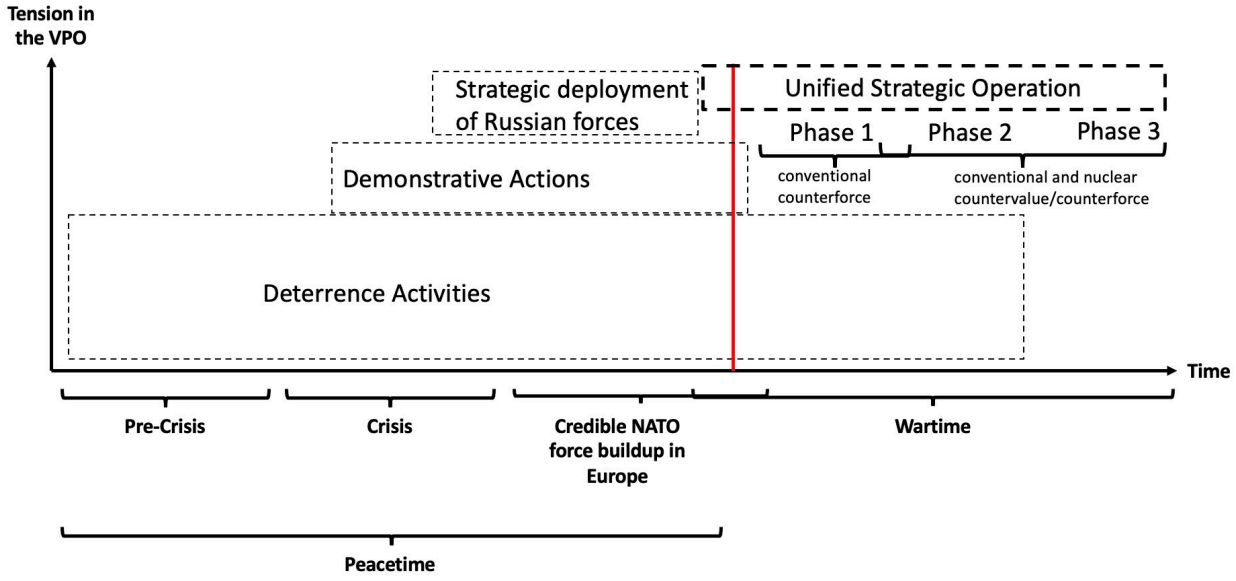
Figure 2.2. Strategic Nonnuclear Forces and the Blending of Strategic Operations



SOURCES: Features information from Burenok and Pechatnov, 2011; A. G. Burutin, G. N. Vinokurov, V. M. Loborev, S. F. Pertsev, and Iu. A. Podkorytov, "Kotseptsiia nepriemlemogo ushcherba: genesis, osnovnye prichiny transformatsii, sovremennoe sostoianie," *Vooruzhenie. Politika. Konversiia*, No. 4, 2010; Danilevich and Shunin, 1992; Makhmut Gareev, "Problemy sovremennoi sistemy voennogo upravleniia i puti ee sovershenstvovaniia s uchetom novykh oboronnykh zadach i izmenenii kharaktera budushchikh voin," *Voennaia mysl'*, No. 5, 2004, p. 67; Gerasimov, 2019; A. A. Protasov, S. V. Kreidin, and Iu. A. Kublo, "Aktual'nye aspekty razvitiia silovykh instrumentov i kontseptsii strategicheskogo sderzhivaniia," *Vestnik Akademii voennykh nauk*, Vol. 3, No. 76, 2021; Rogozin, 2017; and Sterlin, Protasov, and Kreidin, 2019.
NOTE: SNNW = strategic nonnuclear weapons.

[90] Kokoshin et al., 2021, pp. 60–65; and V. N. Kuzmin and N. A. Frolov, "Prognoz tendentsii razvitiia soderzhaniia i kharaktera voennykh konfliktov budushchego i otsenka ikh vliianiia na voenno-kosmicheskuiu deiatel'nost' v mire v XXI veke," *Vestnik Akademii voennykh nauk*, Vol. 1, No. 74, 2021, pp. 36–37.

Figure 2.3. Notional Phases of a Future Unified Strategic Operation in Russian Road to War



SOURCE: Adapted from O. I. Ostapenko, S. V. Baushev, and I. V. Morozov, *Informatsionno-kosmicheskoe obespechenie gruppirovok voisk (sil) VS RF*, St. Petersburg, Russia: Liubavich, 2012, p. 86.
NOTE: VPO = military-political situation.

This sequence aligns closely with what Danilevich and Shunin postulated in 1992:

> The employment of strategic nonnuclear weapons can be carried out sequentially, by increasing the degree of threat along the "stages" of deterrence. Thus, at the first stage of a conventional conflict, strategic nonnuclear munitions could target military facilities, and then, if necessary, against military-economic and civilian infrastructure. If such measures are insufficient and if the war continues, it is not ruled out that strategic nonnuclear forces will strike at strategic nuclear forces, nuclear power plants, and chemical enterprises.[91]

Andrei Kokoshin, General (Ret.) Iurii Baluevskii (former Chief of the General Staff), General-Colonel (Ret.) Viktor Esin (former senior Strategic Rocket Forces commander), and General-Colonel (Ret.) Aleksandr Shliakhturov (former head of the Main Intelligence Directorate [GRU], Russia's military intelligence service) published a work in 2021 that described a conflict escalation ladder roughly corresponding with these phases.[92]

The final two phases could form the broad outline of the SDFO, which is a blend of conventional and nuclear strikes against critical infrastructure. According to a Russian military dictionary published in 2017, the SDFO is

> a prospective type of strategic action of the Armed Forces using strategic strike weapons with conventional payloads, as well as a strictly limited number of

[91] Danilevich and Shunin, 1992, p. 53.

[92] Kokoshin et al., 2021, pp. 60–65.

> strategic nuclear strikes to inflict unacceptable damage on the aggressor and deter him from dangerous actions. It can be carried out by a small force to prevent and disrupt an impending attack in the form of a demonstration of military power or with full-scale use of all means in the event of aggression. [The SDFO] is being developed along the lines of the operation of strategic nuclear forces, but in other forms as appropriate means of combat are created [i.e., greater numbers of conventional PGMs, hypersonic missiles, and perhaps cyber weapons]. In the future, this operation can use both nuclear weapons with limited fallout and conventional high-precision weapons on various platforms, as well as strategic reconnaissance-strike systems.[93]

Russian capacity to sustain the first phase is a key factor to consider. As Danilevich emphasized 30 years ago—and it remains relevant today—the quantitative requirements to inflict sufficient conventional damage on primarily military targets in Europe and beyond are likely to be steep. In the early 2000s, Russian military strategist Vladimir Slipchenko estimated that Russia would require at least 9,000 standoff munitions—and potentially up to 50,000–70,000—in future war.[94] Likely falling well short of Slipchenko's lower bound as of late 2021 (see Chapter 3), Russia could turn to the conventional portion of the SDFO relatively early given limited numbers of munitions to attack distant force potential. At that point, the war could quickly take on a more devastating form focused on civilian infrastructure.[95]

In observations of previous U.S. conflicts in the 1990s, Slipchenko and Gareev noted how the Americans concentrated their limited and expensive precision munitions on critical civilian infrastructure, as opposed to ground forces.[96] They also projected that the United States would be able to launch 60,000 standoff missiles—a massive estimate—over a 60-day period by 2030, giving the Americans greater flexibility in targeting. Russia's modern precision strike complex as of 2021, from a capacity standpoint, is closer to where the United States was in the late 1990s, when the United States purportedly launched around 1,000 guided munitions against Serbian air defenses and civilian infrastructure.[97] To be sure, these Russian assessments occurred prior to Russian efforts beginning in 2011 to build out conventional strike capacity. But Russian production, even as of 2020, has not approached what would be required according to Slipchenko's estimates and past U.S. campaigns.[98] As Sterlin, Protasov, and Kreidin wrote in 2019, "[S]trategic nonnuclear weapons are not a rational military-economic alternative to nuclear weapons in solving the tasks of global and regional strategic deterrence."

---

[93] Rogozin, 2017, pp. 235–236.

[94] As cited in Bērziņš, 2020, p. 365.

[95] Valeriy Akimenko, *Russia and Strategic Non-Nuclear Deterrence: Capabilities, Limitations and Challenges*, London: Chatham House, July 2021, p. 13.

[96] Slipchenko and Gareev, 2007, p. 18.

[97] See Chapter 3.

[98] Reach, Blanc, and Geist, 2022.

The Russians are attempting to build out greater capacity to wage the first phase of the conventional war. Long-range conventional fires—augmented by electronic attack, cyber weapons, counterspace assets, and the threat of nuclear escalation—against military and military-industrial targets are the modern version of *deep operations*.[99] Preemptive nuclear strikes or multiple ground-centric fronts lurching toward the western shores of NATO are being replaced with concepts to inflict damage against critical targets to seize the initiative and win the conventional war before NATO can gather itself for a response.[100] As senior Russian researchers noted, "In a crisis situation, long-range PGMs can be used at the initial stage of the SDFO in order to counter the threat of escalation of a conventional military conflict . . . into a nuclear conflict and to force the enemy to de-escalate and end the confrontation."[101] This idea resembles that of Ogarkov, who wanted to race ground forces quickly into enemy territory, limit NATO's ability to employ tactical nuclear weapons, and disrupt the transition from conventional to nuclear war.

The question of Russia's decision to preemptively escalate to nuclear use is not possible to answer definitively; nuclear escalation is ultimately a political decision. Russia has operational concepts and means for this course of action, which is explicitly allowed by the Military Doctrine when the president decides that the existence of the state is at risk. But Russia also has incentive to convince the West of its readiness to escalate in any number of conflict scenarios that are not existential. In 2012, a former commander of the Aerospace Defense Forces cast doubt on the utility of broad nuclear employment but did allow for the possibility of limited nuclear use:

> At the end of the twentieth century, it was generally recognized that in full-scale forms [the operation of strategic nuclear forces] was dangerous for both sides, could lead to a global ecological catastrophe—a "nuclear winter" and "nuclear night"—and therefore, in practical terms, such an operation should be ruled out. Its role remains as a symbol of deterring the aggressor. At the same time, under certain circumstances, it cannot be ruled out that the operation of strategic nuclear forces [now folded into the SDFO] can be conducted with a strictly limited number of means with a deliberate minimization of the number of targets and strike methods to avoid unpredictable impact on the territory of one's own country and the natural environment.[102]

---

[99] V. V. Kruglov and A. S. Shubin, "O vozrastaiushchem znachenii uprezhdeniia protivnika v deistviiakh," *Voennaia mysl'*, No. 12, 2021, p. 31.

[100] Kofman, Fink, and Edmonds, 2020; N. P. Zubov, "Sovershenstvovanie form primeneniia i sposobov deistvii aviatsionnykh formirovanii voenno-vozdushnykh sil," *Vestnik Akademii voennykh nauk*, Vol. 3, No. 76, 2021, p. 50.

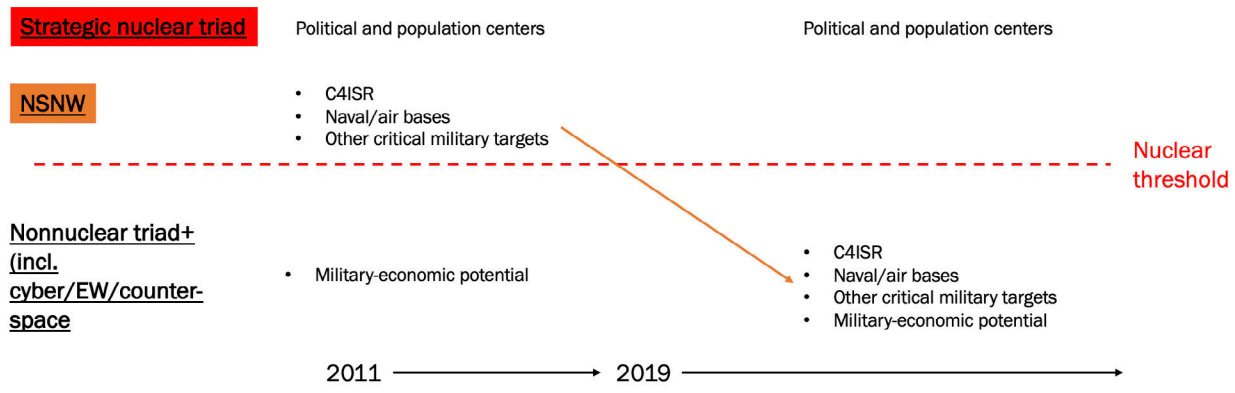
[101] A. A. Protasov, V. A. Sobolevskii, V. V. Sukhorutchenko, and A. S. Borisenko, "Metodicheskoe obespechenie vyrabotki zamysla primeneniia VTO bol'shoi dal'nosti v operatsiiakh (boevykh deistviiakh)," *Voennaia mysl'*, No. 10, 2011, p. 39. See also Rogozin, 2017.

[102] Ostapenko, Baushev, and Morozov, 2012, p. 99.

To a certain extent, this echoes the definition of the SDFO given earlier.[103]

There are two additional points to consider. First, one of the reasons Russia is pursuing greater conventional theater strike capability is the questionable credibility of nuclear use in response to a conventional attack (by a strategic nuclear peer) that does not threaten the existence of the Russian state (i.e., NATO actions that are different from those in Iraq in 2003 or Libya in 2011, in which the state did cease to exist). Second, the Soviets saw a close connection between the achievement of strategic nuclear parity and the greater likelihood of conventional war. If the use of nuclear weapons cannot conceivably improve the situation because of nuclear retaliation, then there is little benefit in escalating to nuclear use. As Andrei Kokoshin noted in 2014, "Many experts and politicians reasonably question the logic of lowering the nuclear threshold [in the 2010 Military Doctrine], especially when applied to a situation in which 'adversaries' of comparable nuclear potential are opposing each other."[104] We believe that these factors influenced remarks by Gerasimov, who expressed the intention to transition to a military deterrent that is more reliant on conventional capabilities over the long term (see Figure 2.4).[105] In the meantime, nonstrategic and strategic nuclear weapons serve as a useful peacetime deterrent against NATO. Their utility in wartime will hopefully remain an open question.

Figure 2.4. Russian Transition to Increased Role of Conventional Systems in Unified Strategic Operation at the Regional Level (European Theater)



SOURCE: Features information from Burenok and Pechatnov, 2011, pp. 150–151; Gerasimov, 2017a; Protasov, Kreidin, and Kublo, 2021, pp. 44–45; Sterlin, Protasov, Kreidin, 2019, p. 15.

[103] Rogozin, 2017, pp. 235–236.

[104] A. A. Kokoshin, 2014, p. 202.

[105] Valerii V. Gerasimov, "O khode vypolneniia ukazov prezidenta Rossiiskoi Federatsii ot 7 maia 2012 goda N603, 604 i razvitie vooruzhennykh sil Rossiiskoi Federatsii," *Voennaia mysl'*, No. 12, 2017a, p. 8.

NOTE: Russia will build out its conventional capability to accomplish the majority of offensive destructive tasks in a unified strategic operation. Nuclear weapons (likely nonstrategic nuclear) probably will be phased out over decades. Implicit in phasing out (or having a lesser role for) nonstrategic nuclear weapons is the idea that a conventional destructive capability is more credible in most scenarios than the threat of nuclear escalation against a nuclear adversary, such as NATO.

As in the past, organization of C2 of multiple JSCs—West, South, North, and Central—will be a critical initial task for a unified strategic operation. Ogarkov experimented with what was called a *theater of military operations command*, or a theater commander and staff responsible for the coordination of perhaps two to four fronts. This C2 layer was an intermediary between front commanders and the high headquarters (Stavka) of the General Staff. The Soviets sought to eliminate the problem of front commanders not effectively coordinating their actions under a unified plan. One analyst has suggested that Russia could revive the theater command concept to coordinate JSC West and South at a minimum.[106] The late General Makhmut Gareev, formerly the head of the Military-Scientific Committee of the Soviet General Staff, highlighted some of the problems with Ogarkov's theater command:

> Experience had shown that the most rational approach was the participation of the theater commands in the advance planning of strategic operations under the leadership of the General Staff and the organizational work of preparing for and executing operations. In the course of operations, the most difficult decisions should have been made by the High Command of the Supreme Commander-in-Chief taking into account the recommendations of the theater commands, and then directives to the fronts should have been passed through the General Staff. . . . Strictly following this protocol for decisionmaking and operational planning—Stavka (General Staff) → Theater Command → Front—command and control was bogged down and the operational utility of directives reduced, which was unacceptable in the conduct of operations at that time.[107]

Despite such challenges, the Russians will need to (or already have) come up with a satisfactory solution to the C2 of multiple JSCs to conduct a theater strike campaign across Europe and into the United States, as well as in space and cyberspace.

In his analysis of Russian strategic exercises from 2009 to 2016, General-Major I. A. Fedotov cited additional C2 challenges of a modern joint force whose mission was evolving from ground-centric to strike-centric:

> Attempts to effectively resolve issues of planning and C2 of new force groupings of Air Force, Air Defense, and Navy that were not an integral part of the C2 system in the past not only did not lead to the desired result, but in fact increased the volume of functional obligations of those responsible for the command apparatus of the OSK [Joint Strategic Command].

---

[106] Greg Whisler, "Strategic Command and Control in the Russian Armed Forces: Untangling the General Staff, Military Districts, and Service Main Commands (Part Two)," *Journal of Slavic Military Studies*, Vol. 33, No. 1, 2020, p. 101. See also Kipp, 1991, p. 631.

[107] Makhmut Gareev, "Ob organizatsii voennogo upravleniia na strategicheskikh napravleniiakh," *Natsional'naia oborona*, No. 10, 2010.

> Information overload of the command staff on account of the increase of functional groups led to an imbalance in the work of the OSK staff during operational planning and, as a result, led to incredibly poor decisions for the practical resolution of tasks.
>
> The commander of the [OSK], as a rule, is a representative of the tank or motor rifle forces and has a thorough understanding of the structural elements of the OSK in commanding the Ground Force grouping. However, at the present time he is in no way prepared to effectively command a force grouping of Air Force, Air Defense, and Naval forces that are included in the [OSK].[108]

In 2017, General-Colonel Sergei Surovikin (who has since been promoted to four-star general) became the head of the VKS. Surovikin was a career Ground Forces officer who formerly commanded the 20th Combined Arms Army. Considering Fedotov's observations above, the Russians apparently were seeking creative solutions to the problem of "joint" competency. Instead of appointing a VKS officer to lead the Ground Forces or the General Staff, however, the Russians moved a Ground Forces officer into the VKS, potentially paving the way for Surovikin to become the next Chief of the General Staff with a better background in air-ground coordination. This solution was not surprising given Russia's military history, traditions as a land power, and possible land conflicts along its southwestern borders.

In sum, multiple JSCs will be required to participate in a future strategic operation based on Russian expectations of NATO actions of future war, which could span from the Arctic to Crimea in the initial period of war. The U.S. experience in C2 of a joint force has shown that this is a highly complex task from many perspectives.[109] And there are several outstanding questions for Russia in this area. How will C2 be organized, and how will coordination between the JSCs occur? How robust and reliable is inter-JSC communication? It is possible that many of these strategic C2 requirements are managed within the Combat Command Center of the National Defense Management Center, which could serve as the theater command, with the relevant JSC commander (or commanders) subordinate. Regardless, these linkages are important for current large-scale operations or a future Russian unified strategic operation, particularly as they relate to any potential Russian theater strike campaign drawing on disparate assets across the JSCs to attack critical targets in Europe and the United States and relay the aerospace threat picture, battle damage assessments, and other vital information.

---

[108] I. A. Fedotov, "Napravleniia razvitiia operativno-strategicheskogo komandovaniia voennogo okruga na sovremennom etape stroitel'stva Vooruzhennykh Sil Rossiiskoi Federatsii," *Vestnik Akademii voennykh nauk*, Vol. 4, No. 57, 2016, p. 67.

[109] David E. Johnson, *Learning Large Lessons: The Evolving Role of Ground Power and Air Power in the Post–Cold War Era*, Santa Monica, Calif.: RAND Corporation, MG-405-1-AF, 2007; Michael Spirtas, Thomas-Durell Young, and S. Rebecca Zimmerman, *What It Takes: Air Force Command of Joint Operations*, Santa Monica, Calif.: RAND Corporation, MG-777-AF, 2009.

Conclusion

Every Soviet strategist going back to the 1920s has grappled with how to defeat an economically and technologically superior alliance, and each era of warfare presented its own unique challenges. Unlike his pre–nuclear era predecessors, Ogarkov faced an economically and technologically superior alliance with thousands of kilometers of strategic depth and a nuclear arsenal that could achieve a decisive outcome in a short time. To overcome this military problem, Ogarkov and the Soviet General Staff developed operations that required a huge military force to conduct preemptive conventional operations deep into NATO territory. It is questionable, and indeed Gorbachev concluded so, that this strategy was sustainable within the economic constraints of the late Soviet Union.

Today, the Russian General Staff and, in particular, the Main Operations Directorate must develop an operational concept that can rapidly engage NATO at the regional and global levels within the economic constraints of the Russian Federation. The same pressures that Ogarkov faced toward offense and rapid destruction and the questionable utility of nuclear weapons against a nuclear peer are still relevant. Gerasimov, like Ogarkov, needs conventional mass and speed to preempt NATO and inflict sufficient damage deep into NATO territory to alter the correlation of forces, to prevent the use of nonstrategic nuclear weapons against Russia, and to change the political calculus in NATO capitals. Russia appears to have gone some way in achieving high readiness, but the question of mass (strike or attack capacity) is arguably as important. Can Russia afford to build and sustain the conventional capacity it needs to convince NATO that the Russian military can conduct decisive destructive operations in the initial period of war in a theater where the main forces are territorially divided?

A future unified strategic operation could be a middle ground between the extremes of conventional strategy for large-scale operations (see Table 2.3). Or, it could be an economically sensible compromise that is militarily ineffective. It might not be possible to have it both ways. In broad terms, the middle ground involves exploiting technology to generate enough conventional capacity to destroy the adversary's system of warfare, as opposed to its component parts—e.g., land forces. This reduces the economic burden of building a force that is sufficiently superior to NATO in multiple areas. It is a force centered on the principles of preemption in crisis and asymmetric targeting of military and civilian infrastructure to create disruptive cascading effects to level the playing field with a superior alliance. The unified strategic operation is a forward-looking concept to simplify the planning and employment of a large joint force that is equipped with large amounts of conventional strike and electronic attack potential but also can reserve enough combat potential to cross the nuclear threshold.

Table 2.3. Trade-Offs in Soviet and Russian Large-Scale Operational Concepts

	Strategic Defense and Attrition	Middle Ground (preemptive conventional destruction with credible defense)	Strategic Offensive and Destruction
Proponent	Svechin	Gerasimov	Ogarkov
Era of warfare	1910s–1940s Ground-centric, large armies	1990s–present Aerospace-centric, small armies, conventional long-range PGMs, nuclear weapons	1950s–1980s Ground-centric, large armies, nuclear weapons
Advantages	Less manpower intensive, low cost, effective	Less manpower intensive, lower cost, heavy damage inflicted in initial period of war	Rapid destruction of enemy force, creates escalation dilemma for nuclear opponent, effective[a]
Disadvantages	High casualties, high levels of damage across Russian territory	Escalatory, high munitions and tech requirements, credibility deficit, questionable effectiveness	High personnel requirements, high cost

SOURCE: Features information from Reach, Blanc, and Geist, 2022.
[a] The assessment of "effective" is based on the following standard: NATO believed it might have to resort to nuclear weapons early in war (which, presumably, it did not want to do).

To investigate the correspondence between Russian force structure and the operational tasks introduced above, and to understand recent statements by senior Russian military officers, we need a firmer grasp of where Russia is in a transition to a force that has the conventional "mass" to wage the type of war Russia believes it would need to fight if deterrence failed. The remainder of the report begins to get into the details.

3. Russia's Conventional Precision Strike Assets in a Notional Unified Strategic Operation

Senior Russian military officers continually discuss the role and importance of long-range precision strike in large-scale operations in modern and future war. These same officers have highlighted the limitations of Russian long-range precision strike in a regional war in Europe or a global war stretching into the United States. This is a critical contradiction, and it calls for deeper analysis into why Russian officers express this view. This issue of Russian conventional long-range strike capacity is at the heart of the evolution of Russian operational thinking, and the remainder of this report is in some way related to this central factor.

This chapter outlines the primary tasks for strategic nonnuclear offensive forces in a notional unified strategic operation, the capabilities and disposition of Russia's strategic nonnuclear deterrence forces as of 2021, and how those forces might change qualitatively and quantitatively to 2030. Because air- and sea-based nonstrategic nuclear weapons are considered part of strategic offensive forces, we include a brief discussion of the roles and capabilities of nonstrategic nuclear weapons if conflict de-escalation or cessation cannot be achieved conventionally. Finally, the chapter offers some conclusions on the capabilities of Russia's conventional precision strike systems in support of the tasks described in the previous chapters.

Scope Note and Data Availability Challenges

Our analysis focuses on priority tasks for Russian strategic offensive forces as derived from Russian strategy, military science literature, and leadership statements. Finding specific numbers for Russian precision strike inventory and production capacity from open-source Russian reporting proved to be our greatest challenge. Russian officials do not provide comprehensive information about their military forces, nor do they discuss inventory levels or production or procurement patterns with specifics. Other sources of information in Russia are also declining; in 2021, Russia's Federal Security Service (FSB) put forth a draft law to label any entity or individual reporting on Russian military "locations, numbers, and armaments" a foreign agent.[110] Furthermore, Russian military strategy or grey literature writings do not provide details of targeting strategies in a conflict with NATO; such materials would most likely be classified documents in the Russian military.

Russian officials do not speculate on the precise number of weapons in or the composition of their conventional precision strike arsenal—especially what they might need to successfully

[110] "Russia's FSB Unveils Broad List of Topics that Could Result in 'Foreign Agent' Label," RadioFreeEurope/RadioLiberty, October 1, 2021.

achieve strategic operations, such as a unified strategic operation against the United States alone or NATO as a bloc. We can only interpret the few data points that are available from military science literature, Russian news sources, and Russian launch platforms, about which there is more information. For example, authors offer vague anecdotes, such as, "The number of land-based, sea-and air-launched long-range cruise missiles grew by 37 times . . . between 2012 and 2020," providing no numbers but specifically highlighting the Kh-101 and Kalibr submarine-launched cruise missiles (SLCMs).[111] These systems did not enter the force until 2013 or later, so the starting number was quite small. Therefore, our analysis of available munitions and platforms of Russia's strategic nonnuclear deterrence forces is a composite estimate derived from Russian news reports where available, military science literature, Western analysis, and our own order-of-battle analysis of Russia's force structure. We consider the inherent tension of shared launch platforms between Russia's conventional weapons and nuclear forces, but we do not have precise information on how Russia would select forces for conventional versus nuclear missions.

Strategic Nonnuclear Offensive Forces

The unified strategic operation concept is a response to forecasted U.S. or NATO warfighting concepts of operations.[112] Russian strategists have assessed for over a decade that the United States and NATO are attempting to create their own "unified combat information space" by the early 2030s.[113] In their analysis, space, air, sea, and land domains and operations will become increasingly integrated and will use precision strike forces, ISR, EW, and strikes in depth. The future theater will be characterized by its large scale. By the 2030s, 80 percent of Russian territory and more than 60 percent of Russian military-economic potential targets will be within NATO conventional strike range. The conflict will be intense but of brief duration (60–190 days), conducted by assets that can form force groups to strike anywhere on the globe.[114] NATO is developing unmanned aerial systems (UAS) and hypersonic missiles to maintain a strategic advantage in this future environment.[115] Others believe that, to respond to U.S. Prompt Global Strike or global missile defenses, Russia must "ensure efficient allocation of enemy targets between nuclear forces and forces with strategic nonnuclear weapons" as part of a coordinated plan under the General Staff.[116]

---

[111] "Number of Long-Range Cruise Missile Carriers in Russia Up 13 Times Since 2012," TASS, December 22, 2020.

[112] Makhnin, 2019; Sterlin, Protasov, and Kreidin, 2019.

[113] Burenok, 2009, pp. 14–16.

[114] Burenok, 2009, pp. 14–16.

[115] Burenok, 2009, pp. 14–16.

[116] Ivanov, Savitskii, and Makarov, 2020, p. 248.

To defend against this type of attack, Russian strategists recommend that their own military develop a strategy and system of unified operations as well. By focusing on the integrated employment of all of Russia's available forces, Russia might be able to generate increased efficacy and efficiency in their operations. This theoretically might allow Russia to retain or regain fires superiority without needing to find numerical parity with the United States.

General-Major Sterlin and colleagues explained in 2019 that Russia's current operations and planning model divide Russia's deterrence forces into three areas: (1) *global deterrence*, which is the responsibility of nonstrategic nuclear weapons and strategic nuclear weapons; (2) *regional deterrence*, which is achieved by nonstrategic nuclear weapons and strategic nonnuclear deterrence forces to de-escalate and suppress major nonnuclear threats; and (3) *local deterrence*, which is achieved through the presence of strategic nonnuclear weapons and general-purpose forces to block local nonnuclear threats and prevent the nuclear threshold from sliding into the lower-echelon local wars and armed conflicts.[117]

Sterlin suggested several tasks for strategic nonnuclear weapons that, as in the Ogarkov era, emphasize disrupting the linkage between conventional and nuclear war in the early phases. These include *regional tasks*, such as halting enemy military actions at the prenuclear phase and attacking enemy nonnuclear forces to create "additional opportunities for de-escalating military actions before crossing the nuclear threshold in regional wars."[118] *Global tasks* for strategic nonnuclear forces consist of denying or degrading the access of enemy forces (such as in-transit U.S. Navy assets capable of launching ballistic missile defense or long-range cruise missiles) and degrading enemy combat capabilities at long ranges to maintain a sufficient retaliatory capability for Russia's strategic nuclear forces. Other tasks at the regional and global levels involve a controlled counter-value escalation of hostilities—that is, attacking NATO fuel and energy facilities to degrade combat power or political control or to create chaos to compel the enemy to halt the conflict.[119] These strikes are all envisioned as conventional methods to raise the consequences to an enemy before resorting to nuclear strikes to compel an end to the conflict.

Some of these weapons and launch platforms cross into different deterrence tasks and echelons. In Sterlin's view, the unified strategic operation would be a better method to centrally manage assets to solve diverse operational problems. This chapter's analysis focuses on the conventional strike tasks listed in Chapter 1 and the use of nonstrategic nuclear weapons that we mentioned briefly in Chapter 2:

- *Conventional strikes to cause "functional destruction" of an enemy's strike power.* Specifically, this means targeting C4ISR infrastructure and enemy naval platforms that can launch long-range strikes and destroying enemy aviation and UAS.

[117] Sterlin, Protasov, and Kreidin, 2019, pp. 7–17.

[118] Sterlin, Protasov, and Kreidin, 2019.

[119] Sterlin, Protasov, and Kreidin, 2019.

- *Conventional strikes against military-economic potential and other critical civilian infrastructure.* Russian sources often focus on energy infrastructure and industrial targets using kinetic means (nonkinetic means will be examined in subsequent chapters of this report).
- *The use of nonstrategic nuclear weapons against military facilities or critical civilian infrastructure if strategic nonnuclear deterrence forces fail to end the conflict or restrain it to the conventional level*. Strategic nuclear weapons would be used against an enemy's nuclear forces and population centers in the event of a general nuclear war, or in limited employment to reduce casualties and environmental fallout.

Each of these tasks has a different targeting strategy, and each is intended to achieve different operational effects. First, *demonstration strikes* can occur at any point in a conflict and are intended to show Russia's capability and resolve to win or escalate if necessary. Targets for demonstration strikes include enemy forces in transit to conflict areas, naval forces in active areas of operation, forces deploying to border areas, and other individually selected targets. *Counterforce* targets, in the Russian understanding, are military targets that, if damaged or destroyed, will allow Russia to gain or regain the initiative and halt enemy aggression; this set of targets likely consists of forces in theater, originating bases from which air or naval forces launch, and forces in transit to a theater of operations. Points of debarkation at airports or ports, units on the march, airfields, warehouses, repair bases, and weapon storage facilities are all valid military targets in this context.[120] *Countervalue deterrence* targets include critical targets and enemy economic targets that create damage roughly on par with nuclear forces. These targets consist of state and municipal government, information or telecommunications sites, defense industrial sites, hazardous materials facilities, and other locations that cause large-scale secondary damaging factors (e.g., transportation infrastructure).[121] If these targets are damaged or destroyed, they might limit NATO's control and ability to sustain conflict and might affect NATO's will to fight.

Task 1: Attacking an Enemy's Strike Power to Achieve Fires Superiority and Create Functional Destruction

This and subsequent sections build on the conventional strike tasks and context for future war that we described in Chapter 1.[122]

Sterlin, Protasov, and Kreidin, 2019, argued that Russia's strategic nonnuclear weapons would be most efficient at such key tasks as gaining air and naval dominance, isolating combat zones, disorganizing C2 of enemy groupings, and destroying key military infrastructure,

---

[120] Durnev and Sviridok, 2021, p 57.

[121] Durnev and Sviridok, 2021.

[122] For an additional discussion of counter-military strikes in the opening phase of the war, see V. I. Poletaev and V. V. Alferov, "O neiadernom sderzhivanii, y ego rol' i mesto v visteme stategicheskogo sderzhevaniia," *Voennaia mysl'*, No. 7, July 2015.

particularly in the early stages of a conflict. Key tasks to degrade or destroy NATO airpower potential will likely occur in the initial period of war. Russian airstrikes will target critical infrastructure (C2 and logistics systems), air defense systems, airfields, and strike aircraft.[123] Although some Russian analysts note that runways are "effectively disabled when guided aerial bombs are used" instead of standoff PGMs, this assessment seems to sidestep the issue of aircraft survivability.[124]

Nevertheless, if these assets are used to blunt or degrade an enemy's airstrike power, they would also likely target NATO runways, satellite communications (SATCOM) or other navigation downlinks, air traffic control towers, and local point air defenses.[125] They might also be used to strike related energy facilities, such as fuel bladders or power plants.[126] This would cause NATO to operate from remote or unfamiliar airfields, thereby reducing the potency of its strike potential. Other missions for Russian bombers include firing air-launched cruise missiles (ALCMs) or other munitions on enemy groups of troops (most likely stationary targets, such as headquarters or troop encampments) and airfields.[127] Tactical aviation also has a role in destroying enemy formations, other ground targets, helicopters, or parked aircraft within tactical or operational tactical depth. Air-to-air interceptors are designed to attack airborne targets and intercept enemy cruise missiles or large UAS.[128] Russia's navy would use its anti-ship cruise missiles (ASCMs) to attack inbound enemy surface action groups, particularly aircraft carriers and ships capable of launching land-attack cruise missiles (LACMs) or ballistic missile interceptors.[129]

NATO forward forces are not necessarily the first targets. Russian emphasis on the eventual transition from targeting forward forces to achieving the functional destruction of a warfighting system suggests that the focus would be on *critical objects*, defined as objects or targets that, if defeated, would most likely have follow-on effects to a greater number of component parts of the aerospace campaign.

---

[123] O. V. Korol and N. L. Romas, "Form of Military Actions: On the Meaning of the Category," *Military Thought*, East View Information Services, No. 3, 2008; S. V. Kuralenko, "Tendencies in the Changing Character of Armed Struggles in Military Conflicts in the First Half of the 21st Century," *Military Thought*, East View Information Services, No. 11, 2012, pp. 40–46.

[124] B. Rog, "Strategiskaya zadacha aviatsii," *Armeiskii Sbornik*, No. 7, 2012.

[125] S. G. Chekinov, V. I. Makarov, and V. V. Kochergin, "Zavoevaniiu i uderzhaniiu gospodstva v vozdukhe (v vozdushno-kosmicheskoi sfere) - dostoinoe mesto v razvitii rossiiskoi voennoi teorii i podgotovke voisk (sil)," *Voennaia mysl'*, No. 2, February 2017.

[126] S. N. Borisko and S. A. Goremykin, "Analiz sostoianiia Vozdushno-kosmicheskikh sil Rossii. Perspektivy razvitiia," *Voennaia mysl'*, January 1, 2019.

[127] Borisko and Goremykin, 2019.

[128] Borisko and Goremykin, 2019.

[129] Samuel Charap, Alice Lynch, John J. Drennan, Dara Massicot, and Giacomo Persi Paoli, *A New Approach to Conventional Arms Control in Europe: Addressing the Security Challenges of the 21st Century*, Santa Monica, Calif.: RAND Corporation, RR-4346, 2020.

Planning and Requirements for Targeting

Russia has a variety of precision-guided cruise and ballistic missiles to strike the targets discussed above. As Table 3.1 shows, many of Russia's theater strike assets, such as the SS-26 short-range ballistic missile (SRBM) or the SSC-7 ground-launched cruise missile (GLCM), have ranges of less than 500 km. These types of systems would be especially useful for targeting NATO military facilities close to Russian borders, in the Baltics, Poland, and perhaps the Black Sea region. Russia would then be able to save its longer-range munitions, such as the Kh-101 LACM and the Kalibr SLCM, for counterforce targeting 500–4,000 km from Russian borders.

Table 3.1. Russian Conventional Precision Strike Munitions as of 2021

Name (NATO name)	Type	IOC	Range	Carriers (salvo size)
Kh-555 (AS-22 Kluge)	ALCM	2012	2,500 km	Tu-95MS (6) Tu-160 (12)
Kh-101 (AS-23a Kodiak)	ALCM	2013	4,000 km	Tu-22M3M (4–6) Tu-95M (6–10) Tu-160 (12)
Kinzhal (AS-X-24 Killjoy)	ALBM	2019	2,000 km (MiG)–2,900 km (Tu-22M3M)	MiG-31BM (1), MiG-31K (1), Tu-22M3M (4), Su-57 (1)
3M54 (SS-N-27A Sizzler)	ASCM	1987	220–660 km	Severodvinsk (32), Gorshkov (16), Grigorovich (8)
P-800 Oniks (SS-N-26 Strobile)	ASCM	2002	120–600 km, depending on profile	Oscar II (24) Severodvinsk (16) Multiple surface ships (4–8)
Kh-32 (AS-4a)	ASCM	2016	600–1,000 km	Tu-22M3M (3), possibly TU-95 (N/A), Su-30SM (1) in future
Kh-35U (AS-20 Kayak)	ASCM and LACM	2015	260 km	Su-34, possibly Su-35S, Tu-95, Su-57
K-300P Bastion (SSC-5 Stooge)	CDCM	2010	300 km ASCM role, 450 km land-attack role	SSC-5 TELs
3K60 Bal (SSC-6 Sennight)	CDBM	2008	120–260 km ASCM	SSC-6 TELs
9K723-M (SS-26 Stone)	SRBM	2015	250–499 km	Iskandr TELs, 12 brigades (132–144 launchers)

Name (NATO name)	Type	IOC	Range	Carriers (salvo size)
9M729 (SSC-7 Southpaw)	GLCM	2013	400–500 km	Iskandr TELs, 12 brigades (132–144 launchers shared with SS-26)
9M729 (SSC-8 Screwdriver)	GLCM	2017	2,000–2,600 km	Modified Iskandr launcher TELs (4–5 battalions estimated)
Tochka (SS-21 Scarab)	SRBM (in storage/deactivated)	1975	70–120 km	Tochka TELS (12 remaining)

SOURCES: Features information from International Institute for Strategic Studies, *The Military Balance 2021*, London, 2021; Fredrik Westerlund and Susanne Oxenstierna, eds., and Gudrun Persson, Jonas Kjellén, Johan Norberg, Jakob Hedenskog, Tomas Malmlöf, Martin Goliath, Johan Engvall, and Nils Dahlqvist Guden, *Russian Military Capability in a Ten-Year Perspective—2019*, Stockholm: Swedish Defence Research Agency, FOI-R--4758--SE, December 2019. Weapon system data were retrieved between September 2021 and March 2022 from multiple sources: the International Institute for Strategic Studies, the Swedish Defence Research Agency, and Janes publication series, such as *Weapons: Air Launched* and *Missiles and Rockets*.
NOTE: ALBM = air-launched ballistic missile; CDCM = coastal defense cruise missile; IOC = initial operational capability; N/A = not applicable; TEL = transporter, erector, launcher.

Because precise Russian targeting information and calculations of weapons per target are not available, we reviewed available information from U.S. operations, other Western analysis, and Russian military science discussions as available, as a proxy to estimate the types of missile expenditures needed against enemy military targets. We first wanted to survey weapons expenditure and targeting using available real-world examples to build our assumptions for weapons expenditure in a unified strategic operation. We considered U.S. military strikes in Operation Desert Storm (1991), operations in the former Yugoslavia in the 1990s, Operation Iraqi Freedom (2003), Operation Odyssey Dawn (2011), and others.

This information is relevant also because Russian strategists often assess how the United States conducts operations, and their assessments have likely informed aspects of Russian strike planning. At times, Russian estimates of U.S. operations are fairly accurate. For example, it was noted that in Operation Desert Storm, the United States used 300 Tomahawk Land Attack Missiles (TLAMs) and CALCMs, a number that is not far off official U.S. estimates.[130] Russian estimates of U.S. strikes on Syria are another example. Other Russian analysis overstated U.S. capabilities in the campaign against the former Yugoslavia in the late 1990s by a significant margin; Russian analysts noted that 1,500 missiles were launched against 900 military and economic targets.[131] In reality, U.S. government documents state that the United States fired around 218 Block III TLAM-Conventional (TLAM-C) and TLAM-Dispenser missiles and 656 Joint Direct Attack Munitions (JDAMs) during this conflict and had around 150 total CALCMs

[130] U.S. General Accounting Office, *Cruise Missiles: Proven Capability Should Affect Aircraft and Force Structure Requirements*, Washington, D.C., GAO/NSIAD-95-116, April 1995.

[131] Slipchenko and Gareev, 2007, pp. 26–27.

in its inventory as of 1999.[132] In Operation Odyssey Dawn, the United States and its allies used around 3,800 PGMs and similar numbers of laser-guided bombs over time; 654 were U.S. ALCMs and SLCMs launched over the course of ten days.[133] During the opening days of this campaign, the United States fired 120 Tomahawk missiles against 20 Libyan military and air defense targets in 2011.[134]

Using available sources and information on Russian weapon characteristics, we estimate that, if Russian forces were to target airfields, they would most likely need around 30–35 cruise missiles to degrade a single airfield's capabilities, with a high-end estimate of up to 60 cruise missiles, according to Russian and Western estimates and recent historical examples, such as the U.S. Tomahawk strike against the Shayrat Air Base in Syria.[135] Our understanding of U.S. targeting in modern campaigns and analysis by the Swedish Defence Research Agency (FOI) suggest that, to target such military facilities as unhardened radar locations or C2 links, Russia might need anywhere from one to five cruise missiles per structure (building, dome, or downlink).[136] A hardened facility or bunker could potentially require seven to over 20 cruise missiles or special warheads to destroy, according to historical U.S. and allied actions.[137] In a heavily defended airspace in Syria in 2018, U.S. and allied forces launched a combination of 76 Tomahawks and 19 Joint Air-to-Surface Standoff Missile–Extended Range (JASSM-ER) cruise missiles against a chemical weapons research facility near Damascus that was theoretically under the protection of Syrian air defenses.[138] We do not have precise estimates of how many anti-ship missiles might be required to degrade or defeat an enemy carrier strike group (CSG) or surface action group. According to one estimate in the Russian military press, it might take up to 70–90

---

[132] U.S. Department of Defense, *Report to Congress: Kosovo/Operation Allied Force After-Action Report*, Washington, D.C., January 31, 2000; Ronald O'Rourke, *Cruise Missile Inventories and NATO Attacks on Yugoslavia: Background Information*, Washington, D.C.: Congressional Research Service, April 20, 1999. There were 656 JDAMs dropped from strategic bombers, but these are not standoff munitions. See also Steve Bowman, *Kosovo and Macedonia: U.S. and Allied Military Operations*, Washington, D.C.: Congressional Research Service, IB10027, November 13, 2001.

[133] Karl P. Mueller, Gregory Alegi, Christian F. Anrig, Christopher S. Chivvis, Robert Egnell, Christina Goulter, Camille Grand, Deborah C. Kidwell, Richard O. Mayne, Bruce R. Nardulli, Robert C. Owen, Frederic Wehrey, Leila Mahnad, and Stephen M. Worman, *Precision and Purpose: Airpower in the Libyan Civil War*, Santa Monica, Calif.: RAND Corporation, RR-676-AF, 2015.

[134] Mueller et al., 2015, p. 21.

[135] Westerlund et al., 2019.

[136] U.S. General Accounting Office, 1995. In Operation Desert Storm, the United States fired 42 Block II TLAM-C cruise missiles against eight buildings at the Zafraniyah nuclear fabrication facility and 23 against Saddam Hussein's intelligence headquarters of six buildings (Tyler Rogoway, "Tomahawk Cruise Missiles Pummel Houthi Controlled Radar Sites in Yemen," *The Drive*, October 13, 2016a). Radar facilities and similarly sized objects could take as few as two conventional warheads, according to FOI analysis (Westerlund et al., 2019).

[137] Dan Parsons, "Air Force Shows Off Stealthy Long-Range JASSM-ER for First Time in Syria Strikes," *Defense Daily*, April 16, 2018.

[138] John A. Tirpak and Brian W. Everstine, "Syria Strike Marks Combat Debut for JASSM-ER," *Air Force Magazine*, April 15, 2018.

missiles to defeat a U.S. CSG.[139] According to U.S. Navy estimates, a CSG can vary in size but usually includes a complement of seven to nine ships, including the carrier.[140] Therefore, we will assume that there are ten Russian ASCMs per ship on average. Russia is still experimenting with combat use of its long-range PGMs, having only used them in combat since 2015 in Syria. In that campaign from 2015 to 2017, the VKS used at least 20 Kh-101 ALCMs in Syria, and the Russian Navy launched 74 Kalibr SLCMs in two years in seven different firings, reportedly against the Islamic State's critical infrastructure in Syria, such as command posts, ammunition and fuel depots, and training facilities.[141] These data points suggest that Russia fires a fairly low number of missiles at these kinds of unhardened targets.[142]

Table 3.2 shows our targeting assumptions and sources of information.

Table 3.2. Targeting Assumptions Based on Target Type

Type of Target	Estimated Missile Requirement to Destroy or Damage Target	Source
Large military area targets (e.g., airfields, APODs, SPODs)	35–60 cruise missiles	U.S. and allied historical campaigns, Russian grey literature, FOI
Hardened or defended military point targets (e.g., headquarters, storage facilities)	7–20 cruise missiles	U.S. and allied historical campaigns
Enemy CSG or enemy surface action group (8 ships assumed)	80 ASCMs	Russian military science estimates
Critical facility or military point target in complex air defense environment	75–100 cruise missiles	U.S. and allied campaigns
Soft or undefended critical infrastructure point targets (e.g., radar facilities or downlinks, POL storage)	1–5 cruise missiles per structure	U.S. and allied historical campaigns, Russian campaign in Syria

SOURCES: Features information from Samuel Charap, Dara Massicot, Miranda Priebe, Alyssa Demus, Clint Reach, Mark Stalczynski, Eugeniu Han, and Lynn E. Davis, *Russian Grand Strategy: Rhetoric and Reality*, Santa Monica, Calif.: RAND Corporation, RR-4238-A, 2021, p. 94; Durnev and Sviridok, 2021; "Genschtab: Osobennostiu konflictkov budushevo stanet primeneniye robotov i kosmicheskix sredstv," TASS, March 24, 2018; Pavel Ivanov, "Borodatye 'Tomagavki,'" *Voenno-promyshlennyi kur'er, (VPK)*, No. 14, April 12, 2017; Hans M. Kristensen, "Russian Nuclear Forces," in Stockholm International Peace Research Institute, *SIPRI Yearbook 2020*, Oxford University Press, 2020; Kuzmin and Frolov, 2021, pp.

[139] Sivkov, 2019.

[140] America's Navy, "Carrier Strike Group (COMCARSTRKGRU) 9: About Us," webpage, undated.

[141] Anton Lavrov, *The Russian Air Campaign in Syria: A Preliminary Analysis*, Arlington, Va.: CNA, COP-2018-U-017903, June 2018; "Koncern VKO 'Almaz-Antey': vklad v potentsial strategicheskovo neyardernovo sderzhivaniye," *Natsonalnaya Oborona*, No. 11, November 2020.

[142] "Koncern BKO 'Almaz-Antey': vklad v potential strategiskovo neyardnovo sderzhivaniya," *Natsionalnaya Oborona*, June 4, 2020.

Type of Target	Estimated Missile Requirement to Destroy or Damage Target	Source

36–37; V. N. Pedyashev, A. V. Mashkovtsev, and V. V. Artemov, "The Approach to the Selection of Enemy Target Destruction Effectiveness Indicators Using Nuclear Weapons and Strategic Nonnuclear Weapons," speech delivered at the XXXI NTK (Scientific-Technical Conference) of the Serpukhov Affiliate of the Petr Velikiy RVSN Military Academy, Moscow, June 28–29, 2012; S. A. Ponomarev, V. V. Poddubnyi, and V. I. Polegaev, "Kriterii i pokazateli neiadernogo sderzhivaniia: voennyi aspekt," *Voennaia mysl'*, No. 11, 2019; "Putin Demands Smart, Precision-Guided Munitions from Defense Industry," Interfax, November 23, 2018; Sterlin, Protasov, and Kreidin, 2019; U.S. Department of Defense, *Nuclear Posture Review*, Washington, D.C., February 2018, p. 53; Westerlund et al., 2019.

NOTES: APOD = air port of debarkation; POL = petroleum, oil, lubricants; SPOD = sea port of debarkation. The numbers are for missiles that arrive on target, and they do not account for such factors as interception by missile defenses, missile failure rate, or destruction of target. This table is derived from historical examples from 1991 to 2019 of U.S., coalition, and Russian airstrikes and, where noted, Western analysis. Official Russian targeting requirements may differ.

How does Russia assess the effectiveness of missile strikes against military targets? Although Russian military science does not provide a clear answer, some analysts offer categories of destruction and how Russia might create efficiencies in strike planning. Some Russian strategists suggest that Russia could create an "operational nonnuclear response grouping" to inflict unacceptable damage on the aggressor.[143] They define this level of damage to the military potential of the aggressor as the loss of military equipment and its means of production. They classify targets as point, area, or infrastructure targets and indicate how well they are defended. They also offer an efficiency criterion for strategic nonnuclear strike planning: The cost of damage to the enemy should exceed the cost to Russia of inflicting it. In one example, if the main task given to strategic nonnuclear forces is the operational defeat of the enemy's air and naval forces, airborne warning and control system (AWACS), and sea-borne ballistic missile defense ships, an appropriate level of damage would be reducing the enemy's "intensity of air and missile strikes by 2–3 times, and intensity of hostilities during the conflict by 5–6 times."[144] To produce this outcome, they propose defeating individual aircraft carriers and ships or submarines carrying SLCMs and missile defense systems, defeating parts of the enemy's tactical aviation and AWACS, "isolat[ing] 1–2 naval theaters of military operations," and defeating enemy ships at up to four bases.[145] Other Russian theorists have identified certain damage thresholds for enemy naval forces in transit across oceans or moving to operational areas as defeat (70 percent of naval forces destroyed), suppression (50 percent losses), and weakening (30 percent suppression).[146]

[143] Ponomarev, Poddubnyi, and Polegaev, 2019, pp. 97–98.

[144] Ponomarev, Poddubnyi, and Polegaev, 2019.

[145] Ponomarev, Poddubnyi, and Polegaev, 2019.

[146] Rog, 2012.

In the ground domain, to *defeat* enemy ground forces, sources suggest a threshold of 50–60 percent losses upon most units and 70 percent losses of enemy helicopters.[147] *Suppression* of enemy forces is achieved with 20–30 percent losses or by delaying their arrival by attacking railway and highway bridges.[148] For countering land power, Russian strategists recommend using PGMs (air-to-surface and surface-to-surface missiles) for rail and large road crossings, using guided bombs for enemy mechanized forces, using mines for ports and rivers, and even launching airstrikes to induce avalanches in winter.[149] Russian long-range artillery and multiple rocket launcher systems can also attack some of these targets at ranges of less than 100 km, alleviating the burden on intermediate- or long-range PGMs.

Task 2: Attacking Military-Economic Potential and Other Critical Infrastructure

As the preceding chapters showed, there is an operational incentive to attack an enemy's military-economic potential and dual-purpose critical infrastructure. Specific infrastructure targets include energy facilities, communication nodes, and other military-industrial targets.[150] According to some, attacking enemy critical infrastructure targets is more cost effective than striking hardened military targets alone; it is allegedly a viable pathway to break the enemy's will to fight, and critical infrastructure is easier to target and destroy than dynamic military targets.[151] These ideas have been discussed for at least 30 years by such prominent Russian strategists as Chekinov and Bogdanov; Danilevich, Burenok and Pechatnov; Slipchenko; and Sterlin, Protasov, and Kreidin.[152]

LRA and other medium-range bombers can be used to launch long-range ALCMs against critically important targets to accomplish two related goals: causing instability in the enemy's homeland and causing the enemy to give up an aerospace attack.[153] Strikes against an enemy's

---

[147] Y. N. Fesenko, "Ob osobennostyakh ognevogo porozheniya gruppirovok voisk," *Voennaya mysl*, No. 5, 2000; Rog, 2012.

[148] Rog, 2012.

[149] V. Litvinenko, "Tseli dyla artillerii," *Armeiskii Sbornik*, No. 4, 2019.

[150] Borisko and Gorymekin, 2019.

[151] Vladimir Slipchenko, "Voini shestovo pokoleniya. Reshayushaya rol' v nikh budet prinadlezhat visotochnomy oruzhiyu," *Na Strazhe Rodiny*, No. 117, July 5, 1997. In 1997, Slipchenko assessed that destroying 300 important economic targets would require 9,000 high-precision munitions, or roughly 30 missiles per target. In actuality, far fewer munitions are needed for this type of target (sometimes as low as one PGM missile per target), but Slipchenko's initial assessment occurred before some of the most modern PGM campaigns took place (Rogoway, 2016a). The United States fired one Tomahawk missile per radar site in recent strikes against Houthi-controlled radar sites in Yemen.

[152] Burenok and Pechatnov, 2011; S. G. Chekinov and S. A. Bogdanov, "Evoliutsia sushchnosti i soderzhania poniatia voina v XXI stoletitti," *Voennaia mysl*, No. 1, 2017, pp. 36–37; Danilevich and Shunin, 1992; Vladimir Slipchenko, *Voiny novogo pokolenia–Distantsionnye i bezkontaktnye*, 2006, p. 94;

[153] Burenok and Pechatnov, 2011; Aleksandr Georgiyevich Tsymbalov, "O razvitii operativnikh form i sposobov deistvii voisk (sil) pri reshenii zadah VKO na sovremennom etape," *Vozdushno-kosmicheskaya oborona*, No. 3, 2012.

military-economic potential are intended to halt the enemy's operations immediately and prevent them from conducting future attacks until the war terminates favorably for Russia. Strikes against military-economic potential are also intended to create panic, sow chaos, and make life extremely difficult for the civilian population by attacking its *anthropogenic shell*, defined as cities, towns, and life-support facilities, such as sewage and water treatment facilities and municipal governments.[154] Other targets include power plants, transportation hubs, key defense industries, and news or media centers. If these targets are damaged or destroyed, the enemy's economy will be thrown into disarray, the quality of life will deteriorate rapidly via sanitation and disease, and large urban populations will flee to the suburbs or countryside, spreading chaos as a ripple effect of "secondary damaging factors."[155] In 2018, General Gerasimov expressed the view that destroying economic and government targets is a priority in modern warfare, while noting the continued importance of striking traditional military infrastructure, such as communications, reconnaissance, and navigation targets.[156]

How does Russia evaluate the success of its strikes against the enemy's critical infrastructure targets or military-economic potential during strategic operations? Some Russian military researchers have suggested that there are two planning factors to consider when planning strikes against critical infrastructure or military-economic potential. The first is the enemy's *primary losses*, which can be expressed in terms of manpower loss estimates and the number of destroyed enemy facilities, government centers, command posts, military-economic targets, and so on. *Secondary losses* refers to the effects of hitting a target. For example, striking a hydroelectric dam would result in the dam being destroyed but could also cause flooding, displace the local population, and disrupt water supplies and transportation. Secondary losses from striking an oil refinery, oil storage center, or electrical plant would affect local or regional civilian and military units. Strikes on factories or other locations with hazardous materials might cause massive chemical or even radiological pollution. These secondary losses amplify chaos and damage from the initial target's destruction, which is a force multiplier of sorts, but Russian authors also note that the effects of secondary losses are difficult to predict during the planning phase.[157]

Other Russian strategists have considered the different demands on their conventional PGM inventory based on target characteristics. To effectively use these resources—i.e., to expend the minimum amount necessary to achieve a high probability of kill (destruction)—Russian strategists pay attention to several factors about targets themselves. Although we were unable to find precise weaponeering estimates (missile to target class) in the available literature, we could identify the types of characteristics that inform strike planning. Table 3.3 shows these sorts of decisions. Several factors inform targeting decisions for critical infrastructure:

---

[154] Durnev and Sviridok, 2021.

[155] Durnev and Sviridok, 2021.

[156] "Genschtab: Osobennostiu konflictkov budushevo stanet primeneniye robotov i kosmicheskix sredstv," 2018.

[157] Pedyashev, Mashkovtsev, and Artemov, 2012.

- the likelihood that the missile will reach the target (whether the target is defended with air defenses or undefended)
- whether the target is part of a structurally durable system (whether destroying a particular target or small group of targets will cause a system-wide failure)
- whether the target is stationary or dynamic (dynamic targets require more data via intelligence [i.e., human spotters or ISR]).

Table 3.3. Target Planning for Critical Infrastructure Strikes

Variable	Characteristics of Target		
Mobility	Moving or dynamic	Stationary (point target)	Stationary (area target)
Geometric form	Point target (0–104 m^2)	Point or linear target	Area target (104 m^2 or more)
Structural durability	Small (low)—destruction of a small number of elements (0–20 percent) leads to termination of functioning	High (destruction of a small number of elements (20 percent) does not result in termination of functioning	N/A
Security	Undefended	Protected from strikes (via air or missile defenses, etc.)	Protected from damage (measures are provided to protect equipment and personnel)

SOURCE: Features information from Durnev and Sviridok, 2021, "Morphological Table of Socio-Economic Objects."
NOTE: N/A = not applicable.

Therefore, we conclude that if Russia were to target military-economic potential and other critical infrastructure during a conflict with NATO, it would need to devote considerable planning effort and would likely prioritize key nodes to maximize the impact of its strikes. Such key nodes could include major power plants that supply other aspects of the electrical grid, other energy-related infrastructure, and major rail hubs that are necessary for the onward movement of troops, equipment, and vital supplies. As referenced in the preceding chapter, Sterlin, Protasov, and Kreidin, 2019, argued that strategic nonnuclear weapons were not a viable alternative to nuclear weapons at that time for the conduct of a countervalue campaign at the regional level.

Task 3: Attacking Infrastructure with Nonstrategic Nuclear Weapons

Russian official policy documents and other Russian sources explain that there are circumstances in a great-power conflict where it might become necessary to use the entire strategic deterrence system, up to and including nuclear force.[158] In a conflict with a peer competitor in which strategic nonnuclear weapons are not halting or slowing the conflict, Russian forces are sustaining unacceptable damage, or employment of Russian platforms,

[158] Durnev and Sviridok, 2021.

munitions, and other conventional assets fails to achieve desired battlefield effects, the Russian president may consider nuclear escalation depending on the state of the conflict and the threat to the Russian state. If Russia's conventional efforts fail to de-escalate or end a conflict on favorable terms and the existence of the state is in jeopardy, Russia may use nonstrategic nuclear weapons for regional tasks in a war with NATO.

There is a consensus in Russian literature that nonstrategic nuclear weapons will remain a critical component of deterrence of regional and global wars for some time. Several authors argue that, although Russia's nonnuclear strategic forces are growing quickly and assuming roles and responsibilities that, not long ago, only nonstrategic nuclear weapons could achieve, Russia still is unable to rely on conventional deterrence against the United States or NATO. This is due to a mismatch in Russia's conventional precision strike inventory versus the combined U.S. and additional NATO inventory. As late as 2021, some argued that Russia was not yet able to rely on nonnuclear deterrence, emphasizing the continued utility of nonstrategic nuclear weapons as a warfighting tool:

> The concept of nuclear deterrence and the foundations of its implementation in the new conditions will change. There is increasing likelihood of putting into practice the concept of preventive limited use of strategic and nonstrategic nuclear weapons to force the enemy to end (de-escalate) a nonnuclear military conflict at various stages.[159]

Another factor besides an insufficient correlation of nonnuclear strategic forces is cost effectiveness. For example, in 2017, General Gerasimov observed that noncontact warfare using conventional PGMs is essentially a rich country's style of war because it is so costly in missiles and the supporting architecture needed for their operation.[160] In 2018, this sentiment was echoed by Russian President Vladimir Putin, who asked that the defense industry's PGM production process be streamlined to conserve funds during a financially difficult period for Russia.[161] In 2019, Sterlin and others wrote that "nuclear weapons are still the main instrument of global and regional deterrence" and are still "superior to conventional weapons, including the latest ones, according to the criterion of 'cost effectiveness.'"[162] The sentiment from Russia appears to be that large-scale attacks across Europe and the United States are possible for Russia only if they include nonstrategic nuclear weapons.

Russia could launch fewer nuclear cruise missiles than conventional cruise missiles to destroy an air base, for example. FOI estimated that it would take the Russian military 35 conventional warheads to disable an airfield but just five tactical nuclear warheads.[163] Others

---

[159] Kuzmin and Frolov, 2021, pp. 36–37.

[160] Charap et al., 2021, p. 94.

[161] "Putin Demands Smart, Precision-Guided Munitions from Defense Industry," 2018.

[162] Sterlin, Protasov, and Kreidin, 2019.

[163] Westerlund et al., 2019.

note that conventional damage simply is not permanent enough. For example, Russian analysts noted that the United States launched around 60 cruise missiles against the Shayrat Air Base in Syria in 2017, which did not permanently disable the location.[164] All of this suggests that Russian military specialists are dubious that Russia's growing conventional precision strike inventory is robust enough to deter or achieve decisive effects in a war with NATO, but they do seem to believe that Russia's inventory has a place in strategic deterrence and as a complement to strategic nuclear forces along a continuum of escalation. As one analyst wrote,

> It is not likely possible to create nonnuclear potential [that is] sufficient to deter a superior enemy in the era of noncontact warfare. Many specialists understand this, rightly proposing that nonnuclear capabilities should augment the nuclear component and introduce the nuclear component into the [SDFO].[165]

Military targets that Russia might seek to permanently disable using nonstrategic nuclear weapons include airfields, ports or other entry points into a theater, and groupings of enemy naval forces at sea. These are potentially some of the more difficult targets to suppress using conventional PGMs and would require high conventional munitions and expenditures, as our analysis in the following section demonstrates.

Stockholm-based think tank SIPRI assesses that, as of 2020, Russia has 1,875 warheads for nonstrategic nuclear forces across all services.[166] The U.S. Department of Defense indicated that Russia possessed up to 2,000 nonstrategic nuclear weapons as of 2018.[167] Other Western scholars estimate that Russia might have around 1,830 tactical nuclear weapons across its entire force as of 2019.[168] Of these numbers, 530 are estimated to be allocated to the Russian Air Force, 820 to the Russian Navy (SLCM, ASCM, torpedoes),[169] 380 to air and ballistic missile defenses, and 70 to the Ground Forces (SS-21 and SS-26 systems).[170] Russian military analyst Igor Sutyagin forecasts a different mixture, believing that the Ground Forces might have 248–372 warheads for the SS-21 SRBM (in long-term storage and retired) and SS-26 combined, with 200 warheads for the Russian Navy.[171] Russian strategists view their country's nonstrategic nuclear

---

[164] Ivanov, 2017.

[165] Ponomarev, Poddubnyi, and Polegaev, 2019.

[166] Kristensen, 2020.

[167] U.S. Department of Defense, 2018, p. 53.

[168] Kristensen, 2020.

[169] Russian Defense Minister Sergei Shoigu acknowledged that only a few hundred of Russia's air-launched nuclear weapons are kept at bomber bases, while most are in central storage, suggesting that Russia has several hundred nonstrategic nuclear weapons and strategic nuclear ALCMs (Hans M. Kristensen and Matt Korda, "Russian Nuclear Weapons, 2021," *Bulletin of the Atomic Scientists*, Vol. 77, No. 2, 2021).

[170] Hans M. Kristensen and Matt Korda, "Russian Nuclear Forces, 2019," *Bulletin of the Atomic Scientists*, Vol. 75, No. 2, 2019, pp. 73–84.

[171] Gudrun Persson, ed., *Russian Military Capability in a Ten-Year Perspective—2016*, Stockholm: Swedish Defence Research Agency, FOI-R--4326--SE, December 2016, p. 40.

weapon holdings as an integral component of strategic deterrence and a comparative advantage relative to NATO. This is why some Russian analysts view attempts to reduce or eliminate nonstrategic nuclear weapons as a NATO attempt to undermine Russian regional deterrence given disparities in conventional long-range munitions.[172]

Examining Russia's Ability to Execute Conventional Strikes in Support of a Notional Unified Strategic Operation

Available Strategic Nonnuclear Forces as of 2021

Russian officials do not discuss their country's annual missile production capacity, nor does the Russian military make its conventional precision strike munition inventory numbers known. They offer only vague anecdotes on proportional increases. As noted earlier, these munitions did not enter full-scale production until 2013 or later, so the starting number was quite small. One Russian source from the 46th Central Scientific Research Institute stated that, from 2016 to 2019, Russia produced 100 Kalibr SLCMs per year, or 300 total.[173] Western researchers have similarly suggested that Russia could manufacture 100 Kalibr SLCMs, 50 Iskandr missiles, and, by 2023 to 2025, around 50 Tsirkon hypersonic ASCMs per year.[174] The Russian firm Novator, which manufactures the SS-N-30A Kalibr LACM, delivered 47 Kalibr missiles in six months in 2016 (eight missiles per month).[175] This small number can be attributed to a retooling process that was taking place at Novator during this time. Up to that point, 56.7 percent of factory machinery was reported to be Soviet-era machinery.[176] By comparison, the United States is set to purchase 400 JASSM-ER cruise missiles, 122 Block IV Tactical Tomahawks, and 48 long-range anti-ship missiles during fiscal year 2021.[177] As of 2021, the U.S. military had purchased around 9,500 long-range conventional weapons and had plans to buy an additional 800 in 2022.[178] As Russian Defense Minister Sergei Shoigu has pointed out, however, Russia is almost exclusively focused on one region, while the U.S. military has global defense obligations.[179]

---

[172] For example, in November 2021, Russia conducted a kinetic anti-satellite test in space and destroyed a satellite.

[173] S. F. Vikulov, ed., *Aktual'nye problemy realizatsii voenno-ekonomicheskogo potentsiala Rossii v pervoi chetverti XXI veka i osnovnye napravleniia voenno-ekonomicheskikh issledovanii*, 2019, p. 101.

[174] Akimenko, 2021.

[175] Sergey Ishchenko, "Slishkom krypnyi 'Kalibr,'" *Armeiskii vestnik*, September 8, 2016; Roger N. McDermott and Tor Bukkvoll, "Tools of Future Wars: Russia Is Entering the Precision-Strike Regime," *Journal of Slavic Military Studies*, Vol. 31, No. 2, 2018.

[176] Ishchenko, 2016.

[177] John R. Hoehn, *Precision-Guided Munitions: Background and Issues for Congress*, Washington, D.C.: Congressional Research Service, R45996, updated June 11, 2021; Dakota L. Wood, ed., *2022 Index of U.S. Military Strength*, Washington, D.C.: Heritage Foundation, 2022, p. 427.

[178] Hoehn, 2022.

[179] Mikhail Rostovskii, "Sergei Shoigu rasskazal, kak spasali rossiiskuiu armiiu," *Moskovskii komsomolets*, September 22, 2019.

Despite Russian senior leadership attention on the issue in the past few years, it is not known whether Russia has been able to fully overcome production bottlenecks. Russia's lower-than-hoped-for missile production rates could be partially attributed to an incomplete retooling and modernization process that slowed maximum production capacity, partly a result of inefficiencies and partly because of issues accessing subcomponents due to Western sanctions.[180] Coronavirus disease 2019–related closures have also affected missile production rates. In the first six months of 2020, the production of some aerospace platforms and missiles fell by 36 percent.[181]

In terms of platform production for the Russian Navy, Air Force, and Ground Forces that would contribute to a unified strategic operation, Russia has had some success fielding large numbers of tactical aircraft, smaller classes of ships that are equipped with advanced ASCMs and SLCMs, and multiple types of submarines from the mid-2000s to 2021. British think tank RUSI estimates that the current number of cruise missile launch tubes in the Russian submarine fleet will be 300 in 2020 and 650 by 2030, with the increase being due to the planned addition of multiple *Yasen*-class submarines into the fleet and some modifications to the *Oscar II*–class cruise missile submarines. RUSI compares this estimate with U.S. force projections of 1,000 submarine-based missile slots in the U.S. Navy fleet in 2020 and 775, given current projections, by 2030.[182] (The U.S. Navy also can launch Tomahawks from *Arleigh Burke*–class destroyers, of which there are 69 in active service.)

Russian additions to the force have resulted in an overall increase in launch capacity for PGMs but not an overall force size expansion. Qualitative upgrades are occurring, whether via new air defense systems, such as the SA-21; the retiring of many third-generation aircraft (e.g., Su-24 and Su-25 fighters) and their replacement with fourth-generation or more-advanced aircraft; or the retiring of SS-21 SRBMs and their replacement with fewer but more-capable Iskander systems (equipped with SS-26 SRBMs and SSC-7 GLCMs). A major refurbishment program is underway for aspects of Russia's surface fleet that are capable of launching Russia's newest SLCMs and ASCMs. The same is true of Russia's strategic bombers and the Kh-101 missile. For example, Russia has plans to build ten new TU-160M2 by 2030.[183]

---

[180] Mark Ashby, Caolionn O'Connell, Edward Geist, Jair Aguirre, Christian Curriden, and Jonathan Fujiwara, *Defense Acquisition in Russia and China*, Santa Monica, Calif.: RAND Corporation, RR-A113-1, 2021; Radin et al., 2019.

[181] Janes Defense Weekly, "Russia Cuts State Armament Programme Funding," July 22, 2020.

[182] H. I. Sutton, "Russia Increasing Submarine Cruise Missile Capacity as US Navy Decreases Its Own," RUSI, August 19, 2021.

[183] Justin Bronk, *Russian and Chinese Combat Air Trends: Current Capabilities and Future Outlook*, London: Royal United Services Institute for Defence and Security Studies, Whitehall Report 3-20, October 2020.

Anticipating Changes in Capabilities to 2030

Over the next decade, Russia's strategic nonnuclear forces are likely to be modified and expanded. There appear to be two primary efforts to do this: modification in the near term and creation of next-generation weapons by the late 2020s and early 2030s. In the near term, Russia is experimenting with different missions and different launch domains for the precision strike systems that it currently has. By repurposing tried-and-true missiles and launchers for different roles or different domains—as opposed to creating new systems from scratch—the Russian military would gain flexibility in the arsenal it has, retain reliability, and likely achieve some cost savings. This approach would allow Russia to flexibly tailor its relatively limited inventory as needs change rather than committing to single-purpose missile families. For example, the Russian defense industry and military are currently experimenting with converting coastal defense cruise missiles and sea-launched anti-ship missiles into land-attack roles as needed.[184] The following systems are currently in or have recently undergone dual-mission testing:

- Iskander-M SRBM (NATO name: SS-26 Stone): The original mission of this missile is stationary ground targets, but the military will experiment on immobile marine targets, such as anchored ships at ports or potentially at sea. In recent years, Russia has begun to consider ports and other stationary offshore sites. This updated target set was achieved by new warhead design.[185]
- Kh-101 ALCM (NATO name: AS-23A Kodiak): A Russian defense firm is testing a smaller version of the Kh-101 ALCM, which, although it has a smaller range, can be carried by tactical aviation to strike command posts, storage depots, air defenses, missile launchers, and other critical targets.[186]
- Kinzhal: The Kinzhal air-launched ballistic missile (ALBM) can be used in both anti-ship roles (mainly against aircraft carriers but also to strike many other maritime targets) and land-attack roles.[187] The Kinzhal is essentially a derivative of the Iskander complex,[188] and it can be carried by several platforms. The modernized Mig-31K or Mig-31BM aircraft can carry the Kinzhal but might be limited to a total force size of around 50 jets.[189] Russia's newest fighter, the Su-57 (NATO name: Felon), might also be able to

---

[184] Tyler Rogoway, "It Has Begun: Russia Is Showcasing New Weapons in Fresh Syrian Offensive," *The Drive*, November 15, 2016b.

[185] "Ordnance; Iskander-M Adjusted to Hit Marine Targets," *Interfax: Russia & CIS Military Information Weekly*, August 3, 2018.

[186] Aleksey Ramm, "God vysokotochnogo oruzhiya v 2017-m Rossiya sovershila proryv v oblasti sozdaniya i primeneniya sverkhtochnykh raket," *Izvestiya*, December 29, 2017; "Vozrozhdeniye 'Belogo lebedya': kak obnovili boyevoy bombardirovshchik Rossii," TASS, January 25, 2018.

[187] "Corridors of Power; Hypersonic System Kinzhal Is Capable of Hitting Both Ground and Sea Targets - Russian Defense Ministry," *Interfax: Russia & CIS Defense Industry Weekly*, February 22, 2019; "Ordnance; Hypersonic Kinzhal Can Hit Aircraft Carriers, Other Types of Ships – Deputy Defense Minister," *Interfax: Russia & CIS Defense Industry Weekly*, March 16, 2018.

[188] "Ordnance; Iskander-M Adjusted to Hit Marine Targets," 2018.

[189] "Aviation: MiG, Russian Defense Ministry Sign Contract for Modernization of MiG-31K Carriers of Kinzhal Hypersonic Missiles," *Interfax: Russia & CIS Defense Industry Weekly*, August 27, 2021.

carry the Kinzhal after 2030, and, by then, Russia is planning to have three air regiments equipped with the Su-57.[190] Some suggest that the Su-57 will have its own hypersonic ASCM that will be carried internally to maintain low-observable properties and will replace the Kh-31 ASCM from the 1980s.[191]

- Tsirkon (NATO name: SS-N-33): The Tsirkon is a ship-based hypersonic missile that is designed to operate as an anti-ship missile but can also perform land-attack duties, although at less than 500 km in that mode, according to Russian analyst Valeriy Akimenko.[192]
- Kalibr (NATO name: SS-N-30A Sagaris): The Kalibr SLCM was primarily designed to be a long-range land-attack missile similar to a Tomahawk. There are rumors that the military seeks a ground-launched version of the Kalibr, which would mean a GLCM with a range of roughly 2,500 km.[193] Russia is reportedly experimenting with using the Kalibr SLCM in an anti-ship role, with a reduced range of 350 km.[194]
- Bastion: Russia used the Bastion coastal-defense system in a land-attack role for the first time in 2016. Russia's defense minister said that the military was able to achieve a 450-km distance against ground targets (in coastal defense mode, the missile has a range of 350 km).[195]

The second effort to 2030 is introducing new, modernized conventional PGMs with longer ranges, improved accuracy, and higher speeds (including hypersonic missiles). Some strategists argue that these new missiles will "permit shifting the bulk of strategic deterrence from the nuclear to nonnuclear sphere."[196] Russia anticipates that hypersonic missiles mounted on different types of delivery vehicles will play an increasing role in the future. One of the earliest announced missions for new hypersonic weapons is defeating U.S. and NATO missile defenses, according to Defense Minister Shoigu.[197] Gerasimov said in 2021 that new systems to 2030 can be used against military and dual-use targets, noting that Russia is creating these new systems in response to NATO buildup in Europe and that the new weapons will used in planning "prospective strikes on decision-making centers and launchers that enable tactical use of cruise

---

[190] "Aviation: Su-57 Aircraft May Be Designated Carrier of Kinzhal Missiles in Future - Aerospace Forces," *Interfax: Russia & CIS Defense Industry Weekly*, December 27, 2019.

[191] "Defense Industry; New Hypersonic Missile, Lichinka-MD, Being Developed for Su-57 Fighter Jet – Media," *Interfax: Russia & CIS Military Daily*, October 7, 2021.

[192] Akimenko, 2021.

[193] Akimenko, 2021; "Koncern BKO 'Almaz-Antey': vklad v potential strategiskovo neyardnovo sderzhivaniya," 2020.

[194] "Koncern BKO 'Almaz-Antey': vklad v potential strategiskovo neyardnovo sderzhivaniya," 2020.

[195] Rogoway, 2016b.

[196] Oleg Falichev, "Goryachiye tochki nauki: Genshtab oboznachil bazy operatsiy i rubezhi dlya uchenykh," *Voenno-promyshlennyy kuryer (VPK)*, March 27, 2018.

[197] "Ordnance; Hypersonic Weapons to Make Up Core of Russia's Non-Nuclear Deterrence Capability – Shoigu," *Interfax: Russia & CIS Defense Industry Weekly*, February 12, 2021.

missiles against facilities on Russian territory."[198] The General Director of NPO Mashinostroenia, Aleksandr Leonov, indicated that Russia is currently researching follow-on platforms to the Avangard hypersonic glide vehicle, the Tsirkon ASCM, and the Kinzhal ALBM.[199] The Avangard is mostly to assist the ensured arrival of intercontinental ballistic missile (ICBM) warheads, while the Tsirkon and the Kinzhal are more tailored toward theater strike roles, such as defeating missile defenses or time-sensitive targets.[200] Deterrence or operational missions of emerging technologies, such as the Burevestnik, Russia's nuclear-powered cruise missile still in development, are less clear. Russian sources claim that this weapon can stay in the air for days and is low-observable because of low flight altitudes.[201] We list Russia's future PGM capabilities in Table 3.4.

Table 3.4. Future Precision-Guided Munitions Capabilities, 2021–2030

Name	Type	Estimated IOC	Range	Carriers (salvo size if known)
Kh-MT, Kh-32	ALCM	2020 or later	900–1,000 km	Tu-22M3, Tu-95M, Tu-160M
Kh50/SD	ALCM	2020–2027	1,500–2,000 km	Tu-22M3 (6), Tu-95M(14), Tu-160M (12)
Kh-95	Air-launched hypersonic missile	In development	Unknown	Tu-160M[a]
3M-25A Meterit A (As-X-19 Koala)	ALCM	Reportedly in development, N/A	2,700 nm	Tu-95M, Tu-160M
GZUR hypersonic missile	ALCM	Early 2020s	1,500 km	Tu-22M3M (8), Tu-95M (14),Tu-160M (12)

[198] "Army; Gerasimov Urges Active Introduction of New Methods to Counter Potential Enemy Military Action in Space," *Interfax: Russia & CIS Military Information Weekly*, March 7, 2019.

[199] "Corridors of Power; Creation of Russia's State-of-the-Art Weapons Peresvet, Avangard, Kinzhal on Track - Deputy PM Borisov," *Interfax: Russia & CIS Military Information Weekly*, October 2, 2020; "Defense Industry; Russia Developing New Hypersonic Vehicles in Furtherance of Avangard, Tsirkon Systems – NPO Mashinostroyenia General Director," *Interfax: Russia & CIS Military Information Weekly*, April 2, 2021; "Syria Experience Prompts Need for Military Satellite Grouping, Says Russian Defense Chief," TASS, February 5, 2019.

[200] Edward Geist and Dara Massicot, "Understanding Putin's Nuclear Superweapons," *SAIS Review of International Affairs*, Vol. 39, No. 2, Summer–Fall 2019.

[201] "Ordnance; Nuclear-Powered Cruise Missile Can Stay in Air for Days - Deputy Defense Minister," *Interfax: Russia & CIS Defense Industry Weekly*, 2018.

Name	Type	Estimated IOC	Range	Carriers (salvo size if known)
Kh-BD	ALCM	Reportedly in development, 2020 or later	4,000–7,000 km	Most likely Tu-95M, Tu-160M, extended-range Kh-101
Ground-launched Kalibr	GLCM	Reportedly in development	2,500 km+	Ground-based TEL, based on Kalibr technology
Tsirkon	Hypersonic ASCM and SLCM	2022	500–1,000 km+	Multiple surface ships and submarines
Tsirkon (ground-based)	Hypersonic ASCM and GLCM	Reportedly in development as of 2019, N/A	500–1,000 km+	Ground-based version of Tsirkon hypersonic missile
Onix-M	ASCM, CDCM, and GLCM	In development as of 2019, N/A	800 km	Extended-range version of SS-N-26 Strobile for land and sea targets
Kalibr-M	LACM	In development, IOC by 2030	4,500 km	Unknown, but likely surface and submarines[b]

SOURCES: Features information from Geist and Massicot, 2019; "Ordnance; Nuclear-Powered Cruise Missile Can Stay in Air for Days - Deputy Defense Minister," 2018; Westerlund et al., 2019. Weapon system data were retrieved between September 2021 and March 2022 from multiple sources: the International Institute for Strategic Studies, the Swedish Defence Research Agency, and Janes publication series, such as *Weapons: Air Launched* and *Missiles and Rockets*.
NOTES: N/A = not applicable.
[a] See Andrey Mihayloff, "Russia's New Kh-95 Hypersonic Missile Ends the Arms Race with the United States," *Pravda*, November 10, 2021.
[b] See Ankit Panda, "Report: Russia Developing 4,500 Kilometer Kalibr-M Range Land-Attack Cruise Missile," *The Diplomat*, January 10, 2019.

Platforms and Missile Inventory

To estimate overall Russian theater strike capabilities to conduct notional unified strategic operation tasks, we consulted open-source Russian reports and other Western sources to identify a composite number of Russian precision strike inventories and launch capacities. Actual numbers of munitions might be lower or higher than our estimates, so we offer a range of estimates to account for this uncertainty in Russian inventory numbers. If Russian official statements are accurate, we think it is unlikely that we failed to capture the upper boundary for munitions.

For the Russian Navy, Russian procurement plans from the early 2010s targeted around 240 Kalibr missiles by 2020.[202] As mentioned earlier, Russia appears to have exceeded that marker. Russia reportedly was supposed to have 1,500 Kalibr-capable launch tubes by 2020, according to estimates of Russian Navy purchases. Russia, according to one article, would need a total stockpile of 4,500–6,000 Kalibr missiles in storage for a total launch capability of that size.[203]

[202] Ishchenko, 2016.

[203] Ishchenko, 2016.

(For reference, it took the U.S. Navy 20 years to procure approximately 5,000 Tomahawks.[204]) Others who have modeled a NATO air attack on Russia suggest that Russia will need, at minimum, 400–500 Kalibr SLCMs to strike NATO air force facilities.[205]

We analyzed the naval order of battle and intermediate- and long-range strike capacity as of 2021 for all fleets and flotillas that would participate in a conflict in the European theater of operations: the Northern Fleet, the Baltic Fleet, the Black Sea Fleet, and the Caspian Flotilla. We calculated the total launch capacity of each fleet by tabulating the number of operational ships and submarines, the estimated maximum missile launch capacity that each class can carry, and the conventional ammunition that they can carry that is more than 500 km. This allowed us to understand the strike potential of each fleet and whether each ship is fully equipped and launching missiles against sea- and land-based targets at one time.

According to our analysis, the affiliated launch tubes resident in these formations suggest that, as of 2021, Russia's western fleets had a total capacity of 360–376 launch tubes capable of launching Kalibr-family missiles (the SS-N-30A Sagaris LACM, SS-N-27A Sizzler ASCM, and SS-N-26 Strobile ASCM, which all fit in the same launch tube), as well as some launch tubes that can fire older P-500 Bazalt and P-700 ASCMs. Our analysis of individual Russian fleets that could be called upon in a NATO contingency, as of 2021, is shown in Table 3.5.

Table 3.5. Estimated 2021 Russian Naval Theater Strike Capacity for a European Theater of Operations

Fleet	Total Launch Tube Capacity
Northern Fleet	164 SLCMs or ASCMs
Baltic Fleet	48–52 SLCMs or ASCMs
Black Sea Fleet	116–128 SLCMs or ASCMs
Caspian Flotilla	32 SLCMs or ASCMs
Total	360–376 SLCMs or ASCMs

SOURCES: Features information from Mathieu Boulègue, *Russia's Military Posture in the Arctic: Managing Hard Power in a 'Low Tension' Environment*, London: Chatham House, June 2019; Igor Delanoe, *Russia's Black Sea Fleet: Toward a Multiregional Force*, Arlington, Va.: CNA, June 2019; Jonas Kjellén, *The Russian Baltic Fleet: Organisation and Role Within the Armed Forces in 2020*, Stockholm: Swedish Defence Research Agency, FOI-R--5119--SE, February 2021, p. 60; Nikolai Litovkin, "Russia's New Breed of Intermediate Range Missiles," *Russia Beyond*, February 6, 2019; Ministry of Defense of the Russian Federation, "Raketnye korabli Baltijskogo flota unichtozhili uslovnye beregovye i morskie celi krylatymi raketami 'Kalibr,'" December 3, 2021; Igor Rozin, "Next-Gen 'Kalibr' Cruise Corvette Joins Russia's Black Sea Fleet," *Russia Beyond*, February 10, 2021; RussianShips.info, webpage, undated; "Russia's Fourth Project 22160 Corvette 'Sergey Kotov' Starts Sea Trials," *Naval News*, October 29, 2021; Westerlund et al., 2019.
NOTES: These numbers represent the total numbers of available launch tubes capable of firing ASCMs and sea-launched cruise missiles as of 2021. We included platforms that are capable of launching the older P-500 and P-700 "carrier killer" ASCMs, although these numbers are small, and these missiles will be phased out by 2030. The remainder of the vertical launch system can fire the SS-N-30A LACM and the SS-N-27A and SS-N-26 ASCMs.

[204] According to Hoehn, 2021, p. 24, "From FY [fiscal year] 1998 through FY2018, the Navy spent $5.87 billion on 4,984 Tomahawk cruise missiles."

[205] Sivkov, 2019.

We also evaluated platform availability and launch capacity for long-range conventional PGMs from the VKS. We did not include tactical aviation in our estimates for 2021 capacity, since the capability is nascent, except for the MiG-BM that was recently upgraded to carry the Kinzhal ALBM, which we did include. Because many of the launchers are part of the LRA and not subordinate to military district, we separated those strategic bomber platforms and their launch capacity for the entire fleet of available Tu-22M Backfire, Tu-95 Bear, and Tu-160 Blackjack bombers as of 2021 (Table 3.6). Because it is unlikely that Russia would make 100 percent of these platforms available for the conventional phase of a unified strategic operation—i.e., Russia would likely want to retain some portion of them for nuclear missions or disperse them to alternative locations for survival—we used a notional 50-percent withhold for nuclear missions, if 70 percent of Russia's total stockpile will be devoted to a unified strategic operation in the European theater.[206]

Because we do not know the number of these munitions in inventory, we analyzed the number of available platforms and their estimated launch capacity to determine what salvo sizes are possible. Our analysis suggests that Russia has a total maximum launch capacity, from LRA assets and a limited number of MIG aircraft that can carry the Kinzhal ALBM, of 804–1,164 LACMs or ASCMs as of 2021, for both nuclear and conventional missiles. Some of this LRA capacity is shared with the intermediate-range Tu-22M3 Backfire, which is also capable of launching 180–240 intermediate-range ASCMs. So far, Russia has only mentioned that the Kh-47M2 Kinzhal will be carried by a limited number of refurbished MiG squadrons, which we assess to be capable of launching 12–48 total Kinzhal missiles. These results are found in Table 3.6.

Russia most likely would position some of these vital aircraft in alternate bases for survival and would likely keep some percentage ready for a nuclear mission, although we do not have estimates of what percentage could be allocated for this purpose. Thus, if we assume that 50 percent of aircraft will be withheld for nuclear missions or other purposes, the number of launch cells for conventional munitions would drop to roughly 500 for LACMs, roughly 100 for anti-ship missiles, and roughly 15 for Kinzhal ALBMs. Again, Russian models of a NATO air attack on Russia estimate that Russia might need, at minimum, 400–500 total conventional Kh-555 ALCMs in its inventory to defeat key NATO air bases; according to our analysis, Russia could launch these missiles in large salvos.[207] We do not know why Kh-101 ALCMs were not mentioned in this assessment. However, Russia has many other types of targets that it will need to neutralize in a conflict with NATO (for example, critical infrastructure targets or other reception sites for enemy forces across Europe, as noted earlier). It is highly unlikely that Russia would choose to allocate nearly all of its conventional precision strike inventory exclusively

[206] Westerlund et al., 2019, assumed that 75 percent of Tu-160 and Tu-95 bombers were reserved for nuclear missions, an estimate based on publications by Igor Sutyagin.

[207] Sivkov, 2019.

against air bases. However, air bases are a quantifiable target for our notional analysis, so we include them in our assessment below.

Table 3.6. Available 2021 Long-Range Aviation Conventional Theater Strike Platforms and Launch Capacity

Platform	Available Launchers as of 2021	Missiles per Aircraft	Maximum Salvo Launch Capacity
Tu-22M3 Backfire	60	4–6 Kh-101 LACMs 3–4Kh-22M ASCMs 4 Kh-32 ASCMs	240–360 Kh-101 LACMs or 180–240 Kh-22M ASCMs or 240 Kh-32 ASCMs
Tu-95MS Bear variants	60	6–10 Kh-101 LACMs 6–10 Kh-555 LACMs	360–600 Kh-101 LACMs or 360–600 Kh-555 LACMs
Tu-160M Blackjack variants	17	12 Kh-101 LACMs 12 Kh-555 LACMs	204 Kh-1051 LACMs or 204 Kh-55 LACMs
MiG-31BM, MiG-31K	12–24	1–2 Kh-47M2 Kinzhal ALBMs	12–48 Kh-47M2 ALBMs
Total launch capacity size if 100 percent allocated for conventional strikes	149–161		804–1,164 LACMs 180–240 ASCMs 12–48 ALBMs
Launch capacity assuming a 50-percent withhold for a nuclear mission	75–81		402–582 LACMs 90–120 ASCMs 6–24 ALBMs

SOURCES: Features information from Congressional Research Service, *The New START Treaty: Central Limits and Key Provisions*, Version 82, Washington, D.C., R41219, updated February 2, 2022; International Institute for Strategic Studies, 2021.

Russia's longest-range ground-launched PGMs as of 2021 are primarily confined to the SSC-7 Southpaw GLCM with a range of nearly 500 km. SSC-7 GLCMs are launched from the same launcher as SS-26 Stone SRBMs, estimated to have a 250–350-km range, depending on the missile. Drawing on multiple sources, we estimate that there are a total of 11–12 brigades across Russia, with 12 launchers per brigade. Some Russian media reports note that the Kremlin plans to enlarge its Iskander brigades from 12 to 16 launchers.[208] For our calculations, we used the current number, 12 launchers.[209] Each SS-26 launcher can fire two missiles, leading to a maximum launch capacity across the entire force of 264–288 SRBMs, or SSC-7 GLCMs. The 9M729 (NATO name: SSC-8 Screwdriver) GLCM is estimated to have a range of 2,500 km and

[208] Center for Strategic and International Studies Missile Defense Project, "9K720 Iskander (SS-26)," *Missile Threat*, last updated August 2, 2021b.

[209] International Institute for Strategic Studies, 2021; Westerlund et al., 2019.

reportedly uses a separate launcher.[210] Estimates vary widely in the open-source literature, from five launchers per battalion with four to five battalions in the force to around 20 launchers with an estimated salvo size of two to four missiles per launch.[211] It is therefore possible that Russia has a total launch capacity of the SSC-8 GLCM of 40–100 maximum missile launchers per salvo in 2021. By 2030, Russia will have several other ground-launched munitions available (shown in Table 3.4) that will expand its overall capacity. For a conflict in Europe, we estimate that, in 2021, Russia has 154–168 SS-26 SRBMs or SSC-7 GLCMs and 20–60 SSC-8 GLCM launch tubes available for conventional precision strikes, not counting the forces in the Eastern Military District. Our estimates of Russia's current 2021 launch capacity can be found in Table 3.7.

Table 3.7. Estimated 2021 Intermediate-Range Ground-Launched Strike Platforms and Launch Capacity

Platform	Available Launchers as of 2021	Missiles per Launcher	Total Maximum Salvo Launch Capacity
9K270 Iskander-M system	132–144 (12 brigades)	2 SS-26 Stone SRBMs or 2 SSC-7 Southpaw GLCMs	264–288 SS-26 SRBMsor 264–288 GLCMs
9M729 (SSC-8 Screwdriver)	20–25 launchers (4 battalions)	2–4 SSC-8 Screwdriver GLCMs	40–100 GLCMs
Total launch capacity size in western and central Russia	77–84 launchers SS-26 SRBMs or SSC-7 GLCMs (7 brigades) 10–15 (2 battalions) SSC-8		154–168 SS-26 SRBMs or SSC-7 GLCMs 20–60 SSC-8 GLCMs
Total force-wide launch capacity size			304–388 SRBMs and GLCMs

SOURCES: Features information from International Institute for Strategic Studies, 2021; Russian Federation Country Dashboard, Jane's, as of August 1, 2022; Westerlund et al., 2019.
NOTE: The SS-26 SRBM and the SSC-7 GLCM share the same launcher. The SSC-8 is believed to have a separate launcher because of its size.

From these estimates, we can create a combined launch cell capacity for a Europe contingency (Table 3.8).

[210] Center for Strategic and International Studies Missile Defense Project, 2021b.

[211] Dave Johnson, *Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds*, Livermore, Calif.: Lawrence Livermore National Laboratory, Center for Global Security Research, Livermore Papers on Global Security No. 3, February 2018; Kristensen, 2020; Kristensen and Korda, 2021; Roger McDermott and Tor Bukkvoll, *Russia in the Precision-Strike Regime – Military Theory, Procurement and Operational Impact*, Kjeller: Norwegian Defence Research Establishment, 17/00979, August 1, 2017.

Table 3.8. Estimated 2021 Available Long-Range Strike Launch Cell Capacity for a NATO Contingency by Launch Domain

Domain	Launch Cell Capacity
Sea	360–376 SLCMs or ASCMs
Air	402–582 LACMs 90–120 ASCMs 6–24 ALBMs
Ground	174–228 SRBMs or GLCMs

NOTE: This table assumes a 50-percent strategic withhold for LRA bombers, as they are dual-hatted as a leg of Russia's strategic nuclear triad. It does not include counts for the Pacific Fleet or the Eastern Military District, as these forces would likely not be redeployed.

Estimating Russian Multidomain Precision Strikes

The next phase in our analysis is to depict a variety of missile futures so that we can explore how they might be used against targets in Europe that correspond to the theater strike tasks in Chapter 1. We focused our analysis on forces that would participate in a Europe-based conflict with NATO: the combined ground and naval holdings of the Western Military District, Southern Military District, Northern Fleet, Caspian Sea Flotilla, and the strike forces of the Central Military District.[212] We assumed a 50-percent launcher engagement of Russian LRA and Kinzhal ALBM launchers for the conventional strike mission, with the other 50 percent remaining for nuclear missions. Because we do not know the precise munitions inventory in Russia, we estimated three scenarios based on 2021 launch cell capacity. This exercise allowed us to estimate the number of targets in Europe that Russian forces might be able to damage or destroy conventionally.

In Table 3.9, in Scenario A, forces have only half the number of missiles for each available launch cell. In Scenario B, Russian forces have one missile for each launch cell. Scenario C represents a well-performing and well-financed Russian defense industry and is based on estimates in some Russian military science literature that Russia will need three missiles in its inventory for each available launch cell. (We believe that this inventory scenario might be a decade away, according to the limited information available and Russian officer statements casting doubt on Russia's ability to sustain a regional war at the conventional level). The results can be found in Table 3.9.

[212] We do not count the forces from the Eastern Military District, as they will have responsibilities for Russia's eastern borders.

Table 3.9. Three Hypothetical Scenarios of Russian Intermediate- to Long-Range Conventional Precision Strike Inventory as of 2021

Missile Type	Inventory Scenario A: One Missile per Two Launch Cells	Inventory Scenario B: One Missile per Launch Cell	Inventory Scenario C: Three Missiles per Launch Cell
Air-launched missiles (anti-ship and land-attack)	201–291 ALCMs 45–60 ASCMs 3–12 ALBMs	402–582 ALCMs 90–120 ASCMs 6–24 ALBMs	1,206–1,746 ALCMs 270–360 ASCMs 18–72 ALBMs
Sea-launched cruise missiles (anti-ship and land-attack)	180–188 SLCMs or ASCMs	360–376 SLCMs or 360–376 ASCMs	1,080–1,128 SLCMs or ASCMs
Ground-launched ballistic or cruise missiles	77–84 SS-26 SRBMs or SSC-7 GLCMs 10–30 SSC-8 GLCMs	154–168 SS-26 SRBMs or SSC-7 GLCMs 20–60 SSC-8 GLCMs	462–504 SS-26 SRBMs or SSC-7 GLCMs 60–180 SSC-8 GLCMs
Total estimated conventional PGM missiles by missile	201–291 LACMs 45–60 ASCMs 3–12 ALBMs 180–188 shared launcher SLCMs or ASCMs 74–84 shared launcher SRBMs or GLCMs 10–30 GLCMs	402–582 ALCMs 90–120 ASCMs 6–24 ALBMs 360–376 shared launcher SLCMs or ASCMs 154–168 shared launcher SRBMs or GLCMs 20–60 GLCMs	1,206–1,746 ALCMs 270–360 ASCMs 18–72 ALBMs 1,080–1,128 shared launcher SLCMs or ASCMs 462–504 shared launcher SRBMs or GLCMs 60–180 GLCMs
Overall total (maximum)	635	1,330	3,990

NOTE: These are estimates only, based on launch tube capacity. Official numbers may vary. Air-launched numbers are based on 50 percent of Russia's overall launch capacity, assuming a 50-percent withhold for nuclear missions. Sea-launched numbers are based on all of Russia's fleets minus the Pacific Fleet, which would not be expected to participate in a European conflict scenario. Ground-launched numbers are based on all brigades except those in the Eastern Military District.

By matching our estimates of missile targeting requirements in Table 3.2 with our estimates of Russian conventional precision strike inventory in Table 3.10, we can estimate the number of targets in Europe that Russia might be able to damage using its intermediate- and long-range precision strike munitions. We want to look at two vignettes, based on what we presented in Chapters 1 and 2. First, we are interested in Russia's capacity to execute a purely counterforce conventional strike campaign, which is where the Russian military wants to go in the future. Then, we will look at a 50-50 strike campaign that targets both military and civilian infrastructure. We will use two vignettes to draw out what might be required to execute desired tasks for the conventional strike tasks of the notional unified strategic operation.

Vignette 1 focuses on military targets—air bases, heavily fortified military C2 facilities, and SLCM platforms. Vignette 2 uses the same military targets but peels off half of estimated Russian strike capacity for soft or hardened civilian infrastructure targets. The results of this analysis are presented in Table 3.10. As is shown, the 100-percent counterforce campaign, at least in our preliminary analysis, raises questions about the cost-effectiveness of that approach. This question has been and continues to be raised in Russian military literature that we cited in Chapter 2.

Table 3.10. Estimates of Targets Damaged with Conventional Precision-Guided Munition Missiles

	Vignette 1: 100 Percent Targeting Counterforce Targets	Vignette 2: 50 Percent Targeting Counterforce Targets, 50 Percent Targeting Critical Infrastructure
Inventory Estimate A	• 14–17 airfields (35 missiles per) or 8–10 airfields (60 missiles per) OR • 68–87 hardened or defended point targets (7 missiles per) or 24–30 (20 missiles per) OR • 7–8 critical targets defended by complex IADS (75 missiles per), 5–6 critical targets (100 missiles per) AND • 5–6 surface combatants	• 7–8 airfields (35 missiles per) or 4–5 airfields (60 missiles per) OR • 34–44 hardened or defended point targets (7 missiles per) or 12–15 (20 missiles per) OR • 4 critical targets defended by complex IADS (75 missiles per), 3 critical targets (100 missiles per) AND • 5–6 surface combatants
Inventory Estimate B	• 27–34 airfields (35 missiles per) or 16–20 airfields (60 missiles per) OR • 135–173 hardened or defended point targets (7 missiles per) or 47–60 (20 missiles per) OR • 13–16 critical targets defended by complex IADS (75 missiles per), 9–12 critical targets (100 missiles per) AND • 9–12 surface combatants	• 14–17 airfields (35 missiles per) or 8–10 airfields (60 missiles per) OR • 68–87 hardened or defended point targets (7 missiles per) or 24–30 (20 missiles per) OR • 7–8 critical targets defended by complex IADS (75 missiles per), 5–6 critical targets (100 missiles per) AND • 471–605 soft or undefended critical infrastructure targets (1 missile per structure) or 94–121 (5 missiles per structure AND • 9–12 surface combatants
Inventory Estimate C	• 81–102 airfields (35 missiles per) or 48–60 airfields (60 missiles per) OR • 405–504 hardened or defended point targets (7 missiles per) or 141–180 (20 missiles per) OR • 38–49 critical targets defended by complex IADS (75 missiles per), 28–36 critical targets (100 missiles per) AND • 27–36 surface combatants	• 40–50 airfields (35 missiles per) or 24–30 airfields (60 missiles per) OR • 203–252 hardened or defended point targets (7 missiles per) or 70–90 (20 missiles per) OR • 19–25 critical targets defended by complex IADS (75 missiles per), 14–18 critical targets (100 missiles per) AND • 1,413–1815 soft or undefended critical infrastructure targets (1 missile per structure) or 283–363 (5 missiles per structure) AND • 27–36 surface combatants

NOTES: IADS = integrated air defense system. Regarding ASCM usage, the TU-22M3 Backfire is the only platform that fires dedicated ASCMs in lieu of ALCMs as of 2021. For illustrative purposes, we opted to list Russian Navy launchers, which can fire the Kalibr family of SLCMs or ASCMs, with 100-percent LACM allocation. In reality, Russian ships could be outfitted with a combination of LACMs and ASCMs, which would reduce ground targets that could be engaged and increase the number of enemy ships that could be targeted. This table is intended to demonstrate Russian capacity and not a real-world strike plan.

This exercise offers insight into potential Russian capacity to engage targets through long-range conventional strike. Table 3.9 shows the influence that munitions and platform limitations have on Russian operational concept development. It puts in numerical terms the trade-offs that are abstractly referred to in Russian military discourse, from the 1992 article by Danilevich and Shunin to the 2011 work of Burenok and Pechatnov to the 2019 piece by Sterlin, Protasov, and Kreidin.

One of the more stressing cases in our analysis is the 100-percent counterforce course of action for Inventory A, wherein Russia has 50 percent fewer PGMs than launcher cells. If Russia were to use that inventory—an average of 35 land-attack ALCMs or SLCMs, which is considerably less than the number used in the U.S. strike on the Shayrat Air Base in Syria—to carry out attacks on key NATO air bases, it would have expended nearly 600 missiles. There are roughly 30 major air bases in the European theater, so this would put a serious dent in NATO air operations if NATO air force units were unable to redeploy to dispersal locations or repair damage. At the same time, this course of action would expend Russia's available long-range land-attack inventory, leaving all other European military and civilian targets, as well as the U.S. homeland, untouched. If Russia's PGM inventory were increased to one missile per launch cell (notional Inventory B), Russian planners could make more-impactful decisions, perhaps electing to target a similar number of air bases while also damaging many critical infrastructure targets.

Conclusion

Over the past decade, Russia has achieved several meaningful internal benchmarks regarding conventional precision strike that would allow it to inflict long-range conventional strikes on multiple NATO targets that were formerly only in the range of nuclear weapons. In 2009, to understand what Russian planners considered to be success, Burenok offered a vision of what a force capable of a notional regional operation should be able to accomplish. In his view, the Russian military would execute combat tasks in a nonnuclear war using conventional PGMs and "reach all categories of targets and achieve surprise with a high probability of overcoming air defense systems."[213] Specifically, Burenok listed the following characteristics of precision strike capabilities:

- increasing roles for conventional precision strike
- increasing accuracy for conventional PGMs
- increasing range for conventional PGMs
- the addition of hypersonic vehicles and UAS to neutralize enemy air defenses and conduct attacks in depth where air defense is missing.[214]

[213] Burenok, 2009.

[214] Burenok, 2009, pp. 14–16.

Since that time, Russia has fielded multiple new conventional systems that are capable of striking targets that could formerly only be ranged by nonstrategic nuclear weapons. Accuracy has improved for new systems as they are used operationally in such places as Syria. Russia has plans to 2030 to extend the ranges of multiple systems that are currently fielded. Finally, Russian officials characterize hypersonic missiles and missiles with unusual trajectories as a method for overcoming missile defenses. To this end, the Russian military has unveiled the following systems that are designed to defeat missile defenses and range enemy targets rapidly and accurately up to 2030: six new superweapons designed to "neutralize" the U.S. "global missile defense system" and advanced Prompt Global Strike and other PGM forces.[215] In many ways, Russia's developing theater strike arsenal is meeting many of these benchmarks. If the Russian defense industry can keep pace with current designs and introduce modernized variants through 2030, Russia will be in a much stronger position conventionally.

As our estimation of Russian missile launch capacity has shown, if Russia is able to manufacture at least one intermediate- or long-range conventional cruise or ballistic missile per launcher, it will be able to inflict damage on several target categories across Eastern Europe, and probably several in Western Europe—be they critical military targets or a more dispersed set of critical infrastructure targets. However, according to the unacceptable damage criteria that some Russian strategists have laid out, discussed earlier in this chapter, Russian conventional forces will not be able to achieve these effects at scale across Europe unless they are able to produce roughly three times as many munitions as they have launchers, or roughly 1,700 ALCMs, 1,100 launcher SLCMs or ASCMs, or roughly 600 SRBMs or SLCMs (our Scenario C inventory).[216]

The rationale of the Russian military's continued emphasis on nonstrategic nuclear weapons as a warfighting tool at higher intensities of conflict is arguably reflected in our analysis in this chapter. Assumptions by Russian military officers who have written publicly about the character of future war with NATO and the multiplicity of tasks in the counterforce and countervalue campaigns suggest that these officers do not yet feel that they have a sufficient depth in their conventional magazine to sustain a conventional conflict against NATO. In light of the above data, consider again the remarks of Sterlin and colleagues in 2019, which suggest that Russia might be closer to the Inventory A or B estimates:

> Strategic nonnuclear weapons are not a rational military-economic alternative to nuclear weapons in solving the tasks of global and regional strategic deterrence. It follows that the search for criteria for the sufficiency of strategic nonnuclear capabilities should be limited to solving the key tasks of local wars.[217]

---

[215] Sterlin, Protasov, and Kreidin, 2019.

[216] Poletaev and Alferov, 2015.

[217] Sterlin, Protasov, and Kreidin, 2019. *Local war* is defined in Russia's 2014 Military Doctrine as "a war pursuing limited military-political objectives when military actions take place within the borders of the warring states and affecting mainly the interests (territorial, economic, political, etc.) of these states" (President of Russia, *Voennaia*

There are several factors that limit the overall efficacy of Russian conventional precision strike capacity. One of the acknowledged challenges is the complexity of successfully targeting moving, dynamic, or fleeing targets. Russian strategists show a starting preference for the more stable fixed targets to ensure a better probability of kill. Another challenge is the overburdening of several launch platforms. For example, long-range bombers are now capable of launching conventional PGMs at increasing ranges, but their primary mission remains nuclear. Russia will need to divide its platforms between these two missions, which will reduce the overall strike power of both missions. Likewise, it is highly unlikely that Russian surface ships and submarines will be equipped with a full load-out of SLCMs or ASCMs—it will likely be a mixture, for several reasons. This allocation will reduce the overall concentrated strike power of both missions. Because of a lack of data, it is difficult to predict Russia's official PGM holdings. However, the small amounts of information that we do have suggest that the numbers are lower than Russian officials would like, which will limit how long Russia can sustain these conventional missions in a unified strategic operation.

Our analysis in this chapter focused exclusively on the European theater. However, if the conflict expands to include eastern Russia or the continental United States, all of these capacity problems will be compounded. The expansion of the conflict with NATO geographically will further strain Russian operations, planning, and capacity to execute conventional attacks in a high-intensity conflict.

In addition, Russian weapons face some technological limitations. In 2009, Russia was a generation behind developed countries, such as the United States, in critical military technologies and would need to "skip" a generation entirely. The critical gap areas were reconnaissance, communications, hypersonic weapons, and "combat platforms."[218] Some Russian military watchers have suggested that Russian precision strike weapons, particularly ASCMs, are limited not by their range but by ISR factors, thus limiting their reach. For example, some of Russia's long-range ASCMs, such as the Tsirkon, are designed to engage remote maritime targets in the "far sea zone" and could end up outrunning the ISR that guides them. This would potentially degrade the functional distances of these weapons to 500 km or less because of ISR limitations from maritime patrol aircraft (that could be intercepted and shot down), limitations from terrestrial over-the-horizon radars, or lack of support from space-based targeting.[219] In 2018, Defense Minister Shoigu mentioned that Russian combat experience in Syria has revealed a need

---

doktrina Rossiiskoi Federatsii, December 25, 2014). In all likelihood, Russia does not conceive of a local war with NATO given the scope of the likely theater and geographic separation of forces. For reference, Russia defines *regional war* as "a war involving several states of the same region waged by national or coalition armed forces in the course of which the sides are pursuing important military-political objectives" (President of Russia, 2014).

[218] Burenok, 2009, pp. 14–16.

[219] Akimenko, 2021.

to modernize and reequip Russian military intelligence satellites.[220] Russia's newest PGMs need high-resolution imagery to support terrain mapping. Given that Syria is not a denied area for Russia, and Russia makes free use of UAS for reconnaissance, Shoigu's statement suggests that Russia may not be able to rely on a sufficient satellite constellation to support a continent-wide strike in Europe, at least with lower-altitude or cruise missile trajectories.

Russia also has uncertainties in its approach to targeting and strategic operations like the unified strategic operation. Russian military leaders know that unacceptable (deterrence) damage, from the enemy's perspective, is a subjective value, will be difficult to accurately predict in conflict, and could lead to critical errors or unwanted conflict escalation. Some Russian analysts have suggested that there are limits to game theory or probabilistic methods like calculations or modeling. They argue that using supercomputing or artificial intelligence might provide additional insights to reduce uncertainty.[221] In 2009, several Russian strategists noted that by striking critical infrastructure targets or military-economic potential targets—particularly culturally significant targets or critical infrastructure—planners could easily make incorrect assumptions about the impact of such strikes on an opponent's will to fight.[222] These strategists argue that such an approach could de-escalate the conflict but could also backfire and compel the enemy to fight harder. This introduces uncertainty into the strike plan that would perhaps be mitigated by striking more-traditional targets with known outcomes. Others raised these concerns as early as 2006 and suggested that a more predictable course of action (in terms of predicting battle damage and enemy reactions) would be to focus on military targets only.[223]

[220] Konstantin Federov, "Minoborony sozdast sovremennuiu orbital'nuiu gruppirovku voennykh sputnikov—Shoigu," *TVZvezda*, March 6, 2018.

[221] Durnev and Sviridok, 2021.

[222] V. V. Sukhorutchenko, A. B. Zelvin, and V. A. Sobolevsky, "Napravleniye issledovaniy boyevykh vozmozhnostei vysokotochnogo oruzhiya bolshoi dalnosti v obychnom snaryazhenii," *Voennaia mysl'*, No. 8, 2009.

[223] V. A. Kulikov, "Military-Technical Aspects of War Prevention," *Military Thought*, East View Information Services, No. 2, 2006.

4. Russian Electronic Warfare Capabilities for Countering NATO C4ISR and a Massed Aerospace Attack

Introduction

Russia has limitations in kinetic attack to disrupt NATO's theater precision strike operations. At the same time, other capabilities can potentially augment Russian capacity constraints. For example, Russia is making a significant investment in electronic attack and will employ jammers to counter a wide variety of U.S. and NATO systems.[224]

In this chapter, we examine selected Russian jammers and show how their stated performance parameters translate into operational effectiveness. The primary criterion for the Russian systems in this chapter is their relationship to the broad operational task of disrupting NATO C4ISR. The systems for doing so are generally, but not exclusively, found in the district-level EW brigades and EW centers attached to each navy fleet.[225] Because there are limited open-source data available for most of these systems, many of the numbers used to make these determinations are notional and should be treated as such. For example, we do not have a clear sense of how many of the examined Russian jammers are in a given unit or deployed across the force. However, even a rough assessment of expected Russian jamming performance should provide insight into the systems and situations in which Russian EW should be most relevant.

In this section, we will discuss some of the jamming concepts that are relevant in this analysis and examine each of the jammers included in a notional laydown and their potential operational utility. This includes showing relevant range rings around the jammer locations and alternate locations within Russia when applicable.

Factors That Can Limit Jamming Effectiveness

Before analyzing specific Russian EW systems and jamming targets, it is worth discussing some of the jamming principles that will come into play for different jamming types. Because we are looking at a broad set of systems, not all of these factors will be relevant for every system, and there are additional factors to consider beyond those that we list. Nevertheless, keeping these ideas in mind should clarify why our assessments will not always align with advertised or stated performance.

[224] Radin et al., 2019.

[225] Tactical employment of Russian EW systems, such as those found within the organic EW companies of the Russian maneuver units, is beyond the scope of this chapter.

First, both the emitter and receiver characteristics of the system being jammed are critical in jamming effectiveness. Whether a jammer is trying to bury the signal in jamming energy or insert false signals into the system's processor, the jamming signal will generally be compared with the emitted signal in one way or another, making the signal coming from the emitter rather important. The receiver, notably the antenna and the resulting pattern from its shape and other characteristics, could be even more important. Most antennas have a spatially variant response, so the effectiveness of the jammer could be significantly degraded if the jammer is not positioned in an advantageous location. The characteristics of the transmitted signal, including the frequency, modulation, and related attributes, can vary greatly and will affect how well the applied jamming technique will perform. On a related note, systems can also be equipped with electronic protection (EP) techniques that are designed to counter adversary jammers.

Although analysis of detailed jamming and EP interactions is outside the scope of this report and likely not feasible because of data limitations, it is worth noting that these interactions can drive whether the jamming succeeds or not. For example, frequency agility is an EP technique that changes the operating frequency at a certain rate. If the jammer is jamming at the wrong frequency, it could be completely ineffective. If the jammer can adjust its frequency fast enough to keep jamming at the correct frequency, it could suffer no degrades at all. There are various other potential outcomes with frequency agility, such as reduced jamming effectiveness due to the spreading of jamming energy over multiple frequencies or "donut hole" effects in which the jamming is effective for ranges beyond the jammer and ineffective for locations between the jammer and the targeted receiver. For the jammers that are discussed here, such techniques as these might be discussed briefly, but specifics are not included.

The other major factor that is relevant to the analysis is the operational geometry of the jamming engagement. Once again, jammers target the receiver, and the receiver antenna gain in the direction of the jammer can drive the result. Thus, the configuration of the emitter and the receiver, as well as the role of the system and the location of the jammer, will determine the angle between the jammer and where the receiver is pointed. This geometry will also determine the ranges between the emitter, the receiver, and the jammer, which can be key in jamming effectiveness against certain systems. For radar jamming, the range between the jammer and the entity the jammer is trying to protect is also relevant. Finally, and most importantly for certain systems, the location of the jammer relative to the receiver will determine whether the jammer is blocked by the horizon.

Russian Jammer Laydown

Table 4.1 shows the Russian electronic warfare units and systems that we focus on for this report.

Table 4.1. Selected Russian Operational Electronic Warfare Order of Battle

Unit Number	EW Unit	System	NATO Target	Location	Service or Combat Arm
71615	15th Ind. EW Brigade			Tambov	GS
	• Battalion "N"	Leer-3; Murmansk-BN	Global System for Mobile Communications; HFGCS	Tambov	GS
	• Battalion "S"	Divnomorye; R-934UM	E-8 J-STARS, Lacrosse satellites, Global Hawk, AWACS; air attack radars	Tambov	GS
	• Battalion "K"	R-330Zh; Tirada-2S; Bylina-MM	GPS; satellite uplinks; Ka and W bands	Tambov	GS
	• Ind. EW Battalion	Unknown	Unknown	Tambov	GS
64055	16th Ind. EW Brigade	Equivalent to 15th EW Brigade	Equivalent to 15th EW Brigade	Kursk	GF
62829	19th Ind. EW Brigade	Equivalent to 15th EW Brigade	Equivalent to 15th EW Brigade	Rostov	GF
41158	18th Ind. EW Brigade	Equivalent to 15th EW Brigade	Equivalent to 15th EW Brigade	Yekaterinburg	GF
11666	17th Ind. EW Brigade	Equivalent to 15th EW Brigade	Equivalent to 15th EW Brigade	Khabarovsk	GF
60135	475th EW Center	R-330Zh; Murmansk-BN; R-934UM (BMV); Divnomorye	GPS; HFGCS; air attack radars	Crimea	Navy
09643	841st EW Center	Equivalent to 475th EW Center	Equivalent to 475th EW Center	Kaliningrad	Navy
60134	186th Ind. EW Center	Equivalent to 475th EW Center	Equivalent to 475th EW Center	Severomorsk	Navy
03047	142nd Ind. EW Battalion	Divnomorye	E-8 J-STARS, Lacrosse satellites, Global Hawk, AWACS	Kaliningrad	VKS
03051	328th Ind. EW Battalion	Divnomorye	E-8 J-STARS, Lacrosse satellites, Global Hawk, AWACS	Kronshtadt	VKS
44440	15th Army Aviation Brigade	Mi-8MTPR-1	SAM radars	Pskov	VKS
54916	49th Ind. EW Battalion			Ostrov-3	SRF
81261	Ind. EW Battalion			Ostrov-3	SRF
32713	Ind. EW Battalion			Pesochny	Unknown

SOURCE: Features information from unpublished 2019 RAND research by D. Sean Barnett, Henry Hargrove, Matthew Lane, Nicholas O'Donoughue, Barry Wilson, Katharina Ley Best, Stephen M. Worman, William Mackenzie, Clint Reach, and Jordan Willcox.

NOTES: GF = Ground Forces; GS = General Staff; HFGCS = High Frequency Global Communications System; Ind. = Independent; J-STARS = Joint Surveillance Target Attack Radar System. We assume that all of the EW brigades and centers are equipped with the same systems. Not included here are the tactical EW units found in Russian maneuver formations or combined arms armies. In the late 2000s, the 328th Ind. EW battalion employed the SPN-2 jammer (Ofitsial'nyy sayt munitsipal'nogo obrazovaniya 'Bol'shesoldatskiy rayon,' "Svedeniia o Voinskoi Chasti 03051," September 4, 2018). The "Krasukha-4" replaced the SPN-2, and the "Divnomorye" is supposed to completely replace the Krasukha family of jammers and the Moskva-1 system. Thus, we assume that the Divnomorye system is or will be in the independent EW battalions of the VKS.

High-Frequency Communications Jamming

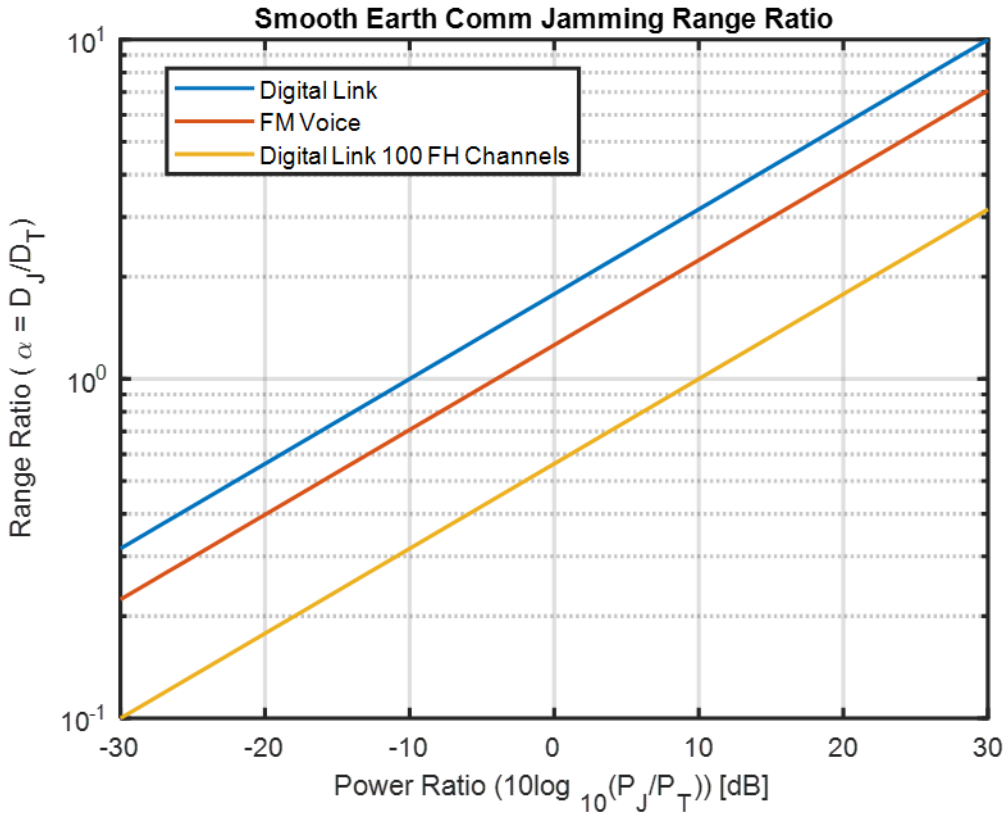
Perhaps the most daunting system that we consider here is the Murmansk-BN ground-based jammer, with its 400-kW power and expected range of 5,000 km.[226] It should not be limited by the horizon, since it operates in the 3–30-MHz high-frequency (HF) range, which is generally used by over-the-horizon radar.[227] It could target the HF Global Communications System (HFGCS), which the United States and NATO use for voice communications, among other things.

Our approach to HF jamming uses a method developed in unpublished 2019 RAND Corporation research by D. Sean Barnett, Henry Hargrove, Matthew Lane, Nicholas O'Donoughue, Barry Wilson, Katharina Ley Best, Stephen M. Worman, William Mackenzie, Clint Reach, and Jordan Willcox. This method relates the ratio of the power levels of the jammer and transmitter to their range ratio, determining how close the jammer needs to be to the receiver to be effective for a given separation distance between the HF emitter and receiver. In Figure 4.1, which is from that report, the range ratio is plotted as a function of the power ratio.

[226] Dmitriy Boltenkov, "Zakryt' volnu: kak sredstva radioelektronnoy bor'by izmenyat silu flota," *Izvestiia*, November 22, 2020.

[227] Despite being called "high" frequency, the HF band is the lowest one that is used by the jammers discussed in this report.

Figure 4.1. Communications Jamming Effective Range



SOURCE: Features information from Milkavkaz.com, "Vooruzhennye sily Rossii," webpage, undated. Site is no longer accessible.
NOTE: FH = frequency hopping; FM = frequency modulated.

An HF jamming example that was given in unpublished 2019 RAND research by Barnett and colleagues used a 42-dBW jammer against a notional HF system with a 100-W (20-dBW) transmitter, resulting in a 22-dB power ratio and a range ratio of 4 for frequency-modulated (FM) voice. Thus, HF voice communications could be denied when the distance between the jammer and the receiver was less than four times the distance between the transmitter and the receiver. For the 30-km separation between the transmitter and the receiver in the example, the jammer would be effective if it were located within 120 km of the receiver.

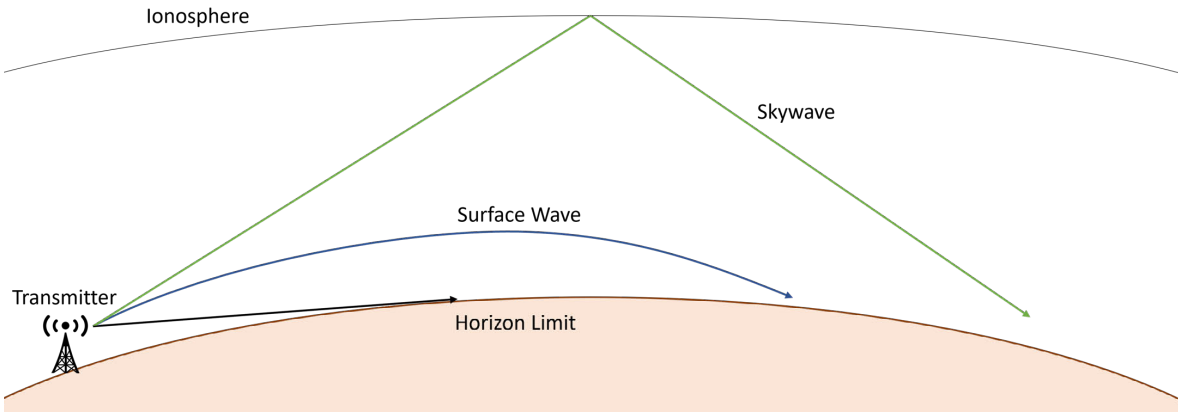
The Murmansk-BN 400-kW (56-dBW) jammer has a 36-dB power ratio when jamming the same notional 100-W HF system that was considered in the report.[228] This power ratio is not shown in the figure but results in a range ratio of 10 for FM voice when the plot is extended to include 36 dB on the *x*-axis. Thus, for the 30-km spacing in the previous example, the Murmansk-BN would deny voice communications if it were within 300 km of the receiver. For

[228] Because the HF transmitter in this example is notional, we do not include any effective power gains from EP techniques.

the Murmansk-BN to be effective at its maximum 5,000-km range, the transmitter and receiver would need to be at least 500 km apart.

The analysis by Barnett and colleagues assumes smooth earth propagation, where signal losses scale with the fourth power of propagation distance. HF propagation, however, is much more complex. Figure 4.2 illustrates the two primary types of HF propagation: *skywave* and *surface wave*. In the former, losses are proportional to the square of the *slant range*, which is the path's distance as it travels up to the ionosphere and back down to earth. In surface wave, the propagation paths are much more direct, but there are myriad ground effects that result in a loss that scales with more than the square of distance (but typically less than the fourth power). The complexities of HF propagation, and which type is dominant for a given scenario, depend on many environmental and geographic conditions, including time of day and solar activity. Therefore, we approximate the effects with the simple *smooth earth* propagation model. For more details on HF propagation, see Chapters 2 and 5 of Fabrizio, 2013.[229]

Figure 4.2. Illustration of High-Frequency Propagation



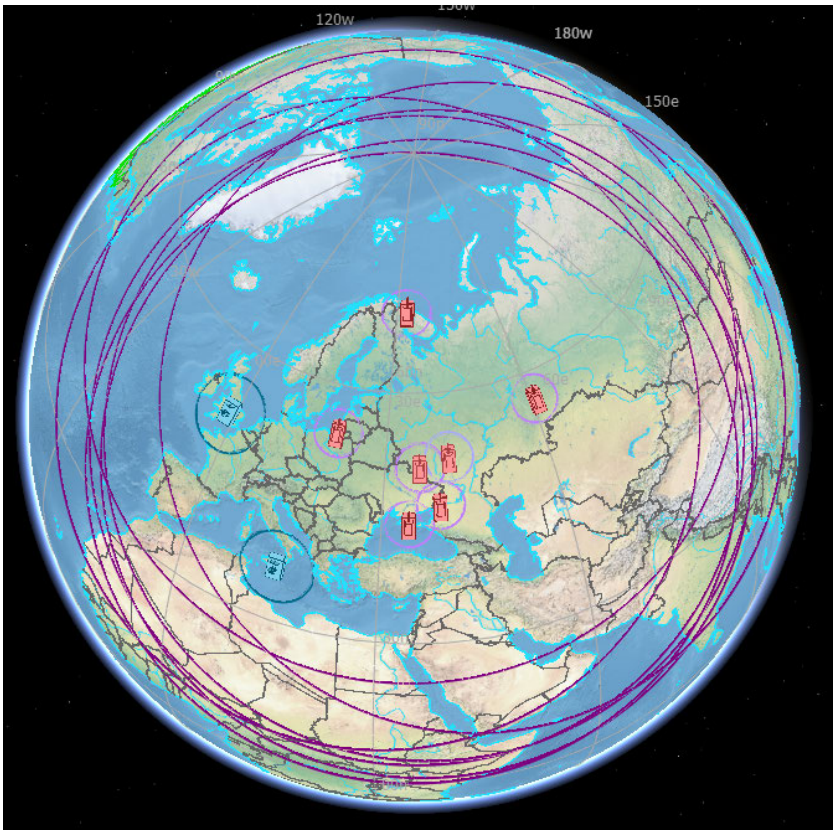
Although some of the numbers in this example are notional, they show situations in which HF communications are likely to be denied. For the European theater, the main HFGCS sites are in Naval Air Station Sigonella, Italy, and Royal Air Force Croughton, United Kingdom. Figure 4.3 shows these sites with 500-km (blue) range rings around them and the Russian Murmansk-BN sites with both 5,000-km (dark purple) and 300-km (light purple) range rings around them.[230] When the HFGCS sites are communicating with systems outside the blue rings, generally anywhere outside southern Italy and the close vicinity of the United Kingdom, the full 5,000-km

[229] Giuseppe Aureliano Fabrizio, *High Frequency Over-the-Horizon Radar: Fundamental Principles, Signal Processing, and Practical Applications*, McGraw-Hill Education, 2013.

[230] Although the range ratio that we are using for the Murmansk-BN was developed using a notional 100 W transmitter, the transmit power of the HFGCS is likely less than 100 W (FAS source).

range of the Murmansk-BN is realized and voice communications should be degraded or denied completely.

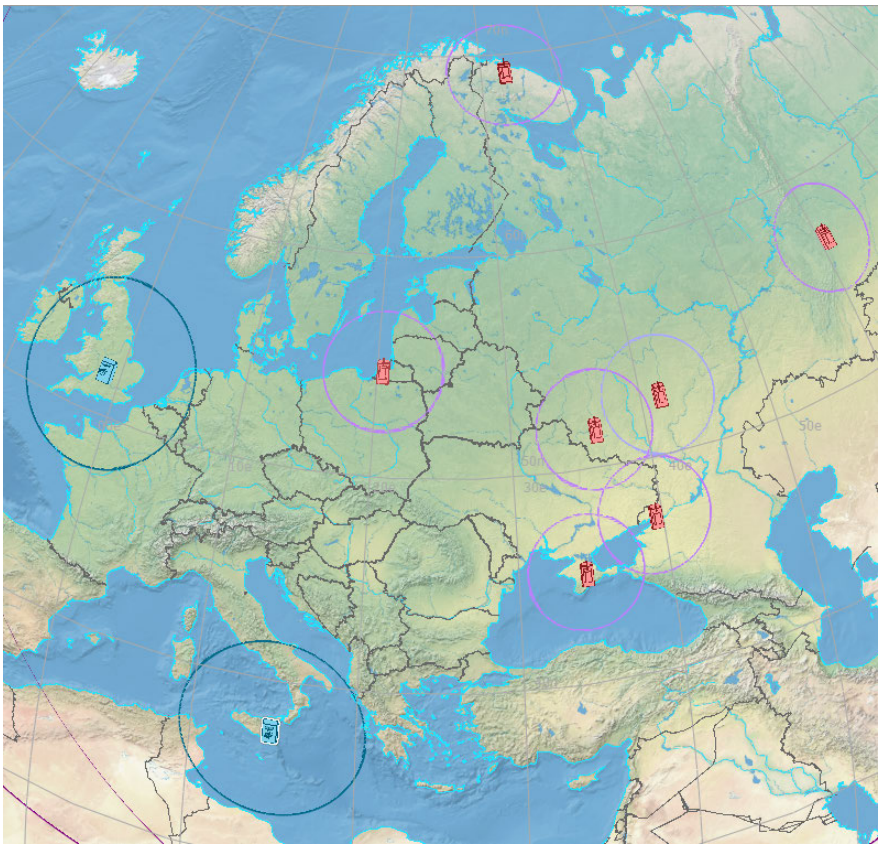
Figure 4.3. Murmansk-BN Ranges Compared with HFGCS Ranges



NOTES: e = east; w = west. The main HFGCS sites (blue icons) are shown with 500-km (blue) range rings around them, and the Russian Murmansk-BN sites (red icons) are shown with 5,000-km (dark purple) and 300-km (light purple) range rings around them.

The outer range rings in the figure basically confirm that the Murmansk-BN can deny HFGCS communications for just about the entire European theater, and the inner range rings provide insight into potential non-HFGCS HF system performance in the region. Figure 4.4 shows a zoomed-in image of this scenario, with the locations of the Murmansk-BN systems shifted somewhat to provide greater coverage with the 300-km effectiveness radius.

Figure 4.4. Murmansk-BN Ranges for Notional High-Frequency Targets



NOTE: The main HFGCS sites (blue icons) are shown with 500-km (blue) range rings around them, and the Russian Murmansk-BN sites (red icons) are shown with 300-km (light purple) range rings around them.

This figure shows a much more limited footprint for Murmansk-BN effectiveness. With the jammers confined to Russian territory, the most NATO territory covered is likely from the jammer in Kaliningrad, which reaches into northern Poland and part of the Baltics. Of course, more territory can be covered if the jammers are pushed forward, either through cooperation with Belarus or by operating from enemy territory.

It is important to remember the assumptions behind the 300-km range ring because these assumptions represent a different kind of HF communications setup than HFGCS. The assumed transmitter power was 100 W, and the separation between the transmitter and the receiver was 30 km, which is more akin to a tactical situation, possibly for communications between adjacent U.S. Army units, than support of, for example, a long-range air strike. That said, similar results may be achieved by alternative means, such as high-power transmitters or a more densely populated network of transmit stations.

Overall, the ability of the Murmansk-BN to disrupt HFGCS should complicate HF communications in the region, causing the United States and NATO to rely on alternative HF architectures or SATCOM. Depending on the specifics of the conflict, SATCOM might be the

preferred communications method anyway. However, losing HFGCS would still be relevant because it would remove the safety net provided for situations in which SATCOM is jammed or otherwise unavailable.

Satellite Communications Jamming

The primary SATCOM jammer that we consider in this analysis is the Tirada-2S ground-based jammer, which is expected to jam satellite uplinks up to 30 GHz in frequency. Our Russian EW laydown also includes the Bylina-MM ground-based jammer, which transmits at frequencies above 30 GHz and may affect satellites communicating in the Ka and W bands. There are more open-source data available for the Tirada-2S, so we focus on it here.

The Tirada-2S is expected to have a much smaller effectiveness footprint than the Murmansk-BN, with open-source ranges of "several tens of kilometers."[231] There are likely several factors that contribute to this difference, including the higher operating frequency of SATCOM, anticipated anti-jam features on satellites, and antenna losses for the jammer when it is operating outside the satellite mainbeam.

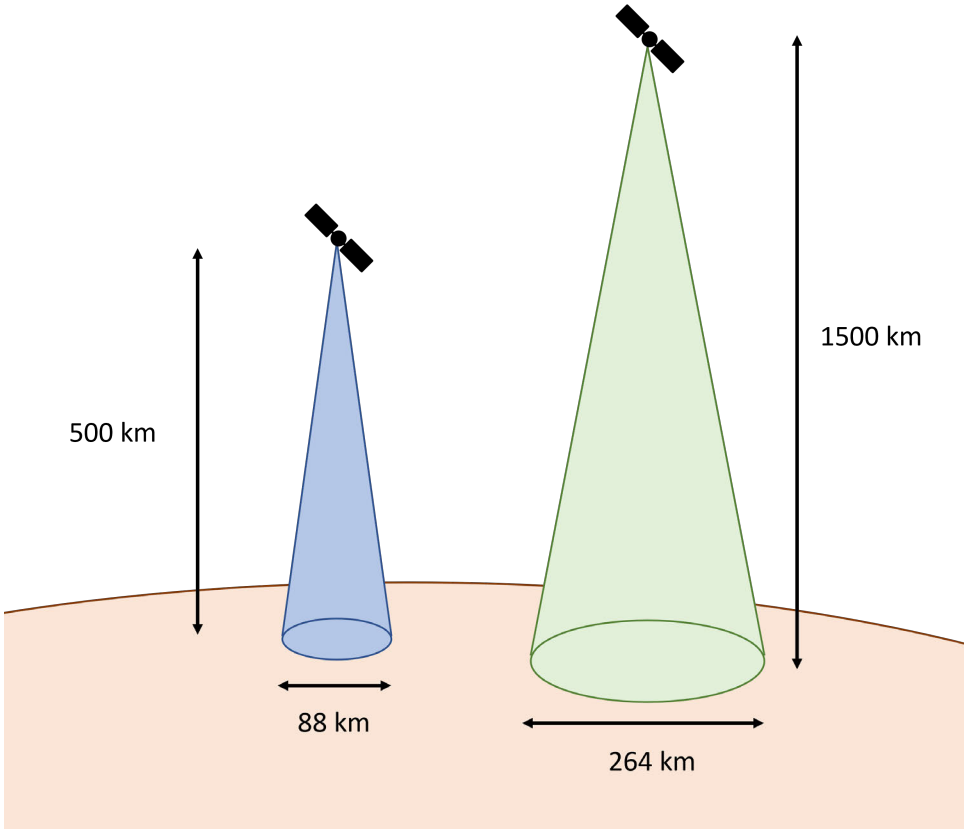
To assess the operational impact of the Tirada-2S, we assume that the Tirada-2S is effective only when it is located within the mainbeam of the satellite. There are a few reasons for this assessment. First, there is likely to be a steep drop-off in antenna gain outside the mainbeam, with the standard sidelobe level being 13 dB below the mainbeam level, and sidelobe levels 30 or more dB down being possible with antenna weighting. Second, certain anti-jam techniques might be applied against sidelobe or backlobe jammers. Third, the mainbeam footprint of a low earth orbit satellite is on the order of "several tens of kilometers," aligning our assessment with that in our source.

For a notional low earth orbit satellite operating at 500-km altitude with a 5-degree sensor half angle (10-degree beamwidth), the coverage diameter is 88 km.[232] This might be a bit generous for the jammer, depending on how one defines "several tens of kilometers." We think that this is reasonable, however, as 500 km is on the lower end of satellite altitudes and the coverage area of the beamwidth will only increase as the altitude is increased. (See Figure 4.5 for an illustration of the dependence of footprint on satellite orbital altitude; low earth orbits can be as much as 2,000 km from the earth's surface.) Figure 4.6 shows the Tirada-2S locations with 88-km (dark purple) range rings around them. There are also 44-km (light purple) range rings, but this range is not long enough to be noticeable, since the Tirada-2S icons are placed at the same locations.

[231] Novyy oboronnyy zakaz. Strategii, "Tirada-2S," webpage, September 25, 2019.

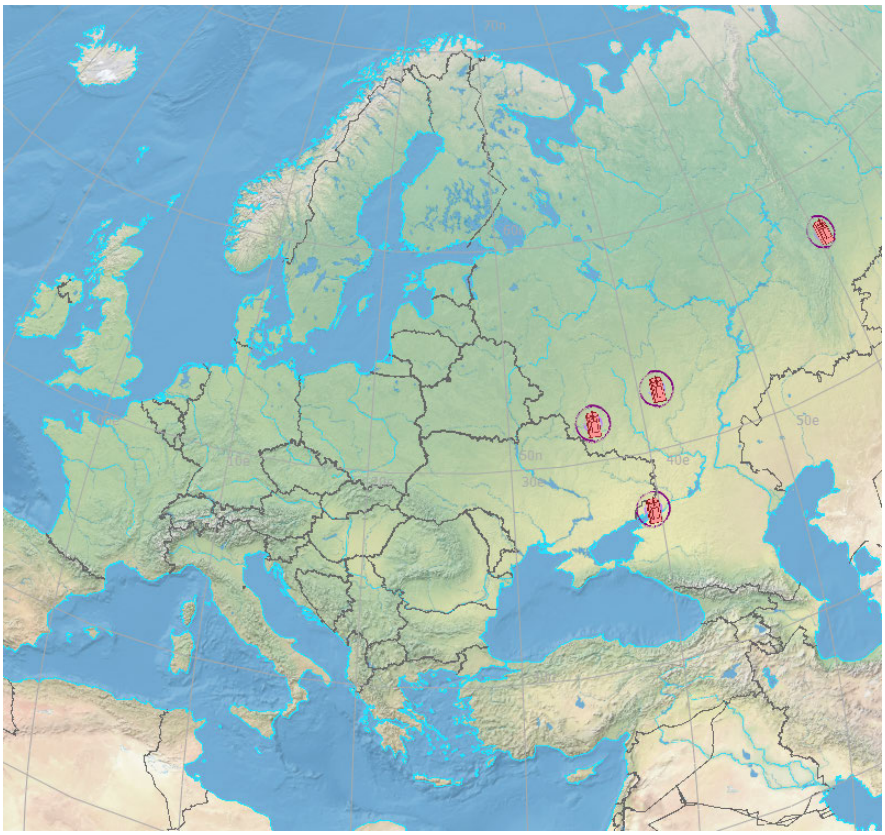
[232] This coverage diameter assumes a flat earth, which is effectively true when the half angle is small and becomes less true as the angle increases.

Figure 4.5. Illustration of Orbital Altitude and Footprint



NOTE: The figure is illustrative and not to scale. The blue and green shapes represent the coverage volumes for two different satellite altitudes. Because coverage volumes increase with altitude, the resulting volume from higher-altitude satellites can be significantly greater than that of the 500-km altitude that we assumed for coverage diameter calculations.

Figure 4.6. Tirada-2S Ranges Against Notional Low Earth Orbit Satellite Communications Target



NOTE: The Tirada-2S sites (red icons) are shown with 88-km (dark purple) range rings around them. There are also 44-km (light purple) range rings, but this range is not long enough to be noticeable, since the Tirada-2S icons are placed at the same locations in the figure.

As the figure shows, the range of the Tirada-2S is not long enough to affect satellites outside its immediate area, meaning that it will likely need to be located in enemy territory or the targeted systems will need to be in Russian territory for the Tirada-2S to have a meaningful effect.

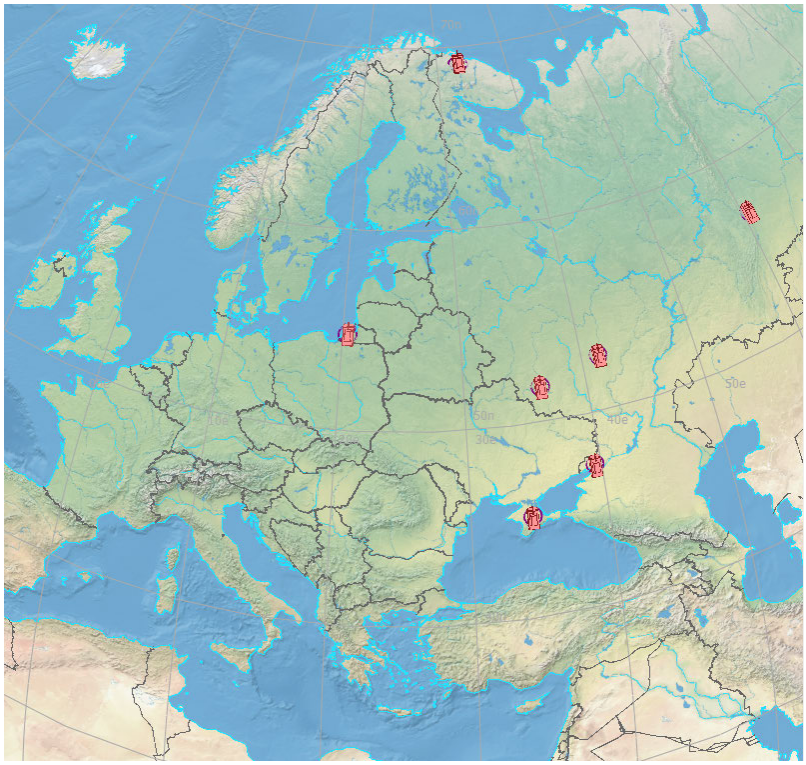
GPS Jamming

Another satellite-enabled communications method that could be affected by jamming is GPS. Unlike SATCOM uplink jamming, the targeted GPS communications receivers will be on the ground or in the air rather than in space, making horizon blockage relevant. This should be especially true for the R-330Zh Zhitel jammer, a Russian ground-based system that lists GPS navigation systems as one of its targets.[233]

[233] Rosoboroneksport, "R-330ZH: Avtomaticheskaya stantsiya pomekh abonentam sistem sputnikovoy svyazi 'INMARSAT', 'IRIDIUM' i sputnikovoy radionavigatsionnoy sistemy GPS," undated.

The listed maximum ranges for the Zhitel are 50 km for airborne targets and 25 km for ground-based targets. These ranges are similar to that of the Tirada-2S, resulting in a similar map (Figure 4.7) to the SATCOM jamming result, but with additional Zhitel locations because Zhitel is part of both the Tirada-2S brigades and the Navy EW Centers. Thus, we expect that Zhitel denial of GPS navigation is more of a tactical capability than a strategic one.

Figure 4.7. R-330Zh Zhitel Maximum Ranges for Air and Ground Targets



NOTE: The R-330Zh Zhitel sites (red icons) are shown with 50-km (dark purple) range rings around them.

Very High–Frequency Communications Jamming

The final ground-based communications jammer in our beddown is the R-934UM very high–frequency (VHF) jammer. The higher frequency (100–400 MHz) compared with the Murmansk-BN should prohibit the R-934UM from being used beyond the horizon, which should significantly limit its utility. In addition, it operates with significantly less power than the Murmansk-BN; the R-934UM has at least 500 W (27 dBW) of transmitter power, which is nowhere near the 400 kW (56 dBW) that the Murmansk-BN has.[234] It is not surprising, then, that

[234] One source (Roman Skomorokhov, "Stantsiya REB R-934U 'Sinitsa'. Kogda 'Sinitsa' v pole, zhuravlyam v nebe tyazhko," *Voennoe obozrenie*, November 3, 2017) says R-934UM has at least 500 W, and another (unpublished 2019 RAND research by Barnett and colleagues) says at least 1,000 W.

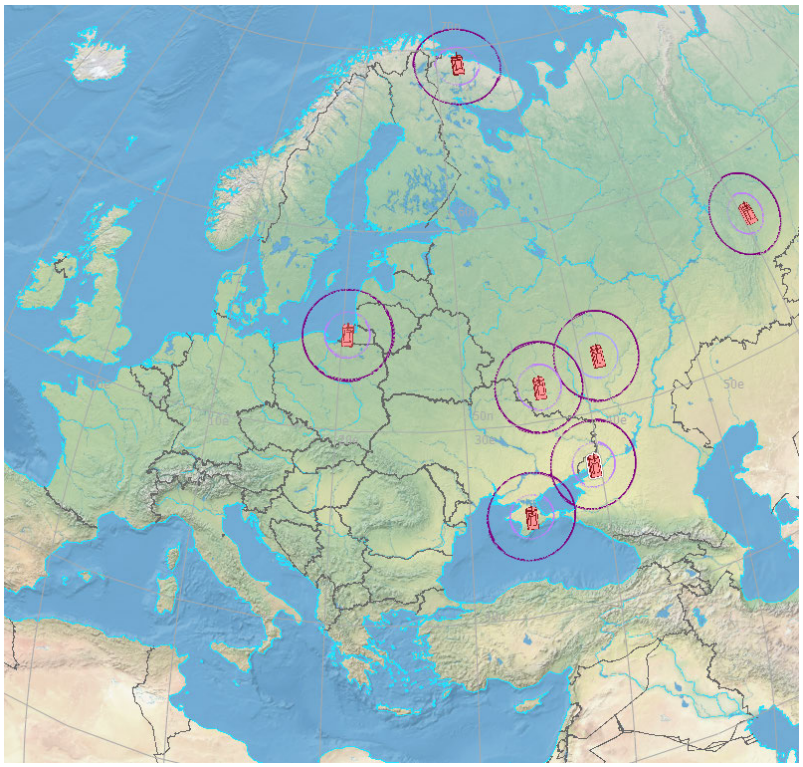
the R-934UM has a much lower reported maximum range, of 250 km.[235] This range is likely against airborne targets, as the horizon-limited result would be much shorter against ground targets.

To analyze the R-934UM, we take a similar approach to analyzing as the Murmansk-BN, using the jamming power ratio to determine the corresponding effectiveness range ratio from Figure 4.1. The work by Barnett and colleagues shows an example of a notional 1-kW (30-dBW) jammer against a 100-W (20-dBW) VHF transmitter, resulting in a range ratio between 1.33 and 2.26, depending on whether the transmitter employs frequency hopping. The researchers conclude that a range ratio of 2 is appropriate for the inputs that were chosen. Because the R-934UM has a power level of at least 500 W, and a 1-kW jammer has only 3 dBW more power than that, we consider 1 kW appropriate for R-934UM analysis and thus use 2 for a range ratio as well.

For a range ratio of 2, the VHF transmitter and receiver must be 125 km apart for the R-834UM to be effective at the maximum 250-km range. This range is plotted with the dark purple rings in Figure 4.8, along with a 125-km range in light purple. The 125-km ring corresponds to the same 125-km spacing between the transmitter and the receiver with a range ratio of 1, which could be from various factors, such as a stronger transmitter or frequency hopping.

[235] Skomorokhov, 2017.

Figure 4.8. Maximum Ranges for Very High–Frequency Communications Jamming



NOTE: The R-934UM sites (red icons) are shown with 250-km (dark purple) and 125-km (light purple) range rings around them.

For this figure, the distance between the jammer and the receiver is not known, as the system being jammed is purely notional in this example. Nevertheless, the jammer should not be effective beyond the dark purple rings, since 250 km is the maximum range of the system. Thus, VHF voice communications should not be affected in most of Europe, unless the R-934UM were operated in enemy territory or Belarus.

Airborne Radar Jamming Using Ground-Based Systems

One of the most noteworthy jammers in this analysis is the Divnomorye, because of both the systems that it targets and the number of them in this laydown. The Divnomorye is a ground-based jammer that seems to target any aircraft that has a radar; its target set includes fighters, drones, helicopters, the AWACS, and even cruise missiles.[236] Sources also list reconnaissance satellites as a target for the Divnomorye.[237]

[236] Vladimir Lytkin, "Perspektivnyye sistemy REB Rossii: chto prikhodit na smenu 'Krasukhe-4'," *Voennoe obozrenie*, July 16, 2020.

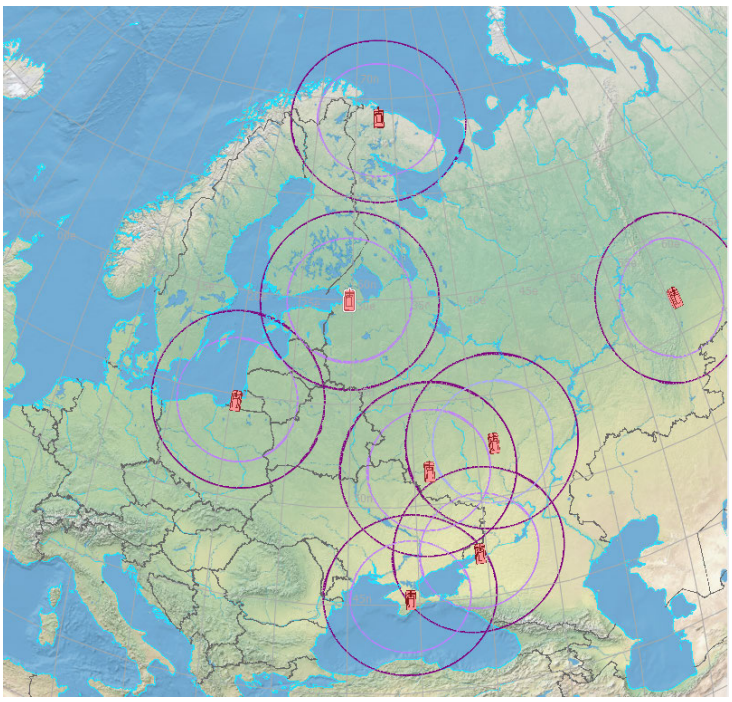
[237] Bart Hendrickx, "Russia Gears Up for Electronic Warfare in Space (Part 1)," *Space Review*, October 26, 2020c.

We did not find power levels for the Divnomorye in open sources, but we expect it to have adequate power to jam airborne platforms within its field of view. Generally speaking, ground-based vehicles tend to have greater power capacity than airborne platforms, and jammers have advantages over long-range radars because radar propagation losses are two-way and jammer propagation losses are only one-way.

The Divnomorye could also have adequate power for satellite jamming, but there are additional factors to consider. These factors include the jammer being limited by radar EP and sidelobe gain levels (similar to the Tirada-2S) if the jammer is located outside the satellite radar mainbeam and the slant range between the Divnomorye and the satellite being greater because of the 500-km+ altitude of the satellite. Because we do not know the power of the Divnomorye and there are several potential terrestrial targets to consider, we focus on airborne targets, but we acknowledge that space sensors could be jammed by this system as well.

Because we assume that the Divnomorye is effective to the radar horizon, the effectiveness range in this analysis is mostly a function of the altitude of the airborne radar. Figure 4.9 shows the Divnomorye laydown with dark purple range rings at 475 km and light purple range rings at 330 km. These ranges were chosen because they are the radar horizon at 42,000-ft and 20,000-ft altitudes, respectively.

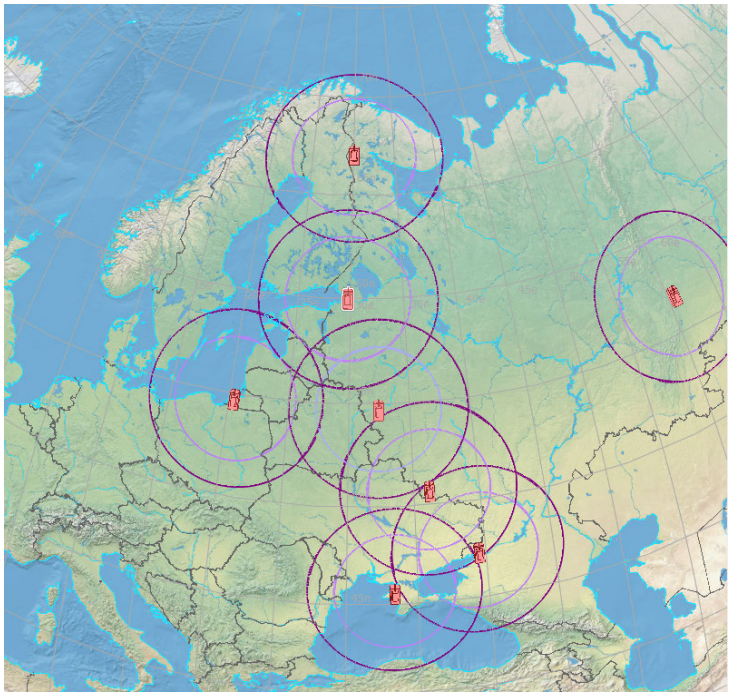
Figure 4.9. Divnomorye Maximum Ranges for Aircraft at 20,000–42,000 ft



NOTE: The Divnomorye sites (red icons) are shown with 475-km (dark purple) and 330-km (light purple) range rings around them.

The figure shows more overlapping coverage than most of the figures that we have included so far, partially because of the larger number of systems and the larger effect radius. Before making too many conclusions about the coverage shown here, we note that coverage can be expanded by spreading out the jammers near the western Russian border.[238] The more dispersed laydown is shown in Figure 4.10.

Figure 4.10. Divnomorye Coverage with Alternate Operating Locations



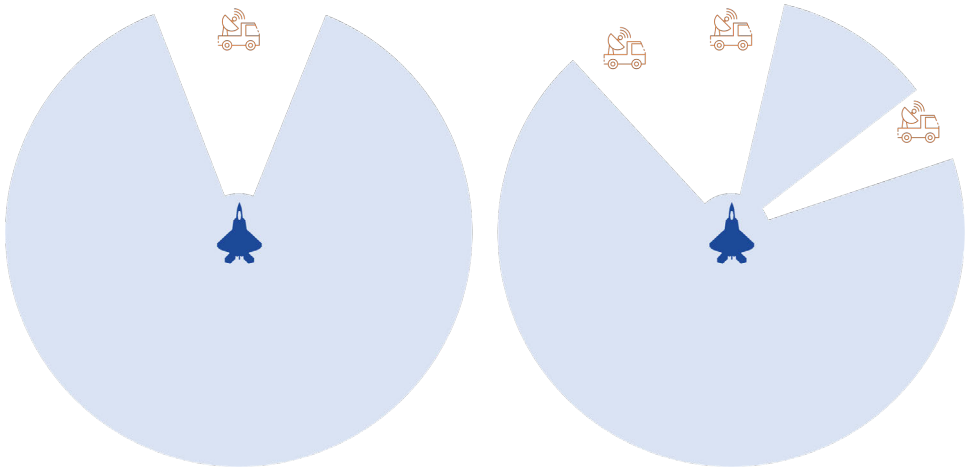
NOTE: The Divnomorye sites (red icons) are shown with 475-km (dark purple) and 330-km (light purple) range rings around them.

These figures show that, depending on the altitude of the aircraft and Russian employment of the jammers, airborne radar can be jammed by multiple Divnomorye jammers in most regions in Eastern Europe. As part of their primary function, radars typically have very narrow angular beams on transmit and receive. The effect is that the impact of the jammers will be much greater when the radar is looking in their direction and heavily reduced when it is not. Figure 4.11 illustrates this effect for a notional scenario. An airborne radar is shown in the center of each graphic in the figure, and one or more ground-based jammers are positioned around the aircraft. In each graphic, the blue circle illustrates the region in which the airborne radar is capable of performing its surveillance mission. In the left graphic, a single jammer is placed in front of the

[238] Our baseline laydown placed both Kaliningrad jammers at the same location, making them appear as a single system in Figure 4.10.

aircraft, affecting performance in that region. In the right graphic, multiple jammers are placed at different angles, further affecting performance.

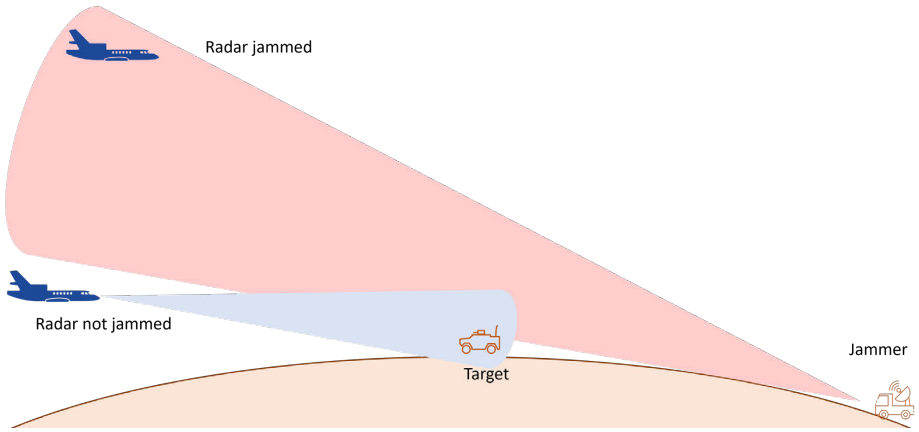
Figure 4.11. Notional Effect of Jammers on Airborne Radar



NOTE: In each graphic, an airborne radar (the blue aircraft icon) is shown in the center, and one or more ground-based jammers (the red truck icons) are positioned around the aircraft. The blue circle illustrates the region in which the airborne radar is capable of performing its surveillance mission.

It is important to note that airborne radar will also be challenged by horizon blockage, so operating at a lower altitude is unlikely to help radar-equipped aircraft unless the jammers are placed behind whatever the radars are trying to detect, as is illustrated in Figure 4.12.

Figure 4.12. Notional Effect of Horizon on Jamming Airborne Radar



Furthermore, the overlapping coverage has advantages for Russia when it comes to overcoming EP techniques, as certain techniques might be effective against one jammer but have degraded effectiveness against additional jammers. Once again, we make this assessment without detailed knowledge of the jammer or radar attributes, and the characteristics of the radar target

are also a factor. That said, if the Divnomorye has effectiveness resembling what is shown here, it could cause airborne radar to be effectively operating blind in key areas in the region.

Cellular Phone Jamming

Cellular phone jamming is generally more of a tactical problem, but we examine it here because Russia's employment of this jamming uses UAS, a different kind of platform from Russia's manned EW vehicles. The Leer-3 jammer is installed on the ORLAN-10 UAS, which has a range of 150 km. In addition to the horizon advantages that come with an airborne jammer, putting the Leer-3 on a UAS extends the effective range of the jammer to include the UAS range, and Russia might be more likely to operate an unmanned platform in enemy territory.[239]

However, it seems that the Leer-3 might still be most useful for tactical purposes. One source lists the jamming power on the fuselage as 10 W, the power on the wings as 2 W, and the range as 6 km.[240] Another source mentions that the range has been extended to 100 km, which brings the total effective range (including the range of the UAS) to 250 km.[241] Figure 4.13 shows the 250-km (dark purple) and 100-km (light purple) range rings that may occur if the ORLAN-10 needs to stay near its operating location for one reason or another.[242]

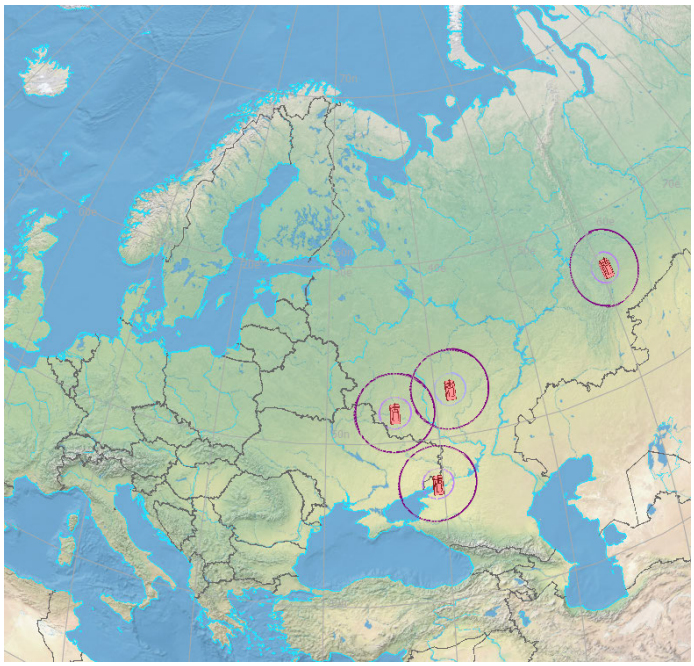
[239] Anton Lavrov, "Russian UAVs in Syria," Centre for Analysis of Strategies and Technologies, undated.

[240] Kirill Ryabov, "Den' innovatsiy YUVO: kompleks REB RB-341V 'Leyer-3,'" *Voennoe obozrenie*, October 16, 2015.

[241] Kelsey D. Atherton, "Russian Drones Can Jam Cellphones 60 Miles Away," *C4ISRNet*, November 16, 2018.

[242] Although the total effective range is 250 km, it requires the ORLAN-10 to be located 150 km from the center of the range ring. Thus, to achieve a true 250-km range ring, multiple ORLAN-10 UAVs would be required.

Figure 4.13. Leer-3 Coverage on ORLAN-10 Unmanned Aerial Systems



NOTE: The ORLAN-10 locations (red icons) are shown with 250-km (dark purple) and 100-km (light purple) range rings around them.

The results in the figure resemble the results for VHF communications, with the 250-km maximum range and the coverage that is limited to Eastern Europe unless the home station of the jammer is moved beyond the Russian border.

Surface-to-Air Missile Radar Jamming

The Mi-8MTPR-1 helicopter-mounted jammer can interfere with SAM radars in the 5–11-GHz range.[243] The range of this jammer is listed as 150 km, with potential for extended range capability.[244] With an 800-kW jammer and a maximum altitude of 20 kft, the extended range should be feasible. In addition, this range is for the jammer itself, and additional range might be possible if the helicopter is willing to fly closer to its intended target.

Although this jammer seems, by its frequency coverage and power levels, to be designed to counter ground-based engagement radars, its role could expand beyond this. Our sources list airborne radar as a potential target for this jammer, which is reasonable. Airborne intercept radar on fighter aircraft might be in the band of this system, and these radars are smaller and might be

[243] "Vertolet radioelektronnoy bor'by Mi-8MTPR1 na forume 'Armiya-2019,'" *Voyenno-tekhnicheskiy sbornik 'Bastion'*, January 29, 2020.

[244] "Kompleks 'Rychag-AV' – pomoshchnik vintokrylykh mashin: ob uvelichenii chisla vertoliotov s sistemami radiopodavleniya," *Voennoe obozrenie*, November 13, 2020.

more susceptible to jamming than more-powerful systems on the ground. AWACS and other radar with a search role tend to operate at lower frequencies, such as L- and S-band, but alternate jamming packages may extend to these bands. As we discuss below, the introduction of helicopter-based jammers adds a new element to Russian jammer analysis.

Figure 4.14 shows range rings for the Mi-8MTPR-1 location in our laydown. The outer (dark purple) ring is the 330-km horizon limit, and the inner (light purple) threat ring is for 150 km. The lack of coverage for most of Europe is likely more a function of the laydown than of the capabilities of the jammer itself, with the range rings extending through most of Latvia and Estonia for the one jammer location alone.

Figure 4.14. Mi-8MTPR-1 Helicopter Jammer Coverage

NOTE: The Mi-8MTPR-1 location (red icon) is shown with 330-km (dark purple) and 150-km (light purple) range rings around it.

Helicopter-based jammers like this one could provide unique utility for Russia. Their airborne nature extends the horizon farther than a ground-based jammer, and the Mi-8MTPR-1 proves that a helicopter like this one has the potential to carry a substantial jamming payload.

There are employment considerations that might come into play, since multiple helicopter sorties might be required to jam an enemy system for the length of time that is required. Helicopters also might be more vulnerable to attack, depending on the operational geometry, among other things. In the case of the Mi-8MTPR-1, the frequency coverage of the system seems geared toward jamming tracking radars, and detections from non-trackers might enable the employment of air assets even if the SAM system is unable to engage directly. On the other

hand, the agility of a helicopter, compared with that of a ground unit or fixed-wing aircraft, might allow Russia to deliver an EW capability more quickly than the other systems could.

Blurring the Lines

In this analysis, we have mostly categorized each Russian jammer by a single target set, discussing jammer utility in the context of the target type that we most expect the jammer to be useful against. For a few reasons, this characterization is far from perfect. First, there are limited data available for several of these systems, and we have derived their expected roles from open-source reporting or author assessments. Second, roles and target sets can evolve as systems are developed. Third, and perhaps most importantly, systems can be used for more than one purpose. For example, the Il-22PP turboprop aircraft is a key Russian jamming platform that can perform several functions.

Despite the lack of technical data available on the Il-22PP, sources list many roles for it. One source lists radio communications, the AWACS, other communications systems, and navigation satellites as targets.[245] Another provides specific radars, notably the E-3 S-band and Patriot C-band systems.[246] Other sources focus on the Il-22PP's potential capability against satellites, calling the platform a "satellite zapping powerhouse"[247] and a "murderer of satellites."[248] Sources also list its signal intelligence potential.[249] Between the jamming payload that is possible on an aircraft of this size and the versatility of employing jammers on an airborne platform, there seems to be a vast array of possibilities for this aircraft.

Although we will not attempt to quantify the effectiveness of a platform with so many unknowns, we do point out that there exists another turboprop jamming aircraft with multiple roles: the U.S. EC-130H Compass Call. This aircraft is primarily a communications jammer, designed to disrupt adversary C2 and coordination among forces, but it also has a secondary mission of jamming early-warning and target-acquisition radars. It has a combat crew of 13 people, including EW officers and cryptological linguists. It has been operational since 1983, and its versatility has enabled it to bring electronic attack capability to "virtually any combat situation."[250]

Because the EC-130H has been a high-demand asset for the United States for decades, it would be reasonable for Russia to attempt to get a similar or even greater capability from the Il-

---

[245] Sergey Ptichkin, "Oslepit i zaglushit," *Russkoye oruzhiye*, August 8, 2018.

[246] Diana Mikhailova, "S shiroko otkrytymi glazami: vozdushnaya radioelektronnaya bor'ba. Chast' 2," *LiveJournal*, January 24, 2018.

[247] Michael Peck, "Russia's Il-22PP Is a Satellite Zapping Powerhouse," *National Interest*, August 19, 2021.

[248] "'Porubshchik-2' kak ubiytsa sputnikov," *Voennoe obozrenie*, July 9, 2018.

[249] nonothai, "Il-22PP Porubschik Electronic Countermeasures Plane," *Thai Military and Asian Region*, blog, last updated August 9, 2018.

[250] U.S. Air Force, "EC-130H Compass Call," webpage, last updated May 2015.

22PP. That said, the limitations of the EC-130H could provide insight into expected limitations of the Il-22PP. A turboprop aircraft is unlikely to have the speed, stealth, and maneuverability to be survivable in high-threat environments. As with the EC-130H, there are currently limited quantities of the Il-22PP available, which would make it critical that each Il-22PP aircraft avoid being intercepted. Thus, we expect that these aircraft will be limited in terms of where they are employed.

Overall, the Il-22PP could be a formidable threat. It has the potential to jam many signals and perform multiple functions. There is much that we do not know about it, including its expected effectiveness against each of its potential targets, but many of the limitations for other jammers (e.g., horizon, satellite field of regard) would apply here as well.

Conclusion

Russia has invested heavily in EW assets, developing systems that are built to affect NATO signals in different domains and across the electromagnetic spectrum. These systems range from over-the-horizon communications jammers that could affect the whole European theater to tactical jammers that should affect only their immediate area. The importance of such jammers will depend on the geometry of their employment, the level of risk that Russia is willing to accept in terms of their location, and the relevance of the targeted NATO assets to their intended mission.

For a long-range NATO strike mission coming from central Europe, we expect Russian jammers to be much more relevant as NATO forces near the Russian border. Although the Murmansk-BN might be able to limit HF communications for most of the theater, other communication methods (e.g., VHF, SATCOM) are likely to be denied only if they are within direct-line-of-sight distance of the jammer or closer. Similar trends are apparent for other signals (e.g., radar, GPS), with most range rings that we show being confined to the Baltics and northern Poland.

As aircraft near the Russian border, the challenges to NATO C4ISR should increase considerably. Powerful ground-based jammers could deny communications and degrade detection from radar sensors. Airborne jammers, some unmanned, could extend the reach of Russian jamming and add a level of flexibility and agility to their employment. Because certain key NATO strike functions (e.g., target geolocation) will likely need to occur when aircraft are within the line of sight of targets in Russian territory, the ability of Russian jammers to affect systems in this region could be critical.

There is a myriad of factors that will determine the effectiveness of this jamming, notably the EP features that NATO systems might include. In addition, the platforms carrying these jammers could be targeted, as most jammers will need to be located near the assets they are protecting to be effective and their emissions could highlight their location. Because we do not have details on NATO EP and other data that would be required for a firmer assessment of Russian jammer

effectiveness, we stress that interactions between jammers and sensors are complex and the existence of a capable jammer does not guarantee effective signal suppression.

The Russian EW threat is diverse and growing, and it will need to be accounted for by NATO systems operating in key regions in Europe. We do not expect this threat to be insurmountable, however, as there are physical and operational challenges that Russian jammers need to overcome to be successful.

5. Russian Capabilities for Functional Suppression and Destruction of Space-Based Assets

Introduction

In this chapter, we examine the role of Russian anti-space capability in a notional unified strategic operation. As General-Colonel V. B. Zarudnitskii articulated in a 2021 article on future war, "Innovative weapons systems located on space combat platforms may soon become a new means of waging modern warfare."[251] As a result, Russia has integrated its capabilities in space and its defensive actions from space into thinking on asymmetric options to disrupt an attack from NATO.[252] Russia's aerospace forces are contemplating new forms of warfare in outer space, including anti-satellite (ASAT) combat to disrupt state infrastructure that supports space missions and counterspace operations.[253] Space assets could become a primary target to disrupt NATO's military capacity as envisioned in Prompt Global Strike, even in the early phases of a regional war. Outer space is also a key domain in the preconflict phases during which Russia's counterspace capabilities are used to signal and deter a potential adversary. Furthermore, most of Russia's counterspace capability is effective in low earth orbit, which is full of civilian and dual-use satellites used by the West, raising the possibility of targeting commercial communications satellites as part of critical infrastructure.

In this chapter, we will explain Russian military thinking on conflict in space as articulated in the literature of the past 15 years. We will then review the major counterspace systems to assess how they might fit within a notional unified strategic operation.

Russia as a Great Space Power

Russia sees space as an increasingly important domain for nation-states. In addition to being a nuclear weapon state, Russia sees itself as second only to the United States as a space power. This view is derived from its history of achievements in space, from the theories of its 19th-century rocket theorist Konstantin Tsiolkovsky to its major firsts in space, including the first satellite in orbit and the first man, woman, and dog in space, as well as its extensive accomplishments in long-duration manned spaceflight.

---

[251] Zarudnitskii, 2021b, p. 41.

[252] Alexey Arbatov, "Nauchno-tekhnologicheskaia proektsia kosmicheskoi deiatel'nosti," in *Kontrol' nad vooruzheniiami v novykh voenno-politicheskikh i tekhnologicheskikh usloviiakh*, Moskva, 2020b, p. 94.

[253] Valerii V. Gerasimov, "Rol' general'nogo shtaba v organizatsii oborony strany v sootvetstvii s novym polozheniem o general'nom shtabe, utverzhdennym prezidentom rossiiskoi federatsii," *Vestnik Akademii voennykh nauk*, Vol. 46, No.1, 2014, p. 15.

Space is an increasingly important domain in great-power competition. According to Russian experts, space is a new sphere of military and political confrontation in a multipolar world.[254] Russia has repeatedly acknowledged the important role of the outer space domain in commercial and national security activity, as well as the military's dependence on space-based assets in armed conflict.[255] The number of spacefaring nations is growing. States that once had a limited presence in outer space, such as China and India, are increasing their extraterrestrial presence to include enlargement of their own military space programs. In response, Russia's military is expanding and modernizing its capabilities in space and contemplating how it would engage its adversaries' space-based assets in the event of a conflict.

Conflict in Outer Space

In thinking about interstate conflict, Russian military and national security experts recognize that outer space and space-based assets will be critical in a future war.[256] During the Cold War, Soviet leaders had anticipated military confrontation in space with the United States, and they subsequently initiated several research programs designed to counter U.S. space-based systems.[257] After the fall of the Soviet Union, Russian military space programs were starved of resources, and many systems were either underfunded or eliminated.

Taking note of the U.S. use of space-based assets in the Gulf War in 1991 and in the air campaign against Serbia in 1999, Russia observed how space-based assets could be used for conducting military operations in a future noncontact war. Within the Russian General Staff, there was an evolution in thinking about the application of military power through space. In the late 20th century, space was viewed as a support arm to conventional and strategic forces, providing navigation, intelligence, and timing. Today, Russia's military leaders accept that the role of outer space is undergoing a transition from a supporting role to one of combat operations.[258] Russia views the outcome of future conflict as largely dependent on the balance of forces in the air and in outer space.

---

[254] Gerasimov, 2014, p. 2; A. B. Palitsyn and D. B. Zhilenko, "Analiz traditsionnykh i perspektivnykh zadach sistemy vozdushno-kosmicheskoi oborony Rossii: problem i puti ikh resheniia," *Voennaia Mysl'*, No. 9, 2020, p. 7.

[255] Arbatov, 2020a, pp. 91–95.

[256] Gerasimov, 2014, p. 20.

[257] Arbatov, 2020a, pp. 109–113. See also A. A. Kokoshin, "Voruzhennaia bor'ba v kosmicheskom prostranstve: novye tekhnologii i ikh vliianie na strategicheskuiu stabil'nost'," in *Vlianie tekhnologicheskikh faktorov na parametry ugroz natsional'noi i mezhdunarodnoi bezopastnosti, voennykh konfliktov i strategicheskoi stabilnosti*, 2017, pp. 1–56.

[258] Arbatov, 2020a, p. 92; Zarudnitskii, 2021, pp. 38–39.

U.S. Militarization of Outer Space as a Component of Global Strike

Russia has been critical of the militarization of space on the part of the United States. The U.S. withdrawal from the Anti-Ballistic Missile Treaty in 2002, development of ballistic missile defense, rapid expansion in dual-use space applications, and recent creation of the U.S. Space Force have reinforced a perception that the United States intends to dominate the space domain.[259] For the United States, these assets are deemed essential to the early 21st-century concept of Prompt Global Strike, which gives the United States the ability to hit targets around the world with conventional standoff weapons with substantially shorter flight times. According to Russia, U.S. military activities in space are part of a general trend among states to use space to solve military problems.[260]

There are several reasons Russia believes the United States is placing a greater emphasis on space and its military utility. Alexey Arbatov observed that the United States seeks to dominate space to make up for a drop in its geopolitical standing in the world.[261] Space is also seen by some Russian military thinkers as essential to developing a conventional standoff capability that can threaten the nuclear arsenals of an adversary without the United States having to resort to the first use of nuclear weapons.[262] However, Russia's military leadership sees the trend as a longer-term effort by the United States. In 2019, General Gerasimov pointed out,

> The Pentagon has recently many times declared its intention of using space for military purposes. With this goal, a new armed service—Space Forces—is being formed and this creates conditions for the militarization of outer space. All these actions may lead to acute aggravation of the military-political situation, emergence of new threats, to which Russia will have to respond with mirror and asymmetric measures.[263]

According to the Russian narrative, U.S. actions in space make up a critical element of the ability of the United States to strike globally. The primary threat for Russia is to its homeland, but it also sees U.S. space-based capabilities as allowing the United States and its allies to dominate in regional conflicts, such as in Serbia (1999), Afghanistan (2001), and Iraq (1991 and 2003).[264] As a result, Russia's concept of aerospace defense emerged in the early part of the 21st

---

[259] See Alexey Arbatov, Vladimir Dvorkin, and Petr Topychkanov, "Entanglement as a New Security Threat: A Russian Perspective," in James M. Acton, ed., *Entanglement: Russian and Chinese Perspectives on Non-Nuclear Weapons and Nuclear Risks*, Washington, D.C.: Carnegie Endowment for International Peace, 2017.

[260] Palitsyn and Zhilenko, 2020, p. 7.

[261] Alexey Arbatov, "Arms Control in Outer Space: The Russian Angle, and a Possible Way Forward," *Bulletin of the Atomic Scientists*, Vol. 75, No. 4, 2019, p. 156.

[262] Arbatov, Dvorkin, and Topychkanov, 2017, p. 24; V. M. Burenok and O. B. Achasov, "Neiardnoe sderzhivanie," *Voennia Mysl'*, Vol. 17, No. 1, 2008, pp. 12–13.

[263] Arbatov, 2019, p. 153.

[264] Burenok and Achasov, 2008, p. 12.

century, and Putin approved the concept in 2006.[265] In the past ten to 15 years, Russia has observed several characteristics of U.S. space programs that present space-based assets as particularly dangerous for Russia. Some of the major threats that Russia sees from the U.S. space expansion are the testing of the X-37B as a potential ASAT platform or orbital weapon system, the proliferation of reusable launch vehicles from such companies as Space X, the deployment of dual-use miniature satellites, and the potential use of satellites to help track and counter Russian hypersonic weapons.[266] Each of these capabilities presents Russia with a challenge, and it does not have the budget to symmetrically counter all U.S. space-related programs. As a result, Russia is looking for ways to degrade U.S. space-based capabilities using various means and methods.

Russia's Strategic Military Objectives in Space

Russia's strategic objectives of aerospace defense as they relate to space-based systems are threefold. First, Russia views its space-based systems as essential to providing its senior leadership with timely warning of an aerospace attack, with either conventional or nuclear weapons, so that it can make key decisions for its response.[267] A foundational element of that early-warning requirement is ensuring that Russia can defend its nuclear deterrence capability from a conventional first strike so that decisionmakers have that option. Second, Russia intends to use its relevant space and anti-space capabilities to suppress and defeat an aerospace attack.[268] Third, Russia seeks to use the aforementioned space capabilities as a means of deterrence in peacetime and as the threat of conflict rises during a crisis.[269] Russian authors note the critical importance to Russia's defense against aerospace attack of a single operating concept by which the entirety of the Russian armed forces contributes to Russia's defense.[270] Each of these objectives will be explored in further detail as it relates to space-based systems of the United States and Russia.

Russian space-based assets provide reconnaissance of adversary force posture and the launch of certain weapons, specifically ballistic missiles. Knowledge of force posture and launches informs senior Russian leaders so that they can decide on a deliberate response. As part of its military modernization effort, Russia developed the Unified Space Detection and Combat Control System (in Russian, *EKS OiB*).[271] Warning is provided by a layer of ground- and space-

---

[265] Sergei Sukhanov, "VKO – eto zadacha, a ne sistema," *Vozdushno-kosmicheskaya oborona*, March 29, 2010.

[266] Arbatov, 2020a, pp. 90–91; Kokoshin, 2017, p. 34; Palitsyn and Zhilenko, 2020, p. 7.

[267] Palitsyn and Zhilenko, 2020, p. 10.

[268] Sukhanov, 2010.

[269] A. A. Romanov and S. V. Cherkas, "Perspektivy razvitiia kosmicheskikh voisk Rossiiskoi Federatsii v usloviiakh sovremennykh tendentsii voenno-kosmicheskoi deiatel'nosti," *Voennaia mysl'*, No. 9, 2020, p. 38.

[270] Sukhanov, 2010.

[271] Victor Miasnikov, "Edinaia kosmicheskaia sistema predupredit o iadernom napadenii," *Nezavisimaya gazeta*, October 17, 2014.

based systems, most notably Russia's Tundra satellites, the first of which was launched in 2015 to replace obsolete systems. Russia's constellation of ten high earth orbit Tundra satellites is expected to be complete by 2024 or 2025 and provides Russia's leadership with notice of ballistic missile launches throughout the globe.[272] Communications satellites, such as Meridian, Raduga, and the planned Sefra-V, make up an Integrated Satellite Communication System, which provides the national command structure and the armed forces with communication capabilities. This gives Russia greater redundancy in its communications systems in case its own communications satellites are degraded.[273] As part of its emphasis on the defense of its Arctic regions, Russia has launched its Arktika series of satellites in highly elliptical orbits. The various satellite warning systems feed their respective information to the 820th Main Centre for Missile Attack in Moscow, which then informs Russia's senior leadership of an attack. Ensuring that these satellite systems continue to provide the necessary early warning is a defensive priority for Russia's aerospace forces.

Related to Russia's early-warning systems, Russian nuclear deterrence depends on protecting Russia's strategic nuclear forces from conventional attack. Russia relies in part on scattering road-mobile ICBMs in times of international tension or in the preconflict phase of a crisis. The effectiveness of a mobile land-based system was reliable in the late 20th century because there was sufficient time for individual launchers to move between the detection of a hostile missile and its impact. The U.S. concept of Prompt Global Strike, with its capability to hit targets around the globe with conventional warheads or, more recently, the future use of hypersonic missiles, makes such mobile land-based systems more vulnerable to a conventional missile attack.[274] Adversary missiles receive updated targeting guidance while in flight from U.S. reconnaissance satellites that can track the mobile launchers. As a result, Russia is developing ASAT systems to degrade the U.S. capability to track its nuclear forces. For example, Russia's Peresvet mobile ASAT system, which can dazzle reconnaissance satellites, is colocated with Topol-MR and RS-24 ICBMs for the purpose of preserving Russia's mobile land-based ICBM force in case of conventional missile attack.[275]

---

[272] Pavel Podvig, "Russian Space Systems and the Risk of Weaponizing Space," in Samuel Bendett, Mathieu Boulègue, Richard Connolly, Margarita Konaev, Pavel Podvig, and Katarzyna Zysk, eds., *Advanced Military Technology in Russia: Capabilities and Implications*, London: Chatham House, September 2021, p. 38. See also Bart Hendrickx, "EKS: Russia's Space-Based Missile Early Warning System," *Space Review*, February 8, 2021.

[273] Anatoly Zak, *Russian Military and Dual-Purpose Spacecraft: Latest Status and Operational Overview*, Arlington, Va.: CNA, June 2019, p. 23.

[274] O. S. Kupach, "Analyzing the U.S. Conventional Prompt Global Strike Program," *Military Thought*, Vol. 27, No. 4, 2018.

[275] Bart Hendrickx, "Peresvet: A Russian Mobile Laser System to Dazzle Enemy Satellites," *Space Review*, June 15, 2020b.

Functional Suppression of an Aerospace Attack in Outer Space

As we explained in Chapter 2, Russia seeks to ensure that it can respond to NATO and the United States through the use of strategic and operational nonnuclear capabilities and, if necessary, nuclear weapons. It also needs to protect its industrial base and critical infrastructure from being targeted by conventional weapons. Therefore, Russia not only needs to ensure that it can maintain the requisite space support for its offensive weapons but also must degrade U.S. space-based systems that the United States and NATO rely on to target Russian industrial capabilities. According to our assumptions about unified strategic operation tasks, this is accomplished through the functional suppression or destruction of the adversary's space-based assets.[276]

Functional suppression entails degrading or destroying the capabilities of U.S. and NATO satellites used for reconnaissance, precision, timing, and navigation to the extent that it prevents the adversary from hitting the required number of targets with its standoff weapons. Space provides a domain in which Russia can affect multiple adversary weapon systems despite it being at a numerical disadvantage with the West. Russia's operational goals are to (1) decrease the combat effectiveness of NATO's aerospace attack, which in turn would lead to a decrease in the effectiveness of NATO's armed forces as a whole; (2) reduce NATO's intelligence capability to target military assets in Russia; and (3) suppress supporting infrastructure required to conduct an aerospace attack, including information and navigation systems.[277]

There are several ways that Russia could degrade or destroy such space-based capabilities as reconnaissance, communications, or navigation satellites. First, and at the high end of the spectrum, Russia has the means to use direct-ascent ASAT weapons that can result in the destruction of an adversary's satellite. Russian ABM and ASAT systems, such as the S-500 and the A-235 Nudol, are thought to provide a kinetic option for destroying satellites or other space vehicles.[278] The debris that would result from the use of these weapons would be problematic for all space users, including Russia. Therefore, these weapons would likely be used in such a capacity as a last resort.

Second, co-orbital systems are satellites that are present in or can be quickly launched into outer space to rendezvous with an adversary satellite and affect it in several ways. They can temporarily disable some of its capabilities through jamming or dazzling its sensors, permanently make it ineffective, or even destroy it by kinetic means. Russia has been testing co-orbital technology since the 1960s, and its latest series of tests began in 2013. These tests included both ground-launched and air-launched co-orbitals. Like any ASAT system, co-orbitals have certain

---

[276] Romanov and Cherkas, 2020, p. 38.

[277] Palitsyn and Zhilenko, 2020, pp. 10–12.

[278] Brian Weeden and Victoria Sampson, eds., *Global Counterspace Capabilities: An Open Source Assessment*, Broomfield, Colo.: Secure World Foundation, April 2021, p. 2-14.

limitations, among which is the time lag between identifying the target satellite and launching the co-orbital so that it can be in a position to rendezvous. However, once a launched space object is established in orbit, it is difficult to determine whether the object has a hostile intent.

A third means of degrading adversary satellites is directed-energy weapons, normally in the form of lasers that can either dazzle (temporary) or blind (permanent) satellites. Russia has developed or is in the process of developing three systems: The Kalina system is a fixed ground-based ASAT system, Peresvet is a mobile ASAT weapon, and Russia continues to work on an airborne ASAT laser called *Sokol-Eshelon*.[279] The advantage of directed-energy weapons is that they can be scaled for effect. In a preconflict phase, Russia can use these systems to dazzle U.S. and NATO satellites as a warning of what it could do during a military conflict. These same systems could be used to blind satellites, potentially rendering them useless, without creating the hazardous debris that would result from a direct-ascent weapon.

Fourth, Russia can apply its EW capabilities against the United States and its allies. Such capabilities could be used during a period of political crisis preceding an actual conflict. Electronic interference of satellites can be reversible, allowing Russian forces to modulate the effects of their EW platforms. Furthermore, GPS jammers within Russian territory can degrade the navigation systems of NATO assets executing an aerospace attack.[280] We will discuss two of Russia's EW systems that would be used to counter NATO space-based platforms, the Tirada-2 and the Bylina-MM.[281]

Finally, Russia could use long-range fires or cyber weapons to target ground-based terminals used to communicate with space assets.[282] In Russia's view, this would be an asymmetric way to use relatively limited resources to exploit a perceived vulnerability in NATO's space-based communication system. As the head of the Russian General Staff Academy argued in a 2021 article,

> All this predetermines the need for a proactive study of the theoretical foundations of new forms of warfare in outer space, such as anti-satellite combat, systematic hostilities to destroy state infrastructure, an orbital satellite battle, an anti-space operation, etc. During these operations, the main efforts will be focused on disorganization of the enemy's command and control system by destroying ground infrastructure supporting the actions of space forces and means. According to [Russian] military experts, this is one of the most vulnerable areas of the United States and NATO. Rejection of their aggressive intentions is directly related to the disabling of reconnaissance, control, and offensive systems.[283]

---

[279] Arbatov, 2020a, p. 113.

[280] Weeden and Sampson, 2021, p. 2-24.

[281] Hendrickx, 2020c.

[282] Beyza Unal, *Cybersecurity of NATO's Space-Based Strategic Assets*, London: Chatham House, July 2019, p. 8.

[283] Zarudnitskii, 2021b, p. 41.

Examining Russia's Counterspace Capabilities

To achieve its strategic objectives in space, Russia has developed several systems that it believes provide an asymmetric counter to U.S. and NATO space-based capabilities. These systems can be categorized as direct-ascent ASAT weapons, co-orbital ASAT systems, directed-energy weapons, EW jammers, and cyber systems. Associated with most of these systems is the required support infrastructure, from launchpads to tracking and communication facilities that are integral to Russian plans to degrade or defeat Western space-based systems. Several of these systems are the progeny of Soviet concepts, some of which date back to the 1960s and 1970s. In this section, we will examine the major Russian systems in further detail and assess their development using available information.

Direct-Ascent ASAT—Nudol, S-500, S-550, and Kontakt

Russia's most mature direct-ascent ASAT weapon is the PL-19 Nudol. It is a two-stage rocket that uses its velocity to kinetically destroy its target. Tracing its ancestry back to Moscow's original ABM defense during the Cold War, the Nudol may have been conceived initially as an ABM system.[284] Unlike the A-135 interceptors that served as the initial ABM system around Moscow, which were nuclear tipped because of the risk of inaccuracy, the Nudol is a hit-to-kill missile. However, the Nudol's primary role appears to be that of a kinetic ASAT weapon capable of hitting satellites in low earth orbit. The system is designed to be stationed on mobile vehicle launchers (transporter-erector-launcher) and consists of a two-stage missile fueled by a solid propellant.[285] Guidance is provided by an internal phased radar array, as well as tracking information provided by the launch control command system and targeting guidance provided by Russia's space tracking facilities.

Nudol testing began in 2014, and Russia tested the system twice in 2020; however, none of the tests targeted an actual satellite. On November 15, 2021, Russia launched a Nudol missile against one of its decaying Tselina-D satellites in low earth orbit at approximately 460 km.[286] The collision resulted in more than 1,500 pieces of debris, a threat that caused the crew of the International Space Station to enter its emergency return capsules for several hours. The intent of the Russian action is unclear. It could have served as a demonstration of Russia's ASAT capability, similar to other weapon tests that are part of a larger deterrence strategy. On the other hand, it could have been an attempt to pressure the United States and other spacefaring nations to come to an agreement on the demilitarization of outer space or, at a minimum, a moratorium on

[284] Weeden and Sampson, 2021, p. 2-15.

[285] Military Russia, "Komplek 14Ts033 Nudol' raketa 14A042," webpage, May 4, 2021.

[286] Ankit Panda, "The Dangerous Fallout of Russia's Anti-Satellite Missile Test," Carnegie Endowment for International Peace, November 17, 2021.

ASAT tests. In any case, it demonstrated the effectiveness of the Nudol system against low earth orbit targets and a willingness on the part of Russia to accept the resulting debris.

Russia also plans to use the S-500 Prometheus, made by Almaz-Antey. This is the fifth-generation ABM system that will be deployed around Moscow. Development of the S-500 began in 2010 as a follow-on SAM to the S-400.[287] Because the S-500 has an exoatmospheric interceptor, it not only is projected to intercept incoming ballistic missiles targeted at Moscow but also could be used to destroy space objects in low earth orbit passing over Russian territory. There are several variants of the S-500, and the 77N6-N is the designation for the S-500 with an ASAT capability. The S-500 was originally supposed to be operational by 2020; however, delays in the program have slipped that forecast by three to five years. Deputy Prime Minister Yuri Borisov announced in September 2021 that the first S-500 ABM was installed around Moscow, but how soon the anti-space 77N6-N will be operational is unclear.[288]

Like the Nudol, the S-500 would be effective against satellites and space vehicles in low earth orbit. Russia has already announced the development of the S-550 kinetic kill vehicle, which might serve as a replacement for the Nudol and be integrated with the S-500 system being installed around Moscow.[289] The S-550 is projected to be operational in 2025; however, the Russian news agency TASS reported it entering service in late December 2021.[290]

In addition, Russia has revived its airborne direct-ascent ASAT known as *Kontakt* or 78M6. Kontakt consists of an ASAT launched from a modified MiG-31D.[291] As with other ASAT systems, the development of an airborne-launched ASAT has been in progress for nearly 40 years. The program for the airborne ASAT initially began in the 1980s, when both the United States and the Soviet Union were experimenting with direct-ascent weapons. The airborne system allowed for a more rapid launch capability, conceivably providing the option of targeting multiple satellites. Two phases of development were planned during the Soviet era, with the goal of hitting satellites at up to 1,500 km.[292] Although some testing did occur, it is doubtful that earlier systems came close to achieving the desired range and accuracy. The economic situation for the Russian government in the 1990s put a hold on further research and development of the airborne system.

---

[287] Center for Strategic and International Studies Missile Defense Project, "S-500 Prometheus," *Missile Threat*, last updated July 1, 2021a.

[288] "First Batch of Russian-Made S-500 System Enters Service – Deputy PM," TASS, September 16, 2021.

[289] "Russia's S-550 Missile Defense System to Intercept Warheads Free of Nuclear Blast – Expert," TASS, November 16, 2021.

[290] "First S-550 Air Defense Systems Enter Service in Russia – Source," TASS, December 28, 2021.

[291] Bart Hendrickx, "Burevestnik: A Russian Air-Launched Anti-Satellite System," *Space Review*, April 27, 2020a.

[292] Weeden and Sampson, 2021, p. 2-20.

In 2009, the renewed desire for an airborne direct-ascent ASAT led the Ministry of Defense to award contracts for Kontakt.[293] The missile was developed by OKB Vympel, which is known for its production of air-to-air missiles. It is a three-stage rocket; the first two stages use a solid propellant, and the final stage uses liquid propellant. Weighing approximately 4,300 kg and 10 m in length, the Kontakt missile is carried aboard the Mig-31D, which climbs to a ceiling of approximately 55,000 ft.[294] As it approaches its ceiling, it zooms up and fires the missile. Guidance to the target is relayed from Russia's Krona space vehicle–tracking complex in the North Caucasus. The estimated range is 120–600 km. In the early 1980s, the Soviets sought to have the capability to shoot down 24 satellites within a 24-hour period. Open sources have not revealed the scope of the Ministry of Defense's requirement; however, Kontakt was scheduled to become operational in 2022.[295]

The Nudol, S-500, S-550, and Kontakt reflect a serious investment in direct ASAT capabilities on the part of Russia. Furthermore, Russia's test of Nudol on one of its decaying satellites in 2021 demonstrates that, from Russia's point of view, it might be willing to risk the use of direct-ascent ASAT weapons—despite the negative effects of creating thousands of additional pieces of space debris—in an attempt to deter, disrupt, and, if needed, destroy an adversary's satellite or space vehicle as part of its aerospace defense. Although the S-500 and Kontakt have yet to become operational, it is clear that Russia has an effective ability to hit targets in outer space with Nudol.

Co-Orbital ASAT Capabilities—Nivelir and Burevestnik

The Soviet Union has a long history of co-orbital weapon development. In the early 1960s, the Soviet Union began developing its *Istrebitel Sputnikov* (IS), or satellite fighter, because of a concern that the United States would develop orbital bombardment systems. An SS-9 rocket would be used as the launch vehicle for the IS, and, once in orbit, the IS would maneuver itself into close proximity to the targeted space vehicle and detonate, causing shrapnel to destroy the spacecraft.[296] The IS system was declared operational in 1973, and testing continued until 1982, with mixed success. Later versions of the IS, designated the IS-M, were able to intercept the target space vehicle after a single orbit, reaching orbits of up to 2,200 km.[297] While co-orbital ASAT testing was suspended during the 1980s, the Soviets continued to develop improved co-

[293] Alexiy Mikhailov and Dmitrii Bal'burov, "Ispytaniia protivosputnikogo kompleksa nachnutsia v kontse goda," *Izvestia*, January 24, 2014.

[294] Mikhailov and Bal'burov, 2014.

[295] Alexei Zakvasin, "Kozyr' v rukave: kakie perspektivnye vidy protivosputnikovogo vooruzheniia razrabatyvaiutsia v Rossii," RT, November 29, 2018.

[296] Laura Grego, *A History of Anti-Satellite Programs*, Cambridge, Mass.: Union of Concerned Scientists, January 2012, p. 2.

[297] Weeden and Sampson, 2021, p. 2-3.

orbital ASATs in the form of *Naryad*, which sought to increase the range of the system up to 40,000 km and provide the ability to launch up to 100 such weapons in short sequence.[298] The collapse of the Soviet Union in 1991 put the development of Naryad on hold.

In 2013, Russia resumed testing co-orbitals. Central to Russia's co-orbital effort is the Central Scientific Research Institute of Chemistry and Mechanics, located in the suburbs of Moscow. The institute was involved in the early co-orbital program of the 1960s and has continued its work on military satellites. Bart Hendrickx notes that it is working on a system referred to as *Nivelir*.[299] Several experts have expressed the belief Nivelir is a space monitoring and tracking system that is connected with Russian co-orbitals. Nivelir suggests a Russian effort to be able to track and target adversary satellites, as mentioned in its theories of conflict in space.

Co-orbitals, with their ability to conduct rendezvous and proximity operations (RPO), present a challenge for determining intent because they can be used for many peaceful purposes, such as the inspection and repair of satellites and intelligence gathering, but also as a weapon system that can degrade, disable, or destroy a satellite. Over the past decade, Russia has continually tested its co-orbital capabilities, and the United States claims that some of these tests have been weapons tests in outer space. In 2013, 2014, and 2015, Russia conducted launches from its Plesetsk Cosmodrome to deploy such co-orbitals. In some cases, the co-orbitals were not disclosed beforehand. For instance, Russia would announce the deployment of three satellites, only to later deploy a fourth satellite. Initial RPO by the satellites were conducted with the upper-stage Briz-KM booster.

Beginning in 2017, however, Russian RPO were conducted using two satellites.[300] In June 2017, Cosmos 2519 deployed and then itself deployed Cosmos 2521 as an inspector satellite. Cosmos 2521 made a number of proximity maneuvers but later returned to Cosmos 2519. Later, Cosmos 2521 deployed its own inspector satellite, Cosmos 2523; this was considered by the United States to be an ASAT test because of the velocity of the separation.[301] In July 2019, Russia launched four military satellites, two of which (Cosmos 2535 and Cosmos 2536) were conducting a series of RPO. In mid-August of that year, during a rendezvous and proximity operation, there was a discharge of nine debris objects that was considered a high-energy event.[302] Additional debris by either Cosmos 2536 or Cosmos 2536 was observed in October and December that same year. Senior U.S. military officials considered this series of events to be evidence of Russian co-orbital weapons testing.

---

[298] Weeden and Sampson, 2021, p. 2-4.

[299] Hendrickx, 2020a.

[300] Weeden and Sampson, 2021, p. 2-6.

[301] U.S. Space Command Public Affairs Office, "Russia Conducts Space-Based Anti-Satellite Weapons Test," July 23, 2020.

[302] Hendrickx, 2020a.

In November 2019, Russia launched Cosmos 2542, which later released a subsatellite, Cosmos 2543. Cosmos 2543 then positioned itself to conduct RPO on the U.S. intelligence satellite USA-245. Cosmos 2543 came within 20 km of USA-245 several times in January 2020. Again, U.S. government officials were critical of the proximity of the Russian vehicle to U.S. satellites. In June 2020, Cosmos 2543 maneuvered to within 60 km of Cosmos 2535; in July, orbital debris was observed between the two satellites.[303] U.S. Space Command asserted that this was a weapons test similar to the activity of Cosmos 2521 and Cosmos 2523 in summer 2017.[304] The activities of Russia's RPO over the past several years indicate that it has the capability to use co-orbitals to degrade, disable, and possibly destroy adversary space vehicles and satellites.

Russia has also conducted RPO in geostationary orbit. In September 2014, Russia launched a geostationary orbit satellite, Luch, which was owned by the GRU.[305] Designated by the United States as the Luch/Olymp satellite, it is likely designed to intercept communications. Over several years, the Luch satellite maneuvered to different locations in geostationary orbit, in some instances placing itself near other countries' communications and military satellites. France complained to Russia when, in 2017, the Luch satellite came too close to a joint French and Italian military communications satellite.[306] So far, the Luch/Olymp system appears to be an intelligence-gathering platform; however, its RPO capabilities make it suitable to perform as a co-orbital ASAT.

A capability related to the co-orbitals discussed above is *Burevestnik*. Burevestnik is an air-launched ASAT system.[307] Similar to the Kontakt direct-ascent ASAT, Burevestnik would be launched from a modified Mig-31 to rapidly place a space vehicle into orbit. This space vehicle could serve as a co-orbital ASAT, much like Cosmos 2543. Maturity of such a system has not been publicly acknowledged, but, at a minimum, such a system is in development. The benefit of using a system like Burevestnik is the ability to conduct rapid launches of ASAT weapons. There are several ways in which a Burevestnik vehicle could damage or destroy a targeted satellite, including the use of nitrogen gas to conceal itself and degrade the other satellite and the use of explosive charges to create fragments. Burevestnik might be related to or a part of the Nivelir co-orbital program led by the Central Scientific Research Institute of Chemistry and Mechanics.[308]

---

[303] Weeden and Sampson, 2021, p. 2-9.

[304] U.S. Space Command Public Affairs Office, 2020.

[305] Weeden and Sampson, 2021, p. 2-11.

[306] John Leicester, Sylvie Corbet, and Aaron Mehta, "'Espionage': French Defense Head Charges Russia of Dangerous Games in Space," *Defense News*, September 7, 2018.

[307] Hendrickx, 2020a.

[308] Hendrickx, 2020a.

Directed-Energy Weapons—Peresvet, Sokol-Eshelon, and Kalina

Russia has also invested in less destructive counterspace capabilities in the form of directed-energy or laser weapons. Perhaps the most developed directed-energy ASAT system in the Russian arsenal is Peresvet. Directed energy is commonly used to either dazzle or blind satellites. Introduced publicly by Putin in 2018, Peresvet is a ground-based laser carried around by mobile trucks. A video released by the Russian Ministry of Defense stated that Peresvet could "efficiently counter any aerial attack and even fight satellites in orbit."[309] Specifically, General Gerasimov acknowledged that the task of Peresvet was to conceal the movements of mobile missiles.[310] The Peresvet systems are stationed at ICBM garrisons in Teykovo, Yoshkar-Ola, Barnaul, and Novosbirsk.[311] The stationing of Peresvet with Russia's newest ICBMs, designated Topol-MR and RS-24, suggests that Peresvet is intended to dazzle satellites that would be tracking the ICBMs. The formal development of Peresvet likely began in 2012 with a contract between the Russian Ministry of Defense and the Russian Federal Nuclear Center–All-Russian Scientific Research Institute of Experimental Physics, based in Sarov. According to Hendrickx, a leading analyst of Russia's military space programs, there are several other pieces of evidence that tie Peresvet to ASAT operations.[312] A video released by the Russian Ministry of Defense noted that Peresvet crews were trained at the Mozhaisky Military Space Academy in Saint Petersburg. In addition, several patents associated with components of Peresvet were linked to the Institute of Laser Physics in Nizhny Novgorod. Contractual and court documents suggest that Peresvet is connected to the 821st Main Space Reconnaissance Center, just east of Moscow, which provides satellite-tracking information that it receives from radars and optical telescopes across Russia. Russia's Peresvet system is its most mature directed-energy weapon and has been operational since 2019.

In addition to ground-based mobile directed-energy weapons, the National Air and Space Intelligence Center has reported that Russia is developing an airborne laser system designed to degrade space-based missile defense sensors.[313] According to Russian Deputy Defense Minister Aleksey Krivoruchko, Russia intends to put Peresvet capabilities on an airborne platform.[314] Airborne directed-energy systems have limitations in that an aircraft in flight provides a less stable platform than a fixed ground-based system and it is harder for an aircraft to generate sufficient power output. However, airborne systems provide their users with greater mobility and

---

[309] Hendrickx, 2020b.

[310] Aleksandr Tikhonov, "Ministerstvo oborony RF otkryto k ravnopravnomu dialogu po obespecheniiu voennoi bezopasnosti," *Krasnaya Zvezda*, December 18, 2019.

[311] Hendrickx, 2020b.

[312] Hendrickx, 2020b.

[313] National Air and Space Intelligence Center, *Competing in Space*, Wright-Patterson Air Force Base, Ohio, December 2018, p. 21.

[314] Oleg Groznyi, "Fundament oboronosposobnosti otechestva nadezhen," *Krasnaya Zvezda*, December 28, 2019.

can often avoid weather conditions that can affect ground-based systems. The *Sokol-Eshelon* system is a laser that is deployed on the A-60 Beriev aircraft, a modification of an Il-76 transport plane.[315] In addition to targeting satellites, Russia's airborne laser program is intended to have the capability to hit aircraft and missiles as part of its defense against aerospace attack. In a possible reference to Sokol-Eshelon, its chief designer at Almaz Antey, Aleksander Ignatyev, stated that Russian systems were designed to "counter air-based and space-based reconnaissance assets in the infrared part of the spectrum."[316]

The development of airborne directed-energy weapons dates back five decades. The initial concept of an airborne laser began in the early 1970s and is associated with Soviet ideas of placing a directed-energy weapon on an orbiting spacecraft.[317] Using an IL-76 aircraft, tests began in 1981, and Russian sources note that, in the mid-1980s, the first airborne platform was successful at shooting down atmospheric balloons at altitudes between 30 and 40 km. A fire destroyed the first test prototype in 1989, and work on the project was discontinued by 1993. Russia revived the idea of an airborne laser with Sokol-Eshelon, at least conceptually, beginning in 2002, around the time that the United States withdrew from the ABM Treaty. Developers of the system include Almaz-Antey, the Beriev Aircraft Company in Taganrog, and Khimpromavtomatika in Voronezh.[318] In 2009, test flights with Sokol-Eshelon are reported to have targeted civilian objects in space, including a Japanese geodetic satellite at an altitude of 1,500 km and possibly the Hubble telescope. A new testbed was designated in 2014, and ground testing of Sokol-Eshelon's laser began in Taganrog. The new test aircraft, designated an IL-76MD-90A, conducted its first flight in 2016. The effectiveness of Sokol-Eshelon has yet to be announced in unclassified sources. Completion of Sokol-Eshelon's research and development was supposed to occur by 2015; however, it appears that the program has not achieved its goals. There are several indications that the program was in jeopardy of cancellation in 2017, but it later received more funding.[319] There is no forecast by Russian military authorities of when the Sokol-Eshelon system could become operational.

In addition, Russia is likely working on a stationary ground-based system designed to dazzle or blind satellites.[320] Known as *Kalina*, the project is associated with the Krona space tracking complex in the North Caucasus. Krona is a radar complex that has a laser optical locator to detect satellites in high orbits. Russia appears to be upgrading the Krona complex with a laser ASAT capability. The concept is tied to the idea of using lasers to help get rid of orbital debris; however, Hendrickx found contractual evidence that the mission of Kalina was for the

---

[315] Military Russia, "A-60/78T6/1LK222," webpage, August 12, 2016.

[316] Hendrickx, 2020b.

[317] Military Russia, 2016.

[318] Military Russia, 2016.

[319] Hendrickx, 2020b.

[320] Arbatov, 2020b, p. 113.

"functional suppression of electro-optical systems of satellites . . . using solid-state lasers and a transmit/receive adaptive optics system."[321] It is possible that Russia intends to provide its Krona space tracking and surveillance complex with the ability to dazzle satellites.

Radio-Electronic Jamming—Tirada-2 and Bylina-MM

As mentioned in Chapter 4 of this report, Russia has significant jamming capability. In the preconflict and conflict phases, Russia would likely use its radio-EW capabilities against NATO. The Russian military has a strong tradition of using EW in a conventional fight, which provides an asymmetry that is particularly suited to space because the effects of electronic jamming can be reversible and local and because it does not create additional space debris. Jamming of satellites can be used throughout the spectrum of conflict, from the posturing phase to an actual conventional or even nuclear war. It is especially useful because its effects can be attenuated to the desired goal, be it to degrade or to destroy the targeted satellite. Of note, Russia employs several radio-electronic jamming systems against communications and reconnaissance satellites, even though their primary design is to interfere with ground and airborne assets.

On land, Russia has deployed a system of GPS jammers within its territory that is intended to disrupt the navigation systems of weapons that would be launched against its territory.[322] In space, Russia is also applying EW to counter space-based capabilities. Russia is developing two systems that are designed to conduct uplink jamming of communications satellites: the Tirada-2S and the Bylina-MM. The Tirada-2 is a descendant of the Soviet Tirada-1 jammer. Development of the Tirada-2 began in 2001, and there are several versions of the base system, depending on which band of the electronic spectrum it targets.[323] An article in the *Military Industrial Courier* (VPK) states that the Tirada-2S generates interference at the satellite's aimpoint with such energy that the satellite can overcome the electromagnetic screen only through a large expenditure of the its energy resources.[324] The same article asserts that the Tirada system could disable communications satellites. A more technical explanation of the Tirada's capabilities is provided in the previous chapter.

The other Russian uplink jammer is the Bylina-MM system. The Bylina is described as a C2 system for radio-electronic jamming with additional subunits.[325] The Bylina-MM targets satellites operating in the extremely high–frequency or millimeter band of the electronic spectrum. There is also a Bylina-KV variant that targets in the Ka-band. The Bylina-MM's mission is to "suppress the on-board transponders of the millimeter band communications

---

[321] Hendrickx, 2020b.

[322] Weeden and Sampson, 2021, p. 2-24.

[323] Hendrickx, 2020c.

[324] Vitalii Orlov, "Voina nevidimaia i effektivnaia: Sovremennye kompleksy REB sposobny neitralizovat' edva li ne liuboe oruzhie protivnika," *Voenno-promyshlennyi kur'er (VPK)*, August 24, 2021.

[325] Hendrickx, 2020c.

satellites Milstar, GBS, Skynet, Sicral, Italsat and Sakura," used by "leading foreign countries."[326]

In addition to ground-based jammers, in 2018, the Russian press observed that Russia is developing an aircraft with the capability to jam satellites. The Porubshchik-2 EW aircraft, using an Ilyushin Il-22 airframe, is designed to interfere with an adversary's airborne and ground weapon systems but is also supposed to be capable of jamming satellites in low earth orbit.[327]

Russia also has two systems that would interfere with space-based radar reconnaissance satellites. These types of satellites are able to make high-resolution images, even in bad weather and at night. The Dvinomorye-U system, mentioned in the previous chapter as an anti-radar jammer, is reported to also be able to sufficiently interfere with radar-tracking satellites enough to degrade their ability to track ground-based targets.[328] The Krasukha-4 is a slightly more antiquated system whose development dates back to the 1990s. It might ultimately be replaced by the Dvinomorye-U system and has also been reported as effective against radar-tracking satellites in low earth orbit.[329]

Finally, Russia appears to be applying its radio-electronic jamming effort toward civilian satellites. In 2016 *Izvestiya* reported that Russia was developing a Complex of Electronic Warfare for Countering Satellite Systems in Low Circular [earth] Orbits (KRBSS).[330] More recently, a 2021 article noting SpaceX's more than 1,000 satellites as part of its Starlink project says that KRBSS was able to block signals from commercial satellites. It states, "At the direction of the Russian Ministry of Defense, the Moscow Research Radio Engineering Institute has developed a state-of-the-art electronic warfare system against signals propagated by low-orbit satellite communication systems such as Starlink, OneWeb, etc."[331] It is unclear what kind of jamming system KRBSS is or whether it is simply a term used to describe an overarching system made up of other known satellite jammers, such as the Tirada or the Bylina-MM, but references to KRBSS suggest that the targets of Russia's military actions in space include civilian satellite systems that make up critical communications and information infrastructure of the United States and its allies.

Disrupting Space Vehicles Through the Cyber Domain

Perhaps a more likely form of counterspace activity from Russia will come from the cyber domain. Unclassified sources note the threat that cyber activities can pose to spacecraft;

---

[326] Hendrickx, 2020c.

[327] "Source Reveals Tech Details of New Russian Anti-Satellite Warfare Plane," Sputnik News, July 9, 2018.

[328] Orlov, 2021.

[329] Hendrickx, 2020c.

[330] Alexsey Ramm, "Minoborony smozhet zaglushit' Iridium I OneWeb," *Izvestiya*, August 30, 2016.

[331] Connect, "Starlink vziala rubezh v 1000 sputnikov obzor zarubezhnoi pressy po tematike sputnikovoi sviazi za fevral' 2021 goda," January 3, 2021.

however, public knowledge of Russia's ability to affect U.S. and NATO space-based platforms is scant. As is mentioned in the following chapter, Russia maintains a robust cyber capability, which it counts on to provide an asymmetric advantage against its adversaries. In the space domain, Russia is likely to use cyber technology to disrupt NATO's space assets. Modern examples are not public; however, in 1998, hackers based in Russia accessed a U.S.-UK-German ROSAT satellite and changed its rotation toward the sun, which rendered its sensors unusable.[332] Faced with the deployment of thousands of military and dual-use satellites by its adversaries, Russia cannot rely only on its counterspace weapons. It will have to try to use its cyber capabilities to penetrate space-related ground systems to disrupt U.S. and NATO space operations.[333]

It is not possible to identify with specificity Russian cyber units or capabilities that have been assigned counterspace missions. What can be surmised is that vulnerabilities exist in space-based systems and cyber units can attempt to exploit those vulnerabilities to disrupt space operations. In general, the National Air and Space Intelligence Center has noted Russia's intent to use cyber capabilities against space assets and has grouped those threats into four areas.[334] First is the threat to ground facilities in the form of hacking, hijacking, and malware. Second is the threat to users through spoofing, denial of service, and malware. Third, Russian cyber actors can attack the link between ground stations and satellites through command intrusion, spoofing, and replay. Finally, albeit more challenging, space assets can be attacked themselves through command intrusion, payload control, denial of service, and malware.

Russia's Space Support System

Effective space and counterspace operations require substantial support facilities, from launch sites to tracking stations. Russia views itself as second only to the United States in terms of its space support infrastructure, and, over the past two decades, it has been gradually modernizing and upgrading its facilities. Russia's space surveillance system consists of launch facilities, C2 centers, and a wide array of systems that monitor objects in outer space.

Russia maintains launch facilities at Plesetsk and Kapustin Yar, as well as Sary Shagan and Baikonur, both located in Kazakhstan.[335] An additional Cosmodrome, known as *Vostochnyi*, is currently under construction in Russia's Far East to reduce Russia's dependence on its Baikonur facility. Although there have been some launches from Vostochnyi since 2015, completion of the launch facility has been delayed. Baikonur remains Russia's most famous launch facility, as it was the primary facility during Soviet times and serves as the main facility for Russia's civilian

[332] Weeden and Sampson, 2021, p. 9.

[333] Arbatov, 2020b, p. 90.

[334] National Air and Space Intelligence Center, 2018, p. 19.

[335] Weeden and Sampson, 2021; see Ch. 11.

space program. Sary Shagan is where Russia conducts most of its ABM testing for the Nudol system. Plesetsk, located south of Russia's northwest city Arkhangelsk, is the most active military launch site where Russia launches its co-orbital systems and is currently the primary location for the Nudol ASAT system. Kapustin Yar, located near Volgograd, is also a Nudol launch site.

Russia also maintains an array of space surveillance control facilities, which make up its Russian Outer Space Control System. Russia's civilian and military functions overlap in some areas, and, as with most national surveillance systems, information is shared. Control of Russia's military space and counterspace assets takes place from several facilities around Moscow, including the 821st Main Space Surveillance Centre, the 820th Main Centre for Missile Attack Warning, and the 153rd Main Trial Centre for the Testing and Control of Space Means. The three control centers are part of Russia's Outer Space Control System.

Russia's primary space surveillance assets are Okno and Krona. Russia maintains an Okno complex near Nurek, Tajikistan, which it recently upgraded. Okno uses ten electro-optical sensors, which have an estimated range of detection of 40,000 km, to monitor space objects in low earth orbit and geostationary orbit.[336] Work has reportedly begun on a second Okno site in Primorski Krai, in Russia's Far East. The Krona complex near Starozhevaya, in the North Caucasus, uses electro-optical and radar sensors for the identification and tracking of space objects. The Krona complex in Starozhevaya also has an associated 30J6 component facility that uses optical telescopes and lasers.[337] Russia had planned to build four Krona facilities; at the moment, however, only a second Krona complex is being developed, near Nakhodka in the Far East. In addition, the Altai Optical Laser Centre, near Savvushka, Siberia, provides high-resolution images of space objects.[338]

Russia also receives information from international partnerships. Russia benefits from its participation in the International Scientific Optical Network (ISON), which it manages from its Keldysh Institute of Applied Mathematics. ISON is a consortium of 30 observation facilities in 16 countries that share information on the location and trajectory of space objects. Established in 2001, ISON shares data on space objects in low earth orbit, geostationary orbit, and high earth orbit, including the tracking of asteroids.[339] It provides Russia with space tracking data from multiple points around the globe. Finally, it is worth noting that some of Russia's ABM early-warning sites have utility in providing information on space objects. Most notable is the Voronezh phased array radar, which serves as a ballistic missile warning radar. The Voronezh is

---

[336] Allen Thompson, *Sourcebook on the Okno, Okno-S, Krona and Krona-N Space Surveillance Sites*, Federation of American Scientists, November 19, 2014, p. 6.

[337] Weeden and Sampson, 2021, p. 11-35.

[338] Allen Thompson, *The Altay Optical-Laser Center Sourcebook*, Federation of American Scientists, March 29, 2011, p. 3.

[339] Weeden and Sampson, 2021, p. 2-36.

replacing older warning systems with approximately eight sites, which are either completed or under construction.[340] In sum, over the past two decades, Russia has invested in upgrading and modernizing its space support structure in anticipation of increased space activity on its part and that of its adversaries.

Conclusion

Since the early 2000s, Russia has reinvigorated its military space and counterspace capabilities. Much of their development is a continuation of Soviet legacy systems that were periodically delayed because of arms control, political, or financial considerations. The U.S. withdrawal from the ABM Treaty, combined with Russian observations on conflict in the 21st century, leads Russian military leaders to prioritize and prepare for conflict in space. This is especially important because Russia views U.S. and NATO dependency on its satellite systems as a potential vulnerability that can be exploited to Russia's advantage. Space is seen as a domain that is essential to NATO's military capability.

Russia's effort to develop its counterspace capabilities as part of a notional unified strategic operation is one that is deserving of attention by the United States and its allies. As shown in this chapter, Russia is developing such capabilities using multiple means, from direct-ascent ASATs to jamming and cyber capabilities. Its recent test of the Nudol ASAT missile and its weapons testing on co-orbitals through its Nivelir system demonstrate both an improved capability and the will to use kinetic weapons against space-based assets. Still, it is unclear whether Russia believes that its counterspace capabilities are sufficient to achieve its objectives, despite pronouncements in the open press.

We do not know how Russia would sequence its counterspace operations, although the sequence of tasks in Chapter 1 suggests that Russian actions to disrupt NATO space surveillance could take place early in a conflict. There are the three command centers around Moscow, but the roles and types of activities that would be used as the conflict escalates are unknown. Counterspace is one of several capabilities addressed in this report that is available to the Kremlin which can impede an aerospace attack from the West until a resolution is achieved. Some of these capabilities, such as Russia's direct-ascent weapons, are costly in terms of the debris that they create when used, and they can also negatively affect space vehicles in low earth orbit, as seen in the recent test of Nudol. Nonetheless, they might be worth it as a form of demonstration or to hit high-value space targets. At the same time, Russia continues to improve ASAT systems that are more measured and that can be reversible. Radio-electronic jamming systems and directed-energy weapons provide such a capability. While less is known in unclassified reporting about the capabilities of Russia's co-orbital program, it appears that Russia is experimenting with different co-orbital ASAT capabilities. Similarly, our knowledge of

[340] Weeden and Sampson, 2021, pp. 2-34–2-35.

Russia's ability to disrupt U.S. and allied space operations through cyberspace is limited (see Chapter 6).

Russia's counterspace programs contain several shortcomings that could reduce the Russian military's ability to functionally suppress NATO's use of its space-based capabilities in a conventional or nuclear fight. Many of Russia's aforementioned counterspace systems and much of Russia's thinking evolved from the Soviet era. During the Cold War, the Soviet state was the driver of space technology and capability. The number of orbiting satellites was relatively small because the cost of launch was expensive. As a result, satellites carried multiple payloads. Incapacitating a high-use satellite using a direct-ascent ASAT like the Nudol or an air-launched co-orbital killer satellite, such as the Burevestnik, was a reasonable asymmetric option. The ability to jam a small number of satellites that rely on direct links with terrestrial stations also made jamming a viable countermeasure. In addition, Russia held an advantage for several years as one of the few launch providers. However, changes in technology and the rise of the commercial space sector in the West pose significant challenges to Russia's ability to disrupt NATO operations in space.

Unlike Russia, whose space industry is overwhelmingly state driven and resourced, the West has benefited from an expansion of its commercial space sector. This civilian capacity and innovation has resulted in an exponential increase in the number of satellites, as well as improvements in the costs, capabilities, and sizes of the vehicles. This development has several consequences for Russia's counterspace capabilities. First, the dispersion and proliferation of smaller satellites, including dual-use satellites, make it harder for direct-ascent ASATs and co-orbital ASATs to target enough satellites. The number of targets can surpass the number of ASATs, and, even if satellites become disabled, the growth in launch capability and the ability to replace satellites in rapid order with greater launch capacity reduce the effectiveness of kinetic weapons. Perhaps more significant is the development of intersatellite links, which allow satellites, particularly in low earth orbit, to transmit to each other to facilitate communication and provide redundancy. Space-based optical communications made with laser technology can reduce the effectiveness of jamming and allow greater security against cyber intrusions.[341] It is perhaps for this reason that Russia is investigating an orbital jammer with sufficient power to conduct interference from space. That idea appears to be in the conceptual phase, however.

Finally, Russian limitations in counterspace have resulted in a push for space arms control. Russian experts, such as Alexey Arbatov and the Russian Foreign Ministry, have promoted a new treaty limiting weapons in space.[342] Submitted jointly with China, the proposed treaty would limit the testing of ASAT and space-based weapons. Russia argues that the proposed treaty

---

[341] Kevin P. Chilton and Lukas Autenried, *The Backbone of JADC2: Satellite Communications for Information Age Warfare*, Arlington, Va.: Mitchell Institute for Aerospace Studies, Mitchell Institute Policy Paper, Vol. 32, December 2021, pp. 23–24.

[342] Arbatov, 2019, pp. 154–158.

would contribute to strategic stability, but such a treaty is also viewed by the Kremlin as a means for offsetting the advantage that the United States has over Russia in terms of space power. However, the push for arms control in some ways inhibits Russia's ability to test and deploy counterspace systems. As a result, Russia can be expected to continue to pursue asymmetric ways to degrade NATO's operations through the space domain, although Western proliferation of space-based assets puts pressure on Russia's counterspace capacity.

6. Russian Cyber Operations to Attack Critical Infrastructure

Introduction

Russian defense strategy broadly refers to the importance of using information, and information technologies, to achieve economic, political, and military goals.[343] Russian military strategists view information warfare as having both technical and psychological components.[344] As the predominant technical means of conducting information warfare, cyber operations are viewed as a mechanism to dominate the information environment.[345] Moreover, cyber operations are seen as a particularly low-cost means of achieving certain military effects.[346]

The opacity of Russian cyber actors and, in particular, the difficulty of tying Russian state actors to specific offensive cyber operations make it difficult to make definite statements regarding Russian intentions in cyberspace, the nature of ties between Russian state and nonstate actors, and official Russian perceptions of the role of cyber operations in broader military strategy. The analysis in this chapter relies on a variety of Russian and English language scholarship, including books and articles written by Russian military scholars and experts on cybersecurity. This scholarship represents a variety of Russian and Western viewpoints on Russian cyber operations, but, because it was not possible to conduct interviews with Russian experts for this research, our findings should be treated as preliminary on this issue and might not be perfectly reflective of Russian perceptions and intentions in the cyber domain.

In this chapter, we begin by considering the historical factors that led to the development of cyber capabilities in Russia in the years following the fall of the Soviet Union. We then examine the major state and nonstate actors involved in Russian cyber operations and discuss their interrelationships, roles, and responsibilities. Finally, we consider ways in which cyber capabilities might be harnessed as part of a unified strategic operation, the role of cyber operations in future war, and factors that could prevent Russia from fully realizing the possibilities associated with cyberwarfare.

---

[343] P. I. Antonovich, "On the Modern Understanding of the Term 'Cyberwar,'" *Bulletin of the Academy of Military Sciences*, No. 2, 2011, p. 89.

[344] For a discussion of the informational-technical and informational-psychological components of information warfare, see Michelle Grisé, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, and Khrystyna Holynska, *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation*, Santa Monica, Calif.: RAND Corporation, RR-A198-8, 2022, pp. 10–13.

[345] Bilyana Lilly and Joe Cheravitch, "The Past, Present, and Future of Russia's Cyber Strategy and Forces," in T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, and G. Visky, eds., *2020 12th International Conference on Cyber Conflict*, Tallinn: IEEE, 2020, p. 133.

[346] Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare*, Arlington, Va.: CNA, March 2017, p. 3.

Historical Background

The role of cyber operations as an element of contemporary Russian military strategy dates back several decades. The fall of the Soviet Union occurred in the early 1990s, a time when computers were becoming increasingly accessible to ordinary people in their homes. In Russia, these concurrent events facilitated the growth of small communities of hackers, particularly in cities and towns where the collapse of the Soviet Union had led to more-severe economic turmoil. As investigative journalist Daniil Turovsky explains, in the 1990s, increased interest in hacking and the formation of groups of hackers were especially noticeable in the cities of Siberia. According to Turovsky, during the Soviet period, economic life in these cities had typically been "organized around a large industrial enterprise."[347] With the fall of the Soviet Union, however, in the typical Siberian town, "the plant closed and most of the residents lost their jobs."[348] Over the course of the 1990s, there was an increasing sense of "dissonance between [this] everyday Russian reality," on the one hand, and the seemingly "endless possibilities of the Internet," on the other.[349] With the growth of communities of hackers across Russia, a "market for buying their services gradually began to form."[350] By the early 2000s, as online forums for hackers emerged, hacking "began to turn into an industry" and hackers "gradually evolved into de facto organized groups."[351] At the same time that these online forums were providing a space for hackers to develop their skills, more-formal options for acquiring computer skills also emerged as technical universities across Russia created new information technology and security departments.[352]

As the Russian hacking community grew, there were early indications that the Russian defense establishment understood the military possibilities of cyber operations. As Jensen explains, in the first few years after the fall of the Soviet Union, Russian military experts recognized that cyberattacks could be used to achieve military effects against an adversary's "communication, reconnaissance, early warning, logistics, and weapons platforms at the tactical and operational levels."[353] Beginning in 1996, a group of Russian hackers called Moonlight Maze gained access to U.S. government and university networks, including those of the U.S. Department of Defense, the U.S. Department of Energy, and the National Aeronautics and Space

---

[347] Daniil Turovsky, *Vtorzhenie: Kratkaya Istoriya russkikh khakerov*, 2019, p. 35.

[348] Turovsky, 2019, p. 35.

[349] Turovsky, 2019, p. 39.

[350] Turovsky, 2019, p. 44.

[351] Turovsky, 2019, p. 57.

[352] Turovsky, 2019, p. 46.

[353] Mikkel Storm Jensen, "Russia and Cyber – Espionage, Sabotage and the Constant Fight for the Truth," in Niels Bo Poulsen and Jørgen Staun, eds., *Russia's Military Might: A Portrait of Its Armed Forces*, Copenhagen: Djøf Publishing, 2021, p. 336.

Administration. The intrusions were uncovered in 1999, by which time the group had "stole[n] a significant number of documents" and provided network access to the FSB.[354]

In the aftermath of the Moonlight Maze attack, the Western media began referring to a new "cold cyberwar" with Russia.[355] In the years that followed, Russia conducted notable cyberattacks in Estonia, Georgia, and Ukraine. In April 2007, the Estonian government removed a Soviet monument in downtown Tallinn. In response, Russian hackers unleashed botnet attacks on Estonian websites.[356] The next year, in the weeks leading up to the Russian invasion of Georgia, Russia conducted a series of distributed denial-of-service (DDoS) attacks on Georgia's internet infrastructure. The attacks, which overloaded and shut down Georgian servers, continued after Russia invaded Georgian territory. Commentators characterized the episode as the "first time a known cyberattack had coincided with a shooting war."[357] During the annexation of Crimea, Russian soldiers "attacked . . . physical cyber infrastructure," including optical fiber cables and internet communication platforms.[358] In December 2015, Russia hackers attacked electricity firms in Ukraine, causing power outages in western Ukraine.[359] Since then, Russia has

> utilized spear phishing, malware, DDoS attacks, telephone denial of service (TDoS) attacks, and other forms of cyber disruption . . . to conduct a steady drumbeat of cyberattacks targeting Ukraine's government, military, telecommunications, and private-sector information technology infrastructure.[360]

Estonia, Georgia, and Ukraine have "served as testing grounds and signaling arenas" for Russia, "providing opportunities for [Russian hackers] to refine their cyberwarfare techniques and procedures while demonstrating their capabilities on the world stage to influence or deter Russia's adversaries."[361]

Russian Cyber Actors

Today, there is a "complex web" of state and nonstate actors, including intelligence and military agencies, commercial actors, criminal organizations, and individuals, that are involved

---

[354] Turovsky, 2019, pp. 43, 126, 189.

[355] Turovsky, 2019, p. 62.

[356] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007.

[357] John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008.

[358] Jensen, 2021, p. 348.

[359] Daniel McLaughlin, "Ukraine Blames Russian Hackers for Airport Attack," *Irish Times*, January 18, 2016.

[360] Connell and Vogler, 2017, p. 19.

[361] Connell and Vogler, 2017, p. 27. For additional discussion of these cyberattacks, see Dorothy Denning, "Tracing the Sources of Today's Russian Cyberthreat," *Scientific American*, August 18, 2017.

in Russian cyber efforts and operations.[362] These actors "have different—yet often overlapping and competing—roles, responsibilities, and influence in implementing cyber-enabled active measures against domestic and foreign adversaries."[363] Both state and nonstate actors have been "actively developing cyber weapons and cyber defense systems" in recent years.[364] This section identifies the major state and nonstate actors involved in Russian cyber operations and describes their respective roles and characteristics.

State Actors

For many years, cyber operations were the "exclusive domain of [Russia's] security services," and the FSB led the coordination of early cyber and disinformation campaigns.[365] In the 1990s, Russia briefly created a separate information security agency, called the Federal Agency for Government Communications and Information (FAPSI). FAPSI was disbanded in 2003, and the FSB "inherit[ed] the bulk" of the organization's personnel and capabilities.[366] This move provided the FSB with an early advantage in developing offensive and defensive cyber capabilities.[367] Today, the FSB's Center for Information Security (CIS) oversees offensive cyber operations against foreign targets.[368] It also surveils internet communications within Russia using its System for Operative Investigative Activities, an internal cyber surveillance system.[369]

Recently, the GRU has played an increasingly prominent role in conducting cyber operations. This stemmed from concerns, which emerged in the 2010s, regarding Russia's apparent "unpreparedness for . . . an inevitable information confrontation with the West."[370] As a result, Russia took steps to diversify the state agencies responsible for conducting cyber research and cyber operations.[371] The GRU, in particular, became a bigger player in the cyber sphere. The GRU's cyber enterprise has been compared to that of the National Security Agency, consisting

---

[362] Robert Morgus, Brian Fonseca, Kieran Green, and Alexander Crowther, *Are China and Russia on the Cyber Offensive in Latin America and the Caribbean? A Review of Their Cyber Capabilities and Implications for the U.S. and Its Partners in the Region*, Washington, D.C.: New America, July 2019, p. 19.

[363] Morgus et al., 2019, p. 20.

[364] Turovsky, 2019, p. 129.

[365] Connell and Vogler, 2017, p. 7.

[366] Lilly and Cheravitch, 2020, p. 139. Some elements of FAPSI were absorbed into the Ministry of Foreign Affairs, the Federal Protective Service of the Russian Federation, and the Foreign Intelligence Service (Connell and Vogler, 2017, p. 7).

[367] Lilly and Cheravitch, 2020, p. 139.

[368] Jensen, 2021, p. 340. Turovsky cites an interview by *Hacker* magazine with an employee of CIS who stated that hackers came to work for the FSB to "realize their beliefs" and support Russian national objectives (Turovsky, 2019, p. 149). CIS is also referred to as the *Second Division of FSB Center 18*.

[369] Connell and Vogler, 2017, p. 7.

[370] Lilly and Cheravitch, 2020, p. 140.

[371] Lilly and Cheravitch, 2020, p. 140.

of network operators who operate in a "very formal code environment" and conduct "research into cyber vulnerabilities, exploits, and code development."[372] GRU information operations teams work closely with network operators to access critical systems while simultaneously disseminating fake information via social media.[373] As discussed later in this section, the GRU also outsources certain aspects of cyber operations to so-called patriotic hackers—individuals or groups that conduct cyberattacks on behalf of state actors. Turovsky and others have alleged that hackers working on behalf of the GRU were behind the 2016 cyberattacks on the U.S. electoral system.[374] Many of the major cyberattacks that have occurred in the past five years have been linked to GRU efforts.[375] As a result of these high-profile attacks, the GRU has gained a reputation for having a high tolerance for operational risk in the cyber domain, which experts have described as "incongruent with the traditionally furtive realm of cyber operations."[376] Compared with the FSB and other state cyber actors, the GRU has "demonstrated [a] greater willingness to take risks and emphasized action over secrecy."[377] Whether the GRU continues to hold responsibility for prominent cyber operations will likely depend on whether the organization successfully balances this predisposition for risk-taking with the strategic necessity for Russia of maintaining a degree of plausible deniability.

The work of state agencies is also supported by an ecosystem of state research institutes, most of which are associated with the Ministry of Defense and provide cyber research and support to operations.[378]

Nonstate Actors

In addition to the state actors described above, various nonstate actors support Russian cyber operations. Among these nonstate actors are several commercial companies, including the Internet Research Agency, Concord Consulting, Digital Security, Kvant Scientific Research

---

[372] Morgus et al., 2019, p. 20.

[373] Morgus et al., 2019, p. 20.

[374] Turovsky, 2019, p. 195. Turovsky specifically alleges that GRU officers were responsible for attacks on "more than three hundred computers associated with the U.S. Democratic National Committee." Turovsky acknowledges, however, that Russia "continues to deny the attacks," and some experts still doubt that the GRU has the in-house capabilities necessary to carry out such a sophisticated cyber operation (p. 197).

[375] Jensen, 2021, p. 341.

[376] Lilly and Cheravitch, 2020, p. 141.

[377] Jensen, 2021, p. 341. Jensen traces this propensity to the organization's ties with Russian special forces units.

[378] Turovsky, 2019, p. 161.

Institute, and Kaspersky Labs.[379] As Turovsky describes, there is an ongoing flow of cyber personnel between these companies and Russian security and military services.[380]

As noted above, individuals and hacker groups, sometimes referred to as *patriotic hackers*, play a role in supporting Russian cyber operations. This trend dates back to Russia's intervention in Chechnya, which Turovsky cites as the "first conflict in which Russian hackers sided with the state."[381] In recent years, the GRU in particular has outsourced aspects of its offensive cyber operations to patriotic hackers. This reliance on nonstate actors to support state cyber actions has its roots in the historical lack of technical capabilities within the security services. As Turovsky explains, the CIS historically had "few technical staff," despite its decidedly technical mission, and it still "often use[s] outside specialists."[382] The co-opting of patriotic hackers to support state-led cyber operations has significant benefits for Russia, especially because it creates a "deliberate blurring of the lines between state and nonstate actors" and makes it more difficult to attribute cyberattacks to Russian state actors with a high degree of certainty.[383] Not only does the use of patriotic hackers provide Russia with plausible deniability, but it is also cost-effective, "as hackers can be summoned to unleash attacks only when needed, and patriotic hackers will also often work for free."[384] As discussed later in this chapter, recent attacks on critical infrastructure targets, including the Colonial Pipeline and the U.S. health care system, provide concrete examples of the way in which patriotic hackers and Russian cybercrime organizations work in support of Russian objectives while providing Russia with some degree of plausible deniability.

The extent to which Russian state actors rely on patriotic hackers remains unclear. Experts have generally characterized the activities of patriotic hackers as "somewhere on the spectrum between state-integrated and state-ignored."[385] The efforts of patriotic hackers frequently align with official Kremlin objectives, however, which lends credence to the alleged linkages between nonstate hackers and state cyber operations.[386] From a personnel perspective, there appears to be a porous relationship between the Russian security services and the hacker community, with state

---

[379] Morgus et al., 2019, pp. 22–23. Concord Consulting has provided financial backing to the Internet Research Agency. Digital Security and Kvant have allegedly provided technical support to FSB cyber operations. Kaspersky Labs allegedly has a relationship, albeit an unclear relationship, with the Russian security services.

[380] Turovsky, 2019, p. 160.

[381] Turovsky, 2019, p. 130.

[382] Turovsky, 2019, p. 149.

[383] Valeriy Akimenko and Keir Giles, "Russia's Cyber and Information Warfare," *Asia Policy*, Vol. 15, No. 2, April 2020, p. 71.

[384] Janne Hakala and Jazlyn Melnychuk, *Russia's Strategy in Cyberspace*, Riga: NATO Strategic Communications Centre of Excellence, June 2021, p. 21.

[385] Morgus et al., 2019, p. 23.

[386] Connell and Vogler, 2017, p. 10. As Turovsky notes, although there is limited evidence of direct ties between hackers and the Russian authorities, the "main evidence still remains that [their] attacks are actually carried out in the interests of the Russian authorities" (Turovsky, 2019, p. 193).

actors frequently inducing or even coercing individual hackers with desired technical skills to work in support of state cyber operations and some hackers even being hired into full-time jobs with state agencies.[387] This inducement may take the form of either payment or, for those hackers who have run afoul of the law, reduced prison sentences.[388]

Cyberattacks Against Critical Infrastructure

Within the context of a notional unified strategic operation, cyber operations could be employed to magnify the effects of conventional operations. However, Russian military experts especially emphasize the utility of harnessing cyber operations to achieve effects against critical infrastructure targets. The importance of targeting critical infrastructure stems from the outsized effect that the disruption of related services can have on both military and civilian populations. Critical infrastructure facilities are viewed as "vitally important for a country" because "the disruption of their work or their total destruction" can "have irreversible negative effects on national and economic security, health care, [and] law and order."[389] Not only can targeting critical infrastructure cripple an adversary's military capabilities by eliminating access to civilian services during a conflict, but these targets are especially vulnerable to cyber intrusions. Cyberattacks on critical infrastructure can even have a "potential[ly] destructive impact on military systems" absent the "direct invasion of [an adversary's] territory"; one group of Russian experts characterizes this dynamic as a "distinctive feature of the global critical infrastructure."[390] Although physical weapons can also be used to disrupt or destroy critical infrastructure, cyber capabilities provide the possibility of "maintain[ing] control of practically any asset of the critical infrastructure" without entering an adversary's territory.[391] Cyber operations can also be used in conjunction with "physical attacks against . . . critical infrastructure and key state resources" to degrade these systems.[392]

There is a particular emphasis on the use of cyber operations to disrupt or destroy critical infrastructure targets in Russian military scholarship. The official Russian definition of *information infrastructure* is "a complex of objects of informatization, information systems, sites on the Internet, and communication networks," which includes "critical information

[387] Akimenko and Giles, 2020, p. 71. See also Turovsky, 2019, p. 149.

[388] Hakala and Melnychuk, 2021, p. 21.

[389] Yu. I. Starodubtsev, P. V. Zakalkin, S. A. Ivanov, "Warfare in the Technosphere as the Basic Method of Settling Conflicts amid Globalization," *Military Thought*, Vol. 29, No. 3, 2020, p. 82.

[390] Starodubtsev et al., 2020, p. 83.

[391] Starodubtsev et al., 2020, p. 83.

[392] Starodubtsev et al., 2020, p. 83.

infrastructure."[393] Russian experts have assessed that not only has the likelihood of cyberattacks on Russian critical infrastructure targets increased in recent years; these attacks are increasingly "more complex, more frequent, and more coordinated."[394] These assessments have likely been informed by lessons learned from the Stuxnet cyberattack on the Iranian nuclear program, which led Putin to instruct the FSB to create GosSOPKA, a state agency responsible for "detecting, preventing, and eliminating the consequences of cyberattacks" within Russia.[395] Russian perceptions of cyberspace focus on the notion that Russia is under constant threat of external cyberattack.[396] One of Russia's stated interests in cyberspace is ensuring the uninterrupted functioning of Russian critical information infrastructure in the face of such attacks.[397] This perception is reinforced by the understanding that Russian communications networks and critical infrastructure assets have become increasingly reliant on cybernetic systems, which "encourages [their] unregulated remote control" by nefarious foreign actors.[398] As a result, the Russian security services perceive the "need to defend government sites and critical infrastructure," including "nuclear power plants, military plants, supply systems and other facilities," from "successful [cyber]attacks which could cause environmental or financial disaster and lead to human casualties."[399]

In recent years, however, there have been indications that Russia is not just focused on defending critical infrastructure assets from cyber intrusions but rather, as one expert writes, is "actively making both offensive and defensive [cyber] preparations."[400] Experts have characterized Moscow as "signal[ing] that it intends to bolster the offensive as well as the defensive cyber capabilities of its armed forces."[401] This characterization stems, in part, from Russia's announcement in 2013 that it intended to create a cyber unit in the Russian military that would be responsible for both offensive and defensive cyber operations.[402] In the years since, according to the U.S. Cybersecurity and Infrastructure Security Agency, Russian actors have

---

[393] Martti J. Kari, *Russian Strategic Culture in Cyberspace: Theory of Strategic Culture – A Tool to Explain Russia's Cyber Threat Perception and Response to Cyber Threats*, Jyväskylä: University of Jyväskylä, JYU Dissertations 122, 2019, p. 54.

[394] Kari, 2019, pp. 54–55.

[395] Turovsky, 2019, p. 217.

[396] Christer Pursiainen, "Russia's Critical Infrastructure Policy: What Do We Know About It?" *European Journal for Security Research*, Vol. 6, 2020, p. 28.

[397] Kari, 2019, p. 60.

[398] Starodubtsev et al., 2020, p. 82.

[399] Turovsky, 2019, p. 209. To support defensive cyber efforts, various commercial companies in Russia, such as Positive Technologies and Kaspersky Labs, produce critical infrastructure–protection tools (Turovsky, 2019, p. 220).

[400] Pursiainen, 2020, p. 28.

[401] Connell and Vogler, 2017, p. 28.

[402] Connell and Vogler, 2017, p. 8.

engaged in multiple efforts to target U.S. government entities and critical infrastructure targets.[403] These efforts include the ransomware attack perpetrated by a Russian cybercrime organization known as DarkSide against Colonial Pipeline, one of the largest pipelines in the United States, in June 2021. The attack led to the temporary shutdown of the pipeline to contain the breach, resulting in long lines at gas stations on the East Coast.[404] Although the Biden administration refrained from characterizing the event as a nation-state attack, this episode represents an example of a Russian nonstate actor with close ties to the Kremlin working to promote Russian interests. As one commentator explained, Russia "benefit[ed] politically from the chaos of this attack . . . even if the weapon [was] in someone else's hands."[405] Another example of Russian efforts to target critical infrastructure in the United States is a wave of ransomware attacks that have targeted the health care industry. Since the start of the pandemic, a Russian cybercrime group known as FIN12 has carried out ransomware attacks on hospitals and health care infrastructure, as well as schools, in the United States.[406] In October 2020, the group launched a coordinated attack targeting six hospitals across the country using the Ryuk ransomware, which encrypted data on the hospitals' computer systems until a ransom was paid. This led to disruptions in patient care, as well as the cancellation of some noncritical surgeries, at a time when the health care system was already stressed by the ongoing pandemic.[407]

It is more difficult to assess Russia's future intentions with respect to offensive cyber operations, especially as compared with conventional operations, because Russia's planned cyber

---

[403] Cybersecurity and Infrastructure Security Agency (CISA), U.S. Department of Homeland Security, "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," National Cyber Awareness System Alert, TA18-074A, March 15, 2018. CISA explains,

> Since at least March 2016, Russian government cyber actors . . . targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors. . . . This campaign comprises two distinct categories of victims: staging and intended targets. The initial victims are peripheral organizations such as trusted third-party suppliers with less secure networks . . . . The threat actors used the staging targets' networks as pivot points and malware repositories when targeting their final intended victims.

Russia has "employed a variety of TTPs, including spear-phishing emails . . . , watering-hole domains, credential gathering, open-source and network reconnaissance, host-based exploitation, and targeting industrial control system (ICS) infrastructure."

[404] Andrew E. Kramer, "Companies Linked to Russian Ransomware Hide in Plain Sight," *New York Times*, December 6, 2021; David E. Sanger, Clifford Krauss, and Nicole Perlroth, "Cyberattack Forces a Shutdown of a Top U.S. Pipeline," *New York Times*, last updated May 13, 2021.

[405] Scott Jasper, "Assessing Russia's Role and Responsibility in the Colonial Pipeline Attack," *New Atlanticist*, blog, June 1, 2021.

[406] Maggie Miller, "Russian-Speaking Hacking Group Scaling Up Ransomware Attacks on Hospitals," *The Hill*, October 7, 2021. For additional information on FIN12 and its activities, see Mandiant, *FIN12 Group Profile: FIN12 Prioritizes Speed to Deploy Ransomware Against High-Value Targets*, Milpitas, Calif., 2021.

[407] Ellen Nakashima and Jay Greene, "Hospitals Being Hit in Coordinated, Targeted Ransomware Attack from Russian-Speaking Criminals," *Washington Post*, October 29, 2020.

operations are "shrouded in much secrecy."[408] Even so, Western analysts have characterized Russia as posing a "serious cyber threat to industrial control systems (ICS), pharmaceutical, defense, aviation, and petroleum companies."[409] This characterization fits with past Russian cyber operations in Ukraine, where Russia has "demonstrated both a willingness and an ability to target critical, civilian infrastructure for the purpose of creating a feeling of insecurity among the Ukrainian population not directly related to simultaneous military operations."[410] Beyond Ukraine, Turovsky alleges that Russian state actors have gained access to the "largest industrial enterprises, government and military entities, financial institutions . . . and sports organizations."[411]

Russia's willingness to conduct cyber operations against critical infrastructure targets is reflected in Russian military scholarship. This literature often consists of general observations regarding the increasing prevalence of cyberattacks on critical infrastructure assets rather than offering insight into Russia's relative inclination to conduct offensive and defensive cyber operations on such targets. Russian military experts acknowledge, however, that Russia must be prepared to conduct offensive cyber operations as part of its broader military strategy. One group of Russian experts notes, for example, that attacks on critical infrastructure targets are "becoming a trend in cyberwarfare."[412] They predict that the destruction of critical infrastructure targets, including "factories and plants, transportation systems, [and] energy [sector] facilities," will "remain a major prerequisite of success in combat operations" for a "long time," seemingly implying that Russia must carry out such attacks to remain competitive against its adversaries.[413]

The vulnerability of critical infrastructure targets results from the fact that the most-advanced countries have become "heavily dependent on telecommunication networks for virtually all activities, be they public, private, social, economic, or military."[414] This heavy reliance on information infrastructure provides a vast array of targets for potential hackers. As a result, cyber operations can be used to

> provok[e] technogenic disasters that cause fatalities among civilians and material damage to the economy . . . [including from] potentially hazardous chemical, radiation, hydrotechnical and other facilities whose destruction results in clouds

[408] Morgus et al., 2019, p. 29.

[409] "Breaking the Code on Russian Malware," *Recorded Future*, November 20, 2014.

[410] Jensen, 2021, p. 347.

[411] Turovsky, 2019, p. 206.

[412] R. A. Durnev, K. Iu. Kriukov, F. M. Deduchenko, "Preventing Man-Made Disasters Provoked by the Adversary in the Course of Fighting," *Military Thought*, 2019b, p. 16.

[413] Durnev, Kriukov, and Deduhenko, 2019b, pp. 15–16.

[414] Antonovich, 2011, p. 90.

> of toxic substances, radioactive contamination of the terrain, huge breakthrough waves, and other [injurious factors].[415]

As another group of Russian military experts explains, "vulnerable objects of urban infrastructure" are particularly vulnerable to cyberattacks; although these experts rate transportation networks as perhaps the "most secure part of the urban complex," they note that "there, too . . . cyber and information attacks" are possible.[416] As a result, in future military operations, it will become more commonplace for "cybernetic influence" to be used to achieve "critical disruptions of production processes," leading to "secondary damaging factors" that will cause "losses of [military] personnel and the [civilian] population."[417] Hackers can effectively cause "disasters and accidents on gas pipelines, power generation systems, heat supply, water supply and sewage systems" while creating uncertainty as to whether these effects resulted from normal accidents, preexisting internal vulnerabilities in the system, or the malfeasance of external cyber actors.[418] The "social tension and chaos" resulting from such an attack could cause "extremely negative political consequences."[419]

Russian military scholarship emphasizes the cost-effectiveness of carrying out cyberattacks on critical infrastructure targets. Compared with conventional operations, "attack[s] on the information systems of a competitor (adversary)" are very "effective in terms of the ratio of costs and huge damage that can be inflicted at any level (state, military, transport management, telecommunications or production)."[420] This view appears throughout the literature, with one expert noting that cyber weapons can be used to "paralyze [critical systems] up to the total economic degradation of a state."[421]

Conclusion

The fall of the Soviet Union and the resulting economic turmoil coincided with a period during which ordinary people had increasing access to computers. These factors facilitated the development of a robust community of hackers in Russia. Early on, the Russian defense establishment recognized the utility of cyberattacks as a means of achieving military effects at a relatively low cost. Beginning in the late 1990s, Russian hackers conducted a series of

---

[415] Durnev, Kriukov, and Deduhenko, 2019b, p. 17.

[416] N. A. Makhutov, V. L. Balanovsky, V. M. Odyakonov, "The Safety of High-Risk Critically and Strategically Important Objects of Urban Infrastructure Under the Conditions of the Emergence of New Types of Threats," *Bulletin of the Academy of Military Sciences*, No. 1, 2020, p. 32.

[417] Durnev and Sviridok, 2021, p. 18.

[418] Makhutov, Balanovsky, and Odyakonov, 2020, p. 32.

[419] S. K. Kuznetsov, S. V. Lebed, and I. A. Sheremet, "Countering Threats to the Cybersecurity of the Banking and Financial Spheres of the Russian Federation," *Bulletin of the Academy of Military Sciences*, 2017, p. 41.

[420] Antonovich, 2011, p. 91.

[421] Starodubtsev et al., 2020, p. 83.

cyberattacks on targets in the United States, Estonia, Georgia, and Ukraine. These attacks have been carried out by both state actors—specifically, hackers working for the Russian security services—and nonstate actors, including commercial entities, cybercrime organizations, and individual patriotic hackers. The exact nature of ties between the Russian security services and these nonstate hackers remains unclear, but the fact that patriotic hackers typically conduct attacks that further Russian interests suggests that there is some degree of coordination. What is clear is that Russian military strategists view cyber operations as a particularly useful tool for achieving effects against adversary critical infrastructure targets.

While there are clear indications—related to both Russian activities in cyberspace and Russian military scholarship and statements on the subject—that Russia conceives of cyber operations as an integral part of future war, several factors might limit Russia's ability to fully realize this vision. These limiting factors relate to the nature of Russia's available cyber labor force and the potential negative effects of competition between powerful state actors in the cyber realm.

First, although Russia has historically benefited from a labor force with substantial technological skills, it has struggled to retain a dedicated cyber labor force. Experts have noted the "persistent emigration of technological expertise from Russia," which has had negative implications for the available cyber workforce.[422] As discussed earlier in this chapter, Russia has tried to compensate for this labor shortage by harnessing the talents and enthusiasm of patriotic hackers willing to conduct cyber operations on Moscow's behalf, while also taking steps to develop in-house cyber capabilities.[423] This reliance on patriotic hackers and other nonstate actors to conduct cyber operations might ultimately limit Russia's ability to use cyber capabilities to achieve its desired effects at the desired time. The interests of nonstate hackers might frequently align with Russian state interests, but this might not always be the case in the future. While further research is needed to understand Russian C2 over nonstate hackers, these hackers likely have varying levels of reliability, meaning that reliance on their support might come at the cost of consistency and predictability in the quality, riskiness, and outcomes of specific cyber operations.

---

[422] Joe Cheravitch and Bilyana Lilly, "Russia's Cyber Limitations in Personnel and Innovation, Their Potential Impact on Future Operations, and How NATO and Its Members Can Respond," in A. Ertan, K. Floyd, P. Pernik, and T. Stevens, eds., *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2020, pp. 32–33. The report notes that "Moscow has faced a plethora of challenges in building the kind of offensive and defensive cyber capability deemed necessary" to counter the cyber activities of NATO member states (p. 32).

[423] Cheravitch and Lilly, 2020, p. 38. As Turovsky notes, however, Russia has faced an uphill battle in ensuring that cyber concepts and operations are sufficiently understood throughout relevant state entities, and particularly within police and investigative agencies, as well as the judiciary (Turovsky, 2019, pp. 102–103, 126–127). For additional discussion of Russia's cyber labor force, see Andrew S. Bowen, *Russian Cyber Units*, Washington, D.C.: Congressional Research Service, January 4, 2021.

Second, as noted earlier in this chapter, competition between state agencies likely limits Russia's ability to effectively coordinate ongoing and planned cyber operations. By "blurring the boundaries [of] the job portfolios" of the security services in the cyber realm, Russia has fostered an "internal competition between the organizations."[424] One the one hand, this competition "increases [the] drive and innovation" of the security services.[425] Interservice competition "means that [state] agencies are often aggressive, imaginative, and entrepreneurial," which might produce more-innovative cyber campaigns and drive creative solutions to technical problems.[426] On the other hand, this interservice competition decreases synergy between parallel efforts.[427] Although GRU and FSB cyber operators have carved out their own cyber niches, there is likely significant duplication of effort through parallel structures in the two agencies.[428] Russian state agencies "refrain from sharing their code with other actors" and have separately "maintained [teams] of malware developers working for years on 'parallel or similar' toolkits."[429] Interservice competition also might drive the security services to take greater risks in an attempt to prove their utility and relative importance to broader strategic efforts.[430]

[424] Jensen, 2021, p. 341.

[425] Jensen, 2021, p. 341.

[426] Mark Galeotti, *Putin's Hydra: Inside Russia's Intelligence Services*, London: European Council on Foreign Relations, May 2016, p. 4.

[427] Jensen, 2021, p. 341. As analysts have noted, "Bureaucratic competition has long stifled Moscow's efforts to develop cyber capabilities" (Cheravitch and Lilly, 2020, p. 43).

[428] Akimenko and Giles, 2020, pp. 69–70.

[429] Cheravitch and Lilly, 2020, p. 44.

[430] Jensen, 2021, p. 341.

7. Conclusion

To understand the key factors influencing Russian operational concept development, we have explored the evolution of Russian operational concept development from the mid-1970s to the present and Russian capability development to execute key regional tasks in a future unified strategic operation in the European theater.

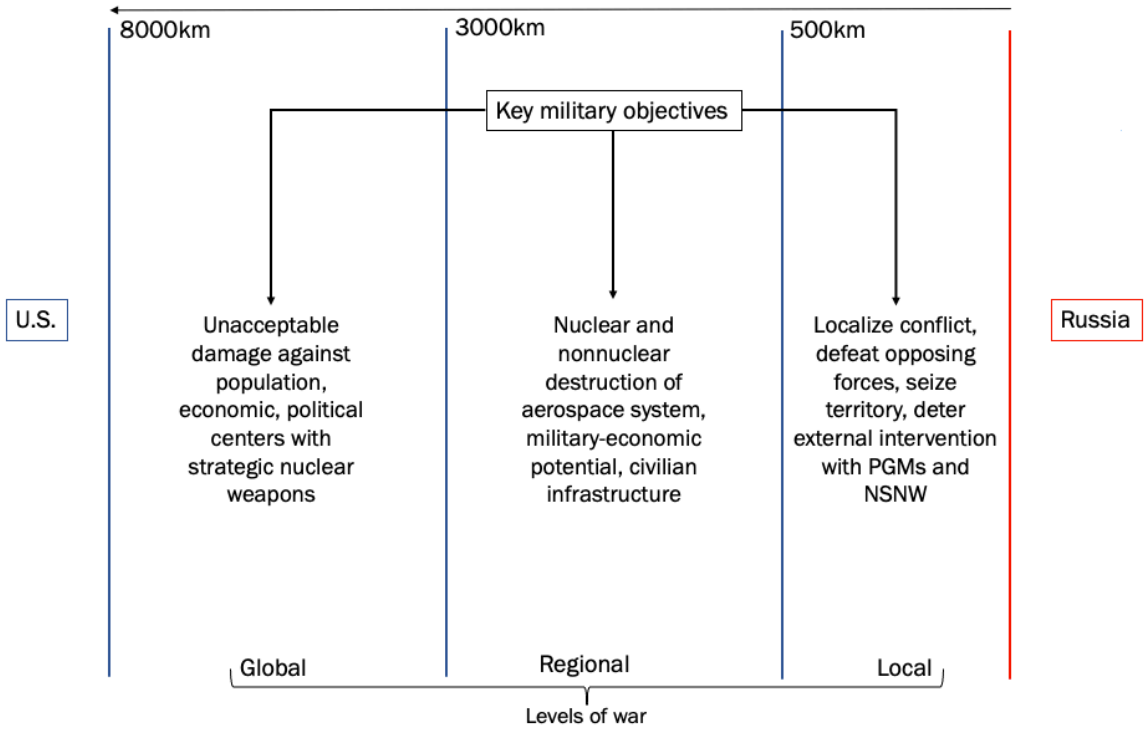
Overcoming the Geographic Separation of Main Forces

Chapter 2 of this report explained that, during the era of strategic nuclear parity in the latter part of the Cold War, the Soviets tested a theater strategic operation that called for echeloned heavy ground formations to conduct conventional deep operations "to the beaches of Western Europe."[431] The purpose was to preempt the ability of NATO to bring its airpower and theater nuclear weapons to bear. The key enablers of this approach were the Soviet Union's possession of a significant portion of European territory and superior numbers of ground forces that could rapidly move into Western Europe and disable critical military targets.

In the post–Cold War period, the enlargement of NATO at the expense of the Soviet Union and the large reduction in land forces have played a critical role in Russian operational concept development. These factors place the military burden on Russia's long-range strike capacity (greater than 500 km) to overcome the geographic separation of main forces (see Figure 7.1). The Russian solution to engage NATO at the regional level of war is to develop a suite of long-range, kinetic, and nonkinetic attack assets to undermine the functionality of NATO's system of warfare, military-industrial potential, and critical civilian infrastructure. Russian operational concept development is driven by how to coordinate, allocate, and employ these forces in a conventional fight that could escalate to nuclear use.

[431] Hines, Mishulovich, and Shull, 1995, p. 7. Quote is as recorded by Hines from an interview with General-Lieutenant Gelii Batenin.

Figure 7.1. Russian Operational Objectives at Various Levels of War



NOTE: *Local war* is defined by Russia as a war with one other country along Russia's periphery (President of Russia, 2014), and 500 km approximately captures the distance from points along Russia's western border to the Baltic countries, Kaliningrad, western Belarus, western Ukraine, and Kyiv. If Russian forces (strike assets) move into Belarus prior to hostilities, this moves the western edge of local war to western Poland.

The unified strategic operation is the proposed solution to the coordination of forces to engage targets at the regional level and degrade NATO's ability to launch an aerospace attack deep into Russia. This operation would merge the GPFO and the SDFO.[432] The GPFO is intended to isolate a conflict at the local level with exclusively conventional weapons, deterring external intervention through the threat of long-range precision strike and nonstrategic nuclear weapons against military targets and civilian infrastructure. Russian formations equipped with missiles with ranges of more than 500 km are part of Russia's SDF. The SDFO, therefore, is tailored to inflict increasing levels of nuclear and conventional damage against critical military and civilian NATO targets in a regional or large-scale war.

As late as 2021, Russian officers questioned Russia's ability to sustain a regional war with NATO at the conventional level, suggesting that the SDFO was oriented primarily toward nuclear missions. Conventional precision weapons and electronic attack continue to be seen by Russian strategists as auxiliary tools in a regional war; if Russian experts believed that these

[432] The Russians might not formally embrace this concept or the nomenclature. More important are the factors driving Russia's operational evolution, the objectives and tasks that Russia believes it needs to accomplish in a regional or large-scale war, and the challenges of coordinating the actions of a joint force in a high-intensity conflict.

conventional weapons could generate sufficient effects, they likely would not describe nonnuclear strategic weapons as the primary means of deterrence at the regional level. As Russian conventional capacity grows over the next two decades, nuclear targeting at the regional (and local) level will be replaced by precision conventional strikes. The unified strategic operation is the concept to prepare for that eventuality.

Russia's Challenges in Engaging Targets Throughout the Depth of NATO with Nonnuclear Weapons

In Chapters 3–6 of this report, we examined ends, ways, and means of Russia's current force structure to execute the primary offensive tasks that Russia wants to accomplish in a future unified operation at the regional level.

Chapter 3 presented the details of the conventional theater strike tasks listed above. Our preliminary analysis aligned with the rhetoric of senior Russian officers and analysts cited in Chapter 2. Our examination of Russian conventional theater strike capacity suggested that Russia's ability to achieve its desired effect of long-range conventional strike over a sustained period could be limited by its platforms and munitions. The platform ceiling is arguably a bigger issue for Russia than munitions, but there is more work to be done to estimate Russian munitions stockpiles and to understand the effects that Russia could generate against assumed target sets.

Chapter 4 of this report noted that Russian EW systems might present challenges for NATO communications across domains, particularly as NATO forces near the Russian border. (The use of Belarusian territory is an important question in this and other domains.) However, electronic protection and other countermeasures, such as the use of terrain, suggest that the problem is not insurmountable. NATO communications are likely to be denied only if they are within direct-line-of-sight distance of the jammer or closer. Similar trends are apparent for other signals (e.g., radar, GPS) and are largely confined to the Baltics and northern Poland.

In Chapter 5, we observed that although Russia is building out several systems that could threaten NATO's space-based assets, the proliferation and use of commercial technology by Russia's adversaries could dilute Russia's capacity in this area. One solution, proposed by the head of the General Staff Academy, could be to target ground-based terminals that facilitate the functioning of space-based communications.

As discussed in Chapter 6, Russian cyber capacity remains an open question. Real-world evidence suggests that there is a considerable threat to civilian infrastructure in both Europe and the United States in the event of a crisis or conflict. The lasting effects of such attacks on a military campaign or society and how to think about offensive capacity in the cyber domain are important areas for future study.

Overall, we did not find evidence that Russian military officers and analysts believe that augmenting capabilities in EW, space, and cyber could fully compensate for a lack of conventional theater strike capacity.

Implications and Application of This Report

Russia is in the relatively early stages of exploiting the so-called revolution in military affairs identified by Soviet officers in the 1970s. Its lack of conventional long-range munitions and platforms, combined with NATO's strategic depth, imposes a continued reliance on nonstrategic nuclear weapons for regional deterrence and warfighting. The more conventional-laden unified strategic operation might be a decade or more away, according to authoritative Russian sources, examination of recent NATO conflicts, and the research in Chapter 3 of this report.

This cuts several ways. Were a large war to break out in Europe between NATO and Russia in the near term, NATO would need to be prepared for the Russian SDFO, which accounts for the allocation and employment of Russia's nuclear and long-range conventional weapons and means of electronic attack to generate highly destructive and cascading effects in targeting. On the other hand, in the near to middle term, Russia is unlikely to embark on a course of action that it does not think it can execute without the use of nuclear weapons against a nuclear peer. Russia may well be deterred from taking preemptive military action against NATO, in part because of a lack of conventional capacity to—over a sustained period—engage targets throughout the European theater and the U.S. homeland. As Russian conventional strike capacity grows into the 2030s, NATO will need to continue to evaluate and consider countermeasures to Russia's ability to engage greater numbers of targets with conventional weapons and electronic attack weapons.[433]

To assist in such an evaluation over time, this report offers an analytic pathway toward defining and measuring what some in the U.S. defense community have referred to as *integrated deterrence*. Drawing on the information in this report, we can identify key capability areas and measure not only the effects that Russia can generate against NATO but also the effects that NATO can generate against Russia in a high-intensity war scenario. With regard to the Russian side of the framework, one possibility would be to use modeling or mathematical methods to estimate effects of the tasks that we have associated with the unified strategic operation; such methods would involve assumptions about Russia's ability to build up and deploy the requisite assets in a crisis and the associated features of C2 of a large, joint force.

Table 7.1 and Figure 7.2 show the indicators of military deterrence and the overall integrated deterrence framework, respectively. These are taken from this report and informed by our research on the Russian military since 2015.[434] (Highlighted in red in the table are the capability areas covered in this report.) RAND researchers have developed approaches to account for EW

[433] One analyst looked to the 2030s and 2040s and considered the implications of an international security environment that is more saturated with conventional long-range destructive capacity (Bruce M. Sugden, "Nuclear Operations and Counter-Homeland Conventional Warfare: Navigating Between Nuclear Restraint and Escalation Risk," *Texas National Security Review*, Vol. 4, No. 4, Fall 2021).

[434] Reach, 2022; Reach, Blanc, and Geist, 2022; Reach et al., 2022; Reach, Kilambi, and Cozad, 2020.

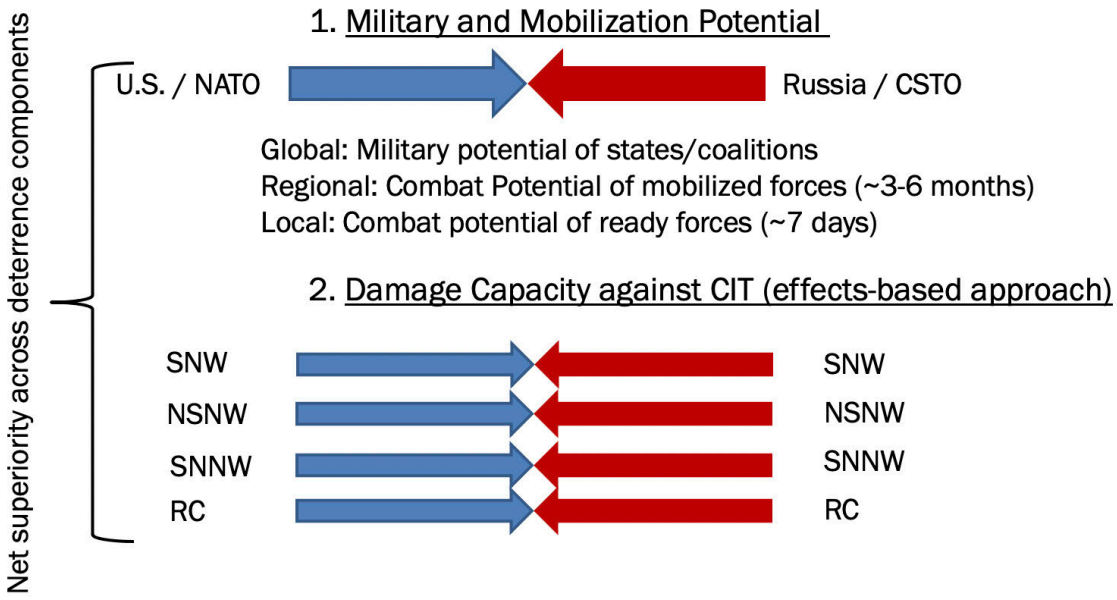
and cyber effects in the context of regional war, the former of which we describe in Chapter 4 of this report.

Table 7.1. Key Indicators and Components of Military Deterrence

Military and Mobilization Potential	Means to Inflict Damage to Critically Important Targets
• Political, economic, scientific-technical indicators • Military alliances	• Strategic nuclear weapons • Nonstrategic nuclear weapons • Strategic nonnuclear weapons – Long-range PGMs – EW – Counterspace weapons – Cyber weapons • Reflexive control to influence leadership and society

SOURCE: Features information from Reach et al., 2022.
NOTE: Red text indicates capability areas covered in this report.

Figure 7.2. Integrated Deterrence Framework



SOURCE: Features information from Reach, Blanc, and Geist, 2022; Reach, Kilambi, and Cozad, 2020; S. R. Tsyrendorzhiev, "O kolichestvennoi otsenke voennoi bezopasnosti," *Voennaia mysl'*, No. 10, 2014.
NOTE: CSTO = Collective Security Treaty Organization; RC = reflexive control; SNNW = strategic nonnuclear weapons; SNW = strategic nuclear weapons.

Abbreviations

ABM	antiballistic missile
ALBM	air-launched ballistic missile
ALCM	air-launched cruise missile
ASAT	anti-satellite
ASCM	anti-ship cruise missile
AWACS	airborne warning and control system
C2	command and control
C4ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CALCM	conventional air-launched cruise missile
CDCM	coastal defense cruise missile
CIS	Center for Information Security
CSG	carrier strike group
DDoS	distributed denial-of-service
EP	electronic protection
EW	electronic warfare
FAPSI	Federal Agency for Government Communications and Information
FM	frequency modulated
FOI	Swedish Defence Research Agency
FSB	Federal Security Service
GLCM	ground-launched cruise missile
GPFO	general-purpose forces operation
GRU	Main Intelligence Directorate
HF	high frequency
HFGCS	High Frequency Global Communications System
ICBM	intercontinental ballistic missile
IOC	initial operational capability
ISR	intelligence, surveillance, and reconnaissance
JASSM-ER	Joint Air-to-Surface Standoff Missile–Extended Range
JDAM	Joint Direct Attack Munition
JSC	joint strategic command
LACM	land-attack cruise missile
LRA	Long-Range Aviation
NATO	North Atlantic Treaty Organization
NSNW	nonstrategic nuclear weapons

OSK	Joint Strategic Command
PGM	precision-guided munitions
RF	Russian Federation
RPO	rendezvous and proximity operations
SAM	surface-to-air missile
SATCOM	satellite communications
SDF	strategic deterrence forces
SDFO	strategic deterrence forces operation
SLBM	submarine-launched ballistic missile
SLCM	submarine-launched cruise missile
SODCIT	strategic operation to destroy critically important targets
SONF	strategic operation of nuclear forces
SRBM	short-range ballistic missile
SRF	Strategic Rocket Forces
TEL	transporter, erector, launcher
TLAM	Tomahawk Land Attack Missile
TLAM-C	Tomahawk Land Attack Missile–Conventional
UAS	unmanned aerial systems
VHF	very high frequency
VKS	Aerospace Forces

References

To support conventions for alphabetizing, bibliographic details in Russian are introduced with and organized according to their transliteration into the Latin alphabet.

Akimenko, Valeriy, *Russia and Strategic Non-Nuclear Deterrence: Capabilities, Limitations and Challenges*, London: Chatham House, July 2021.

Akimenko, Valeriy, and Keir Giles, "Russia's Cyber and Information Warfare," *Asia Policy*, Vol. 15, No. 2, April 2020, pp. 67–75.

America's Navy, "Carrier Strike Group (COMCARSTRKGRU) 9: About Us," webpage, undated. As of January 20, 2022: https://www.surfpac.navy.mil/Ships/Carrier-Strike-Group-COMCARSTRKGRU-9/About-Us/

Antonovich, P. I., "On the Modern Understanding of the Term 'Cyberwar,'" *Bulletin of the Academy of Military Sciences*, No. 2, 2011.

Arbatov, Alexey, "Arms Control in Outer Space: The Russian Angle, and a Possible Way Forward," *Bulletin of the Atomic Scientists*, Vol. 75, No. 4, 2019, pp. 151–161.

———, ed., *Kontrol' nad vooruzheniiami v novykh voenno-politicheskikh i tekhnologicheskikh usloviiakh*, Moscow: IMEMO RAN, 2020a.

———, "Nauchno-tekhnologicheskaia proektsia kosmicheskoi deiatel'nosti," in *Kontrol' nad vooruzheniiami v novykh voenno-politicheskikh i tekhnologicheskikh usloviiakh*, Moscow IMEMO RAN, 2020b.

Arbatov, Alexey, Vladimir Dvorkin, and Petr Topychkanov, "Entanglement as a New Security Threat: A Russian Perspective," in James M. Acton, ed., *Entanglement: Russian and Chinese Perspectives on Non-Nuclear Weapons and Nuclear Risks*, Washington, D.C.: Carnegie Endowment for International Peace, 2017, pp. 11–46.

"Army; Gerasimov Urges Active Introduction of New Methods to Counter Potential Enemy Military Action in Space," *Interfax: Russia & CIS Military Information Weekly*, March 7, 2019.

Ashby, Mark, Caolionn O'Connell, Edward Geist, Jair Aguirre, Christian Curriden, and Jonathan Fujiwara, *Defense Acquisition in Russia and China*, Santa Monica, Calif.: RAND Corporation, RR-A113-1, 2021. As of July 14, 2021: https://www.rand.org/pubs/research_reports/RRA113-1.html

Atherton, Kelsey D., "Russian Drones Can Jam Cellphones 60 Miles Away," C4ISRNET, November 16, 2018.

"Aviation: MiG, Russian Defense Ministry Sign Contract for Modernization of MiG-31K Carriers of Kinzhal Hypersonic Missiles," *Interfax: Russia & CIS Defense Industry Weekly*, August 27, 2021.

"Aviation: Su-57 Aircraft May Be Designated Carrier of Kinzhal Missiles in Future - Aerospace Forces," *Interfax: Russia & CIS Defense Industry Weekly*, December 27, 2019.

Baluevskii, Iu. N., *General'nyi shtab Rossoiskoi armii: istoriya i sovremennost'*, Akademicheskii Proekt, 2006.

Bērziņš, Jānis, "The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria," *Journal of Slavic Military Studies*, Vol. 33, No. 3, 2020, pp. 355–380.

Boltenkov, Dmitriy, "Zakryt' volnu: kak sredstva radioelektronnoy bor'by izmenyat silu flota," *Izvestiia*, November 22, 2020.

Bondarenko, A. P., N. I. Turko, and S. I. Fedorchenko, "Evolutsiia form strategicheskikh deistvii v bor'be s vozdushno-kosmicheskim protivnikom," *Voennaia mysl'*, 1994.

Borisko, S. N., and S. A. Goremykin, "Analiz sostoianiia Vozdushno-kosmicheskikh sil Rossii. Perspektivy razvitiia," *Voennaia mysl'*, January 1, 2019, pp. 25–37.

Borzov, Arkadii, "Vchera – Iugoslaviia. A kto zavtra?" *Vozdushno-kosmicheskaia sfera*, No. 3, 2008.

Boulègue, Mathieu, *Russia's Military Posture in the Arctic: Managing Hard Power in a 'Low Tension' Environment*, London: Chatham House, June 2019.

Bowen, Andrew S., *Russian Cyber Units*, Washington, D.C.: Congressional Research Service, January 4, 2021.

Bowman, Steve, *Kosovo and Macedonia: U.S. and Allied Military Operations*, Washington, D.C.: Congressional Research Service, IB10027, November 13, 2001.

"Breaking the Code on Russian Malware," Recorded Future, November 20, 2014. As of January 4, 2022:
https://www.recordedfuture.com/russian-malware-analysis/

Bronk, Justin, *Russian and Chinese Combat Air Trends: Current Capabilities and Future Outlook*, London: Royal United Services Institute for Defence and Security Studies, Whitehall Report 3-20, October 2020.

Burenok, V. M., "Razvitie sistemy vooruzheniia i novyi oblik vooruzhennykh sil RF," *Zaschita i bezopasnost'*, No. 2, 2009.

Burenok, V. M., and O. B. Achasov, "Neiardnoe sderzhivanie," *Voennia Mysl'*, Vol. 17, No. 1, 2008.

Burenok, V. M., R. A. Durnev, and K. Iu. Kriukov, "Sukhoputnye voiny budushchego: opyt futurologicheskogo analiza," *Innovatika i ekspertiza*, Vol. 2, No. 27, 2019.

Burenok, V. M., and Iu. A. Pechatnov, *Strategicheskoe sderzhivanie*, pre-publication copy, 2011.

Burutin, A. G., G. N. Vinokurov, V. M. Loborev, S. F. Pertsev, and Iu. A. Podkorytov, "Kotseptsiia nepriemlemogo ushcherba: genesis, osnovnye prichiny transformatsii, sovremennoe sostoianie," *Vooruzhenie. Politika. Konversiia*, No. 4, 2010.

Buval'tsev, I. A., O. A. Abdrashitov, and A. V. Garvard, "Razvitie taktiki v sovremennykh usloviiakh," *Voennaia mysl'*, No. 10, 2021.

Center for Strategic and International Studies Missile Defense Project, "S-500 Prometheus," *Missile Threat*, last updated July 1, 2021a. As of January 4, 2022: https://missilethreat.csis.org/defsys/s-500-prometheus/

———, "9K720 Iskander (SS-26)," *Missile Threat*, last updated August 2, 2021b. As of December 1, 2021: https://missilethreat.csis.org/missile/ss-26-2/

Charap, Samuel, Alice Lynch, John J. Drennan, Dara Massicot, and Giacomo Persi Paoli, *A New Approach to Conventional Arms Control in Europe: Addressing the Security Challenges of the 21st Century*, Santa Monica, Calif.: RAND Corporation, RR-4346, 2020. As of January 4, 2022: https://www.rand.org/pubs/research_reports/RR4346.html

Charap, Samuel, Dara Massicot, Miranda Priebe, Alyssa Demus, Clint Reach, Mark Stalczynski, Eugeniu Han, and Lynn E. Davis, *Russian Grand Strategy: Rhetoric and Reality*, Santa Monica, Calif.: RAND Corporation, RR-4238-A, 2021. As of January 4, 2022: https://www.rand.org/pubs/research_reports/RR4238.html

Chekinov, S. G., and S. A. Bogdanov, "Evoliutsia sushchnosti i soderzhania poniatia voina v XXI stoletitti," *Voennaia mysl*, No. 1, 2017.

Chekinov, S. G., V. I. Makarov, and V. V. Kochergin, "Zavoevaniiu i uderzhaniiu gospodstva v vozdukhe (v vozdushno-kosmicheskoi sfere) - dostoinoe mesto v razvitii rossiiskoi voennoi teorii i podgotovke voisk (sil)," *Voennaia mysl'*, No. 2, February 2017, pp. 58–66.

Cheravitch, Joe, and Bilyana Lilly, "Russia's Cyber Limitations in Personnel and Innovation, Their Potential Impact on Future Operations, and How NATO and Its Members Can Respond," in A. Ertan, K. Floyd, P. Pernik, and T. Stevens, eds., *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2020, pp. 31–59.

Chilton, Kevin P., and Lukas Autenried, *The Backbone of JADC2: Satellite Communications for Information Age Warfare*, Arlington, Va.: Michell Institute for Aerospace Studies, Mitchell Institute Policy Paper, Vol. 32, December 2021.

Congressional Research Service, *The New START Treaty: Central Limits and Key Provisions*, Version 82, Washington, D.C., R41219, updated February 2, 2022.

Connable, Ben, Abby Doll, Alyssa Demus, Dara Massicot, Clint Reach, Anthony Atler, William Mackenzie, Matthew Povlock, and Lauren Skrabala, *Russia's Limit of Advance: Analysis of Russian Ground Force Deployment Capabilities and Limitations*, Santa Monica, Calif.: RAND Corporation, RR-2563-A, 2020. As of May 2, 2022: https://www.rand.org/pubs/research_reports/RR2563.html

Connect, "Starlink vziala rubezh v 1000 sputnikov obzor zarubezhnoi pressy po tematike sputnikovoi sviazi za fevral' 2021 goda," January 3, 2021.

Connell, Michael, and Sarah Vogler, *Russia's Approach to Cyber Warfare*, Arlington, Va.: CNA, March 2017.

"Corridors of Power; Creation of Russia's State-of-the-Art Weapons Peresvet, Avangard, Kinzhal on Track - Deputy PM Borisov," *Interfax: Russia & CIS Military Information Weekly*, October 2, 2020.

"Corridors of Power; Hypersonic System Kinzhal Is Capable of Hitting Both Ground and Sea Targets - Russian Defense Ministry," *Interfax: Russia & CIS Defense Industry Weekly*, February 22, 2019.

Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," National Cyber Awareness System Alert TA18-074A, March 15, 2018. As of January 4, 2022: https://www.cisa.gov/uscert/ncas/alerts/TA18-074A

Danilevich, A. A., and O. P. Shunin, "O neiadernykh silakh sderzhivaniia," *Voennaia mysl*, No. 1, 1992.

Davis, Joshua, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007.

"Defense Industry; New Hypersonic Missile, Lichinka-MD, Being Developed for Su-57 Fighter Jet – Media," *Interfax: Russia & CIS Military Daily*, October 7, 2021.

"Defense Industry; Russia Developing New Hypersonic Vehicles in Furtherance of Avangard, Tsirkon Systems – NPO Mashinostroyenia General Director," *Interfax: Russia & CIS Military Information Weekly*, April 2, 2021.

Delanoe, Igor, *Russia's Black Sea Fleet: Toward a Multiregional Force*, Arlington, Va.: CNA, June 2019.

Denning, Dorothy, "Tracing the Sources of Today's Russian Cyberthreat," *Scientific American*, August 18, 2017.

Durnev, R. A., K. Iu. Kriukov, and F. M. Deduchenko, "Preduprezhdenie tekhnogennykh katostrof, provotsiruemykh protivnikom v khode voennykh deistvii," *Voennaia mysl'*, No. 10, 2019a.

———, "Preventing Man-Made Disasters Provoked by the Adversary in the Course of Fighting," *Military Thought*, 2019b.

Durnev, R. A., and E. V. Sviridok, "Sistema strategicheskogo neiadernogo sderzhivaniia: ekspertnyi podkhod k obosnovaniiu," *Vooruzhenie i ekonomika*, Vol. 3, No. 57, 2021.

Fabrizio, Giuseppe Aureliano, *High Frequency Over-the-Horizon Radar: Fundamental Principles, Signal Processing, and Practical Applications*, McGraw-Hill Education, 2013.

Falichev, Oleg, "Goryachiye tochki nauki: Genshtab oboznachil bazy operatsiy i rubezhi dlya uchenykh," *Voenno-promyshlennyy kuryer (VPK)*, March 27, 2018.

Federov, Konstantin, "Minoborony sozdast sovremennuiu orbital'nuiu gruppirovku voennykh sputnikov—Shoigu," *TVZvezda*, March 6, 2018.

Fedotov, I. A., "Napravleniia razvitiia operativno-strategicheskogo komandovaniia voennogo okruga na sovremennom etape stroitel'stva Vooruzhennykh Sil Rossiiskoi Federatsii," *Vestnik Akademii voennykh nauk*, Vol. 4, No. 57, 2016, pp. 65–69.

Fesenko, Y. N., "Ob osobennostyakh ognevogo porozheniya gruppirovok voisk," *Voennaya mysl*, No. 5, 2000.

Fink, Anya Loukianova, and Olga Oliker, "Russia's Nuclear Weapons in a Multipolar World: Guarantors of Sovereignty, Great Power Status & More," *Daedalus*, Vol. 149, No. 2, Spring 2020, pp. 37–55.

"First Batch of Russian-Made S-500 System Enters Service – Deputy PM," TASS, September 16, 2021.

"First S-550 Air Defense Systems Enter Service in Russia – Source," TASS, December 28, 2021.

Galeotti, Mark, *Putin's Hydra: Inside Russia's Intelligence Services*, London: European Council on Foreign Relations, May 2016.

Gareev, Makhmut, "Problemy sovremennoi sistemy voennogo upravleniia i puti ee sovershenstvovaniia s uchetom novykh oboronnykh zadach i izmenenii kharaktera budushchikh voin," *Voennaia mysl'*, No. 5, 2004.

———, “Ob organizatsii voennogo upravleniia na strategicheskikh napravleniiakh,” *Natsional’naia oborona*, No. 10, 2010.

Geist, Edward, and Dara Massicot, “Understanding Putin’s Nuclear Superweapons,” *SAIS Review of International Affairs*, Vol. 39, No. 2, Summer–Fall 2019, pp. 103–117.

“Genschtab: Osobennostiu konflictkov budushevo stanet primeneniye robotov i kosmicheskix sredstv,” TASS, March 24, 2018.

Gerasimov, Valerii V., “Osnovnye tendentsii razvitiia form i sposobov primeneniia Vooruzhennykh sil, aktual’nye zadachi voennoi nauki po ikh sovershenіiu,” *Vestnik Akademii voennykh nauk*, Vol. 1, No. 42, 2013.

———, “Rol’ general’nogo shtaba v organizatsii oborony strany v sootvetstvii s novym polozheniem o general’nom shtabe, utverzhdennym prezidentom rossiiskoi federatsii,” *Vestnik Akademii voennykh nauk*, Vol. 46, No. 1, 2014.

———, “O khode vypolneniia ukazov prezidenta Rossiiskoi Federatsii ot 7 maia 2012 goda N603, 604 i razvitie vooruzhennykh sil Rossiiskoi Federatsii,” *Voennaia mysl’*, No. 12, 2017a.

———, “Sovremennye voiny i aktual’nye voprosy oborony strany,” *Vestnik Akademii voennykh nauk*, Vol. 2, No. 59, 2017b.

———, “Vliianie sovremennogo kharaktera vooruzhennoi bor’by na napravlennost’ stroitel’stva i razvitiia vooruzhennykh sil Rossiiskoi Federatsii. Prioritetnye zadachi voennoi nauki v obespecheniia oborony strany,” *Vestnik Akademii voennykh nauk*, Vol. 2, No. 63, 2018.

———, “Vektory v razvitii voennoi strategii,” *Krasnaia zvezda*, March 4, 2019.

Gerasimov, V. V., S. F. Rudskoi, V. V. Trushin, and S. P. Belokon’, *Osnovy pobedy v boiu*, General’nyi shtab Vooruzhennykh sil Rossiiskoi Federatsii, 2018.

Glantz, David M., *Soviet Military Operational Art: In Pursuit of Deep Battle*, Abingdon, United Kingdom: Frank Cass, 1991.

———, *The Military Strategy of the Soviet Union: A History*, Abingdon, United Kingdom: Frank Cass, 1992.

———, “Inheriting Ogarkov: Soviet and Russian Views of the Changing Nature of War,” remarks translated into Russian by Centre for Analysis of Strategies and Technologies, March 13, 2015.

Grego, Laura, *A History of Anti-Satellite Programs*, Cambridge, Mass.: Union of Concerned Scientists, January 2012.

Grisé, Michelle, Alyssa Demus, Yuliya Shokh, Marta Kepe, Jonathan W. Welburn, and Khrystyna Holynska, *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation*, Santa Monica, Calif.: RAND Corporation, RR-A198-8, 2022. As of December 9, 2022: https://www.rand.org/pubs/research_reports/RRA198-8.html

Groznyi, Oleg, "Fundament oboronosposobnosti otechestva nadezhen," *Krasnaya Zvezda*, December 28, 2019.

Hakala, Janne, and Jazlyn Melnychuk, *Russia's Strategy in Cyberspace*, Riga: NATO Strategic Communications Centre of Excellence, June 2021.

Hendrickx, Bart, "Burevestnik: A Russian Air-Launched Anti-Satellite System," *Space Review*, April 27, 2020a.

———, "Peresvet: A Russian Mobile Laser System to Dazzle Enemy Satellites," *Space Review*, June 15, 2020b.

———, "Russia Gears Up for Electronic Warfare in Space (Part 1)," *Space Review*, October 26, 2020c.

———, "EKS: Russia's Space-Based Missile Early Warning System," *Space Review*, February 8, 2021.

Hines, John, Ellis M. Mishulovich, and John F. Shull, *Soviet Intentions 1965–1985:* Vol. II, *Soviet Post-Cold War Testimonial Evidence*, McLean, Va.: BDM Federal, Inc., September 22, 1995.

Hoehn, John R., *Precision-Guided Munitions: Background and Issues for Congress*, Washington, D.C.: Congressional Research Service, R45996, updated June 11, 2021.

International Institute for Strategic Studies, *The Military Balance 2021*, London, 2021.

Ishchenko, Sergey, "Slishkom krypnyi 'Kalibr,'" *Armeiskii vestnik*, September 8, 2016.

"Istochnik: pervaia brigada S-500 zashchitit nebo Moskvy i Tsentral'nogo promyshlennogo raiona RF," TASS, October 12, 2021.

Ivanov, Pavel, "Borodatye 'Tomagavki,'" *Voenno-promyshlennyi kur'er (VPK)*, No. 14, April 12, 2017. As of January 4, 2022: https://dlib.eastview.com/browse/doc/48605323

Ivanov, V. G., A. Iu. Savitskii, and S. G. Makarov, "Vliianie voin i vooruzhennykh konfliktov na sistemu sviazi voennogo naznacheniia," *Radiolokatsiia, navigatsiia, sviaz': Sbornik trudov XXVI Mezhdunarodnoi nauchno-tekhnicheskoi konferentsii*, Voronezhskii gosudarstvennoi universitet / Sozvezdie Contsern, 2020.

Ivasik, V. A., A. S. Pis'iaukov, and A. L. Khriapin, "Iadernoe oruzhie i voennaia bezopasnost' Rossii," *Voennaia mysl'*, No. 4, 1999.

Janes Defense Weekly, "Russia Cuts State Armament Programme Funding," July 22, 2020.

Jasper, Scott, "Assessing Russia's Role and Responsibility in the Colonial Pipeline Attack," *New Atlanticist*, blog, June 1, 2021. As of January 4, 2022: https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/

Jensen, Mikkel Storm, "Russia and Cyber – Espionage, Sabotage and the Constant Fight for the Truth," in Niels Bo Poulsen and Jørgen Staun, eds., *Russia's Military Might: A Portrait of Its Armed Forces*, Copenhagen: Djøf Publishing, 2021, pp. 327–354.

Johnson, Dave, *Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds*, Livermore, Calif.: Lawrence Livermore National Laboratory, Center for Global Security Research, Livermore Papers on Global Security No. 3, February 2018.

Johnson, David E., *Learning Large Lessons: The Evolving Roles of Ground Power and Air Power in the Post–Cold War Era*, Santa Monica, Calif.: RAND Corporation, MG-405-1-AF, 2007. As of May 2, 2022: https://www.rand.org/pubs/monographs/MG405-1.html

Kari, Martti J., *Russian Strategic Culture in Cyberspace: Theory of Strategic Culture – A Tool to Explain Russia's Cyber Threat Perception and Response to Cyber Threats*, Jyväskylä: University of Jyväskylä, JYU Dissertations 122, 2019.

Khudoleev, Viktor, "Voiska s velikoi istoriei," *Krasnaya Zvezda*, 2015.

Kipp, Jacob W., "The Evolution of Soviet Operational Art: The Significance of 'Strategic Defense' and 'Premeditated Defense' in the Conduct of Theatre-Strategic Operations," *Journal of Soviet Military Studies*, Vol. 4, No. 4, December 1991, pp. 621–648.

Kjellén, Jonas, *The Russian Baltic Fleet: Organisation and Role Within the Armed Forces in 2020*, Stockholm: Swedish Defence Research Agency, FOI-R--5119--SE, February 2021.

Kofman, Michael, Anya Fink, and Jeffrey Edmonds, *Russian Strategy for Escalation Management: Evolution of Key Concepts*, Arlington, Va.: CNA, DRM-2019-U-022455-1Rev, April 2020.

Kofman, Michael, Anya Fink, Dmitry Gorenburg, Mary Chesnut, Jeffrey Edmonds, and Julian Waller, *Russian Military Strategy: Core Tenets and Operational Concepts*, Arlington, Va.: CNA, August 2021.

Kokoshin, A. A., "Strategicheskoe iadernoe i neiadernoe sderzhivanie: prioritety sovremennoi epokhi," *Vestnik Rossiiskoi akademii nauk*, Vol. 84, No. 3, 2014.

———, “Voruzhennaia bor’ba v kosmicheskom prostranstve: novye tekhnologii i ikh vliianie na strategicheskuiu stabil’nost’,” in *Vlianie tekhnologicheskikh faktorov na parametry ugroz natsional’noi i mezhdunarodnoi bezopastnosti, voennykh konfliktov i strategicheskoi stabilnosti*, 2017.

Kokoshin, A. A., Iu. N. Baluevskii, V. I. Esin, and A. V. Shliakhturov, *Voprosy eskalatsii i deescalatsii krizisnykh situatsii, vooruzhennykh konfliktov, i voin*, Moscow: LENAND, 2021.

“Kompleks ‘Rychag-AV’ – pomoshchnik vintokrylykh mashin: ob uvelichenii chisla vertoliotov s sistemami radiopodavleniya,” *Voennoe obozrenie*, November 13, 2020.

“Koncern BKO ‘Almaz-Antey’: vklad v potential strategiskovo neyardnovo sderzhivaniya,” *Natsionalnaya Oborona*, June 4, 2020. As of January 4, 2022: https://2009-2020.oborona.ru/includes/periodics/navy/2020/0604/194029571/detail.shtml

“Koncern VKO ‘Almaz-Antey’: vklad v potentsial strategicheskovo neyardernovo sderzhivaniye,” *Natsonalnaya Oborona*, No. 11, November 2020.

Korol, O. V., and N. L. Romas, “Form of Military Actions: On the Meaning of the Category,” *Military Thought*, East View Information Services, No. 3, 2008, pp. 149–153.

Kramer, Andrew, E., “Companies Linked to Russian Ransomware Hide in Plain Sight,” *New York Times*, December 6, 2021.

Kreidin, S. V., “Global’noe i regional’noe iadernoe sderzhivanie: k sisteme printsipov i kriteriev,” *Voennaia mysl’*, No. 4, 1999.

Kristensen, Hans M., “Russian Nuclear Forces,” in Stockholm International Peace Research Institute, *SIPRI Yearbook 2020*, Oxford University Press, 2020, pp. 336–345.

Kristensen, Hans M., and Matt Korda, “Russian Nuclear Forces, 2019,” *Bulletin of the Atomic Scientists*, Vol. 75, No. 2, 2019, pp. 73–84.

———, “Russian Nuclear Weapons, 2021,” *Bulletin of the Atomic Scientists*, Vol. 77, No. 2, 2021, pp. 90–108.

Kruglov, V. V., and A. S. Shubin, “O vozrastaiushchem znachenii uprezhdeniia protivnika v deistviiakh,” *Voennaia mysl’*, No. 12, 2021.

Kulikov, V. A., “Military-Technical Aspects of War Prevention,” *Military Thought*, East View Information Services, No. 2, 2006.

Kupach, O. S., “Analyzing the U.S. Conventional Prompt Global Strike Program,” *Military Thought*, Vol. 27, No. 4, 2018, pp. 26–31.

Kupriianov, G. P., “Osnovnye tendentsii razvitiia form i sposobov vooruzhennoi bor’by v vozdushno-kosmicheskoi sfere i ikh vliianie na razvitie teorii strategii operativnogo iskusstva VS RF,” *Vestnik Akademii voennykh nauk*, Vol. 2, No. 7, 2004.

Kuralenko, S. V., "Tendencies in the Changing Character of Armed Struggles in Military Conflicts in the First Half of the 21st Century," *Military Thought*, East View Information Services, No. 11, 2012, pp. 40–46.

Kuzmin, V. N., and N. A. Frolov, "Prognoz tendentsii razvitiia soderzhaniia i kharaktera voennykh konfliktov budushchego i otsenka ikh vliianiia na voenno-kosmicheskuiu deiatel'nost' v mire v XXI veke," *Vestnik Akademii voennykh nauk*, Vol. 1, No. 74, 2021.

Kuznetsov, S. K., S. V. Lebed, and I. A. Sheremet, "Countering Threats to the Cybersecurity of the Banking and Financial Spheres of the Russian Federation," *Bulletin of the Academy of Military Sciences*, 2017.

Lavrov, Anton, "Russian UAVs in Syria," Centre for Analysis of Strategies and Technologies, undated.

———, *The Russian Air Campaign in Syria: A Preliminary Analysis*, Arlington, Va.: CNA, COP-2018-U-017903, June 2018.

Leicester, John, Sylvie Corbet, and Aaron Mehta, "'Espionage': French Defense Head Charges Russia of Dangerous Games in Space," *Defense News*, September 7, 2018.

Levshin, V. I., A. V. Nedelin, and M. E. Sosnovskii, "O primenenii iadernogo oruzhiia dlia deeskalatsii voennykh deistvii," *Voennaia mysl'*, No. 3, 1999.

Lilly, Bilyana, and Joe Cheravitch, "The Past, Present, and Future of Russia's Cyber Strategy and Forces," in T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, and G. Visky, eds., *2020 12th International Conference on Cyber Conflict*, Tallinn: IEEE, 2020, pp. 129–155.

Litovkin, Nikolai, "Russia's New Breed of Intermediate Range Missiles," *Russia Beyond*, February 6, 2019.

Litvinenko, V., "Tseli dyla artillerii," *Armeiskii Sbornik*, No. 4, 2019, pp. 17–23.

Lytkin, Vladimir, "Perspektivnyye sistemy REB Rossii: chto prikhodit na smenu 'Krasukhe-4,'" *Voennoe obozrenie*, July 16, 2020.

Makhnin, V. L., "Voina kak sotsial'no-politicheskoe iavlenie: ot bipolarnosti do tranzitarnosti," *Vestnik Akademii voennykh nauk*, Vol. 3, No. 68, 2019.

Makhutov, N. A., V. L. Balanovsky, and V. M. Odyakonov, "The Safety of High-Risk Critically and Strategically Important Objects of Urban Infrastructure Under the Conditions of the Emergence of New Types of Threats," *Bulletin of the Academy of Military Sciences*, No. 1, 2020.

Mandiant, *FIN12 Group Profile: FIN12 Prioritizes Speed to Deploy Ransomware Against High-Value Targets*, Milpitas, Calif., 2021.

Markoff, John, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008.

McDermott, Roger, and Tor Bukkvoll, *Russia in the Precision-Strike Regime – Military Theory, Procurement and Operational Impact*, Kjeller: Norwegian Defence Research Establishment, 17/00979, August 1, 2017.

———, "Tools of Future Wars: Russia Is Entering the Precision-Strike Regime," *Journal of Slavic Military Studies*, Vol. 31, No. 2, 2018, pp. 191–213.

McLaughlin, Daniel, "Ukraine Blames Russian Hackers for Airport Attack," *Irish Times*, January 18, 2016.

Miasnikov, Victor, "Edinaia kosmicheskaia sistema predupredit o iadernom napadenii," *Nezavisimaya gazeta*, October 17, 2014.

Mihayloff, Andrey, "Russia's New Kh-95 Hypersonic Missile Ends the Arms Race with the United States," *Pravda*, November 10, 2021. As of January 4, 2022: https://english.pravda.ru/science/149597-hypersonic_missile/

Mikhailov, Alexiy, and Dmitrii Bal'burov, "Ispytaniia protivosputnikogo kompleksa nachnutsia v kontse goda," *Izvestia*, January 24, 2014.

Mikhailova, Diana, "S shiroko otkrytymi glazami: vozdushnaya radioelektronnaya bor'ba. Chast' 2," *LiveJournal*, January 24, 2018.

Military Russia, "A-60/78T6/1LK222," webpage, August 12, 2016. As of January 20, 2022: http://militaryrussia.ru/blog/index-873.html

———, "Komplek 14Ts033 Nudol' raketa 14A042," webpage, May 4, 2021. As of January 20, 2022:
http://militaryrussia.ru/blog/topic-806.html

Milkavkaz.com, "Vooruzhennye sily Rossii," webpage, undated. Site is no longer accessible. As of May 4, 2021:
www.milkavkaz.com

Miller, Maggie, "Russian-Speaking Hacking Group Scaling Up Ransomware Attacks on Hospitals," *The Hill*, October 7, 2021.

Ministry of Defense of the Russian Federation, "Strategicheskie sily sderzhivaniia," Voenno-entsiklopedicheskii slovar', Ministerstvo oborony RF, undated.

———, "Raketnye korabli Baltijskogo flota unichtozhili uslovnye beregovye i morskie celi krylatymi raketami 'Kalibr,'" December 3, 2021.

Morgus, Robert, Brian Fonseca, Kieran Green, and Alexander Crowther, *Are China and Russia on the Cyber Offensive in Latin America and the Caribbean? A Review of Their Cyber Capabilities and Implications for the U.S. and Its Partners in the Region*, Washington, D.C.: New America, July 2019.

Mueller, Karl P., Gregory Alegi, Christian F. Anrig, Christopher S. Chivvis, Robert Egnell, Christina Goulter, Camille Grand, Deborah C. Kidwell, Richard O. Mayne, Bruce R. Nardulli, Robert C. Owen, Frederic Wehrey, Leila Mahnad, and Stephen M. Worman, *Precision and Purpose: Airpower in the Libyan Civil War*, Santa Monica, Calif.: RAND Corporation, RR-676-AF, 2015. As of January 4, 2021: https://www.rand.org/pubs/research_reports/RR676.html

Nakashima, Ellen, and Jay Greene, "Hospitals Being Hit in Coordinated, Targeted Ransomware Attack from Russian-Speaking Criminals," *Washington Post*, October 29, 2020.

National Air and Space Intelligence Center, *Competing in Space*, Wright-Patterson Air Force Base, Ohio, December 2018.

NATO—*See* North Atlantic Treaty Organization.

nonothai, "Il-22PP Porubschik Electronic Countermeasures Plane," *Thai Military and Asian Region*, blog, last updated August 9, 2018.

North Atlantic Treaty Organization, *The Secretary General's Annual Report*, Brussels, 2020.

Novyy oboronnyy zakaz. Strategii, "Tirada-2S," webpage, September 25, 2019. As of January 20, 2022: https://dfnc.ru/katalog-vooruzhenij/rls-sprn-i-pvo/tirada-2s/

"Number of Long-Range Cruise Missile Carriers in Russia Up 13 Times Since 2012," TASS, December 22, 2020.

Ofitsial'nyy sayt munitsipal'nogo obrazovaniya 'Bol'shesoldatskiy rayon,' "Svedeniia o Voinskoi Chasti 03051," September 4, 2018. As of January 20, 2022: http://bol.rkursk.ru/index.php?sub_menus_id=30791&id_mat=211900

Ogarkov, N. V., *Istoriia uchit bditel'nosti*, Voenizdat, Moscow, 1985.

Ogarkov, N. V., "Doklad nachal'nika Shtaba rukovodstva—nachal'nika General'nogo shtabe Vooruzhennykh Sil SSSR Marshala Sovetskogo Soiuza Ogarkova N.V.," in *Materialy rasbora operativno-strategicheskogo komandno-ucheniia 'Zapad-77'*, Moscow: Ministerstvo oborony SSSR, 1977.

"Ordnance; Hypersonic Kinzhal Can Hit Aircraft Carriers, Other Types of Ships – Deputy Defense Minister," *Interfax: Russia & CIS Defense Industry Weekly*, March 16, 2018.

"Ordnance; Hypersonic Weapons to Make Up Core of Russia's Non-Nuclear Deterrence Capability – Shoigu," *Interfax: Russia & CIS Defense Industry Weekly*, February 12, 2021.

"Ordnance; Iskander-M Adjusted to Hit Marine Targets," *Interfax: Russia & CIS Defense Industry Weekly*, August 3, 2018.

"Ordnance; Nuclear-Powered Cruise Missile Can Stay in Air for Days - Deputy Defense Minister," *Interfax: Russia & CIS Defense Industry Weekly*, 2018.

Orlov, Vitalii, "Voina nevidimaia i effektivnaia: Sovremennye kompleksy REB sposobny neitralizovat' edva li ne liuboe oruzhie protivnika," *Voenno-promyshlennyi kur'er (VPK)*, August 24, 2021.

O'Rourke, Ronald, *Cruise Missile Inventories and NATO Attacks on Yugoslavia: Background Information*, Washington, D.C.: Congressional Research Service, April 20, 1999.

Ostapenko, O. I., S. V. Baushev, and I. V. Morozov, *Informatsionno-kosmicheskoe obespechenie gruppirovok voisk (sil) VS RF*, St. Petersburg, Russia: Liubavich, 2012.

Palitsyn, A. B., and D. B. Zhilenko, "Analiz traditsionnykh i perspektivnykh zadach sistemy vozdushno-kosmicheskoi oborony Rossii: problem i puti ikh resheniia," *Voennaia Mysl'*, No. 9, 2020.

Panda, Ankit, "Report: Russia Developing 4,500 Kilometer Kalibr-M Range Land-Attack Cruise Missile," *The Diplomat*, January 10, 2019.

———, "The Dangerous Fallout of Russia's Anti-Satellite Missile Test," Carnegie Endowment for International Peace, November 17, 2021.

Parsons, Dan, "Air Force Shows Off Stealthy Long-Range JASSM-ER for First Time in Syria Strikes," *Defense Daily*, April 16, 2018.

Peck, Michael, "Russia's II-22PP Is a Satellite Zapping Powerhouse," *National Interest*, August 19, 2021.

Pedyashev, V. N., A. V. Mashkovtsev, and V. V. Artemov, "The Approach to the Selection of Enemy Target Destruction Effectiveness Indicators Using Nuclear Weapons and Strategic Nonnuclear Weapons," speech delivered at the XXXI NTK (Scientific-Technical Conference) of the Serpukhov Affiliate of the Petr Velikiy RVSN Military Academy, Moscow, June 28–29, 2012.

Persson, Gudrun, ed., *Russian Military Capability in a Ten-Year Perspective—2016*, Stockholm: Swedish Defence Research Agency, FOI-R--4326--SE, December 2016.

Podvig, Pavel, "Russian Space Systems and the Risk of Weaponizing Space," in Samuel Bendett, Mathieu Boulègue, Richard Connolly, Margarita Konaev, Pavel Podvig, and Katarzyna Zysk, eds., *Advanced Military Technology in Russia: Capabilities and Implications*, London: Chatham House, September 2021, pp. 34–46.

Poletaev, V. I., and V. V. Alferov, "O neiadernom sderzhivanii, y ego rol' i mesto v visteme stategicheskogo sderzhevaniia," *Voennaia mysl'*, No. 7, July 2015, pp. 3–10.

Ponomarev, S. A., V. V. Poddubnyi, and V. I. Polegaev, "Kriterii i pokazateli neiadernogo sderzhivaniia: voennyi aspekt," *Voennaia mysl'*, No. 11, 2019, pp. 97–98.

"'Porubshchik-2' kak ubiytsa sputnikov," *Voennoe obozrenie*, July 9, 2018.

President of Russia, *Voennaia doktrina Rossiiskoi Federatsii*, December 25, 2014.

———, "Ob osnovakh gosudarstvennoi politiki Rossiiskoi Federatsii v oblasti iadernogo sderzhivaniia," decree, No. 355, June 2, 2020.

Protasov, A. A., S. V. Kreidin, and Iu. A. Kublo, "Aktual'nye aspekty razvitiia silovykh instrumentov i kontseptsii strategicheskogo sderzhivaniia," *Vestnik Akademii voennykh nauk*, Vol. 3, No. 76, 2021.

Protasov, A. A., V. A. Sobolevskii, V. V. Sukhorutchenko, and A. S. Borisenko, "Metodicheskoe obespechenie vyrabotki zamysla primeneniia VTO bol'shoi dal'nosti v operatsiiakh (boevykh deistviiakh)," *Voennaia mysl'*, No. 10, 2011, pp. 36–48.

Ptichkin, Sergey, "Oslepit i zaglushit," *Russkoye oruzhiye*, August 8, 2018.

Pursiainen, Christer, "Russia's Critical Infrastructure Policy: What Do We Know About It?" *European Journal for Security Research*, Vol. 6, 2020, pp. 21–38.

"Putin Demands Smart, Precision-Guided Munitions from Defense Industry," Interfax, November 23, 2018.

Radin, Andrew, Lynn E. Davis, Edward Geist, Eugeniu Han, Dara Massicot, Matthew Povlock, Clint Reach, Scott Boston, Samuel Charap, William Mackenzie, Katya Migacheva, Trevor Johnston, and Austin Long, *The Future of the Russian Military: Russia's Ground Combat Capabilities and Implications for U.S.-Russia Competition*, Santa Monica, Calif.: RAND Corporation, RR-3099-A, 2019. As of May 2, 2022: https://www.rand.org/pubs/research_reports/RR3099.html

Ramm, Alexsey, "Minoborony smozhet zaglushit' Iridium I OneWeb," *Izvestiya*, August 30, 2016. As of July 28, 2022: https://iz.ru/news/629395

———, "God vysokotochnogo oruzhiya v 2017-m Rossiya sovershila proryv v oblasti sozdaniya i primeneniya sverkhtochnykh raket," *Izvestiya*, December 29, 2017.

Reach, Clint, *Russian Military Forecasting Translation Volume: 1999–2018*, Santa Monica, Calif.: RAND Corporation, RR-A198-5, 2022. As of May 2, 2022: https://www.rand.org/pubs/research_reports/RRA198-5.html

Reach, Clint, Alexis A. Blanc, and Edward Geist, *Russian Military Strategy: Organizing Operations for the Initial Period of War*, Santa Monica, Calif.: RAND Corporation, RR-A1233-1, 2022. As of December 9, 2022: https://www.rand.org/pubs/research_reports/RRA1233-1.html

Reach, Clint, Alyssa Demus, Eugeniu Han, Bilyana Lilly, Krystyna Marcinek, and Yuliya Shokh, *Russian Military Forecasting and Analysis: The Military-Political Situation and Military Potential in Strategic Planning*, Santa Monica, Calif.: RAND Corporation, RR-A198-4, 2022. As of July 26, 2022: https://www.rand.org/pubs/research_reports/RRA198-4.html

Reach, Clint, Vikram Kilambi, and Mark Cozad, *Russian Assessments and Applications of the Correlation of Forces and Means*, Santa Monica, Calif.: RAND Corporation, RR-4235-OSD, 2020. As of May 2, 2022: https://www.rand.org/pubs/research_reports/RR4235.html

Rog, B., "Strategiskaya zadacha aviatsii," *Armeiskii Sbornik*, No. 7, 2012, pp. 54–58.

Rogoway, Tyler, "Tomahawk Cruise Missiles Pummel Houthi Controlled Radar Sites in Yemen," *The Drive*, October 13, 2016a.

———, "It Has Begun: Russia Is Showcasing New Weapons in Fresh Syrian Offensive," *The Drive*, November 15, 2016b.

Rogozin, D. O., ed., *Voina i mir v terminakh i opredeleniiakh*, Moscow: Veche, 2017.

———, "Operatsiia strategicheskikh sil sderzhivaniia," *Voina i mir v opredeleniiakh*, Book 1, Moscow: Veche, 2017.

Romanov, A. A., and S. V. Cherkas, "Perspektivy razvitiia kosmicheskikh voisk Rossiiskoi Federatsii v usloviiakh sovremennykh tendentsii voenno-kosmicheskoi deiatel'nosti," *Voennaia Mysl'*, No. 9, 2020.

Rosoboroneksport, "R-330ZH: Avtomaticheskaya stantsiya pomekh abonentam sistem sputnikovoy svyazi 'INMARSAT', 'IRIDIUM' i sputnikovoy radionavigatsionnoy sistemy GPS," undated.

Rostovskii, Mikhail, "Sergei Shoigu rasskazal, kak spasali rossiiskuiu armiiu," *Moskovskii komsomolets*, September 22, 2019.

Rozin, Igor, "Next-Gen 'Kalibr' Cruise Corvette Joins Russia's Black Sea Fleet," *Russia Beyond*, February 10, 2021.

RussianShips.info, webpage, undated. As of December 29, 2021: http://russianships.info/

"Russia's Fourth Project 22160 Corvette 'Sergey Kotov' Starts Sea Trials," *Naval News*, October 29, 2021.

"Russia's FSB Unveils Broad List of Topics that Could Result in 'Foreign Agent' Label," RadioFreeEurope/RadioLiberty, October 1, 2021.

"Russia's S-550 Missile Defense System to Intercept Warheads Free of Nuclear Blast – Expert," TASS, November 16, 2021.

Ryabov, Kirill, "Den' innovatsiy YUVO: kompleks REB RB-341V 'Leyer-3,'" *Voennoe obozrenie*, October 16, 2015.

Sanger, David E., Clifford Krauss, and Nicole Perlroth, "Cyberattack Forces a Shutdown of a Top U.S. Pipeline," *New York Times*, last updated May 13, 2021.

Sivkov, Konstantin, "Nebesnye bastiony," *Voenno-promyshlennyi kur'er (VPK)*, February 18, 2019.

Skomorokhov, Roman, "Stantsiya REB R-934U 'Sinitsa'. Kogda 'Sinitsa' v pole, zhuravlyam v nebe tyazhko," *Voennoe obozrenie*, November 3, 2017.

Slipchenko, Vladimir, "Voini shestovo pokoleniya. Reshayushaya rol' v nikh budet prinadlezhat visotochnomy oruzhiyu," *Na Strazhe Rodiny*, No. 117, July 5, 1997.

———, *Voiny novogo pokolenia–Distantsionnye i bezkontaktnye*, 2006.

Slipchenko, Vladimir, and Makhmut Gareev, *Future War*, translation, Ft. Leavenworth, Kan.: Foreign Military Studies Office, 2007.

"Source Reveals Tech Details of New Russian Anti-Satellite Warfare Plane," Sputnik News, July 9, 2018.

Spirtas, Michael, Thomas-Durell Young, and S. Rebecca Zimmerman, *What It Takes: Air Force Command of Joint Operations*, Santa Monica, Calif.: RAND Corporation, MG-777-AF, 2009. As of May 2, 2022: https://www.rand.org/pubs/monographs/MG777.html

Starodubtsev, Yu. I., P. V. Zakalkin, and S. A. Ivanov, "Warfare in the Technosphere as the Basic Method of Settling Conflicts amid Globalization," *Military Thought*, Vol. 29, No. 3, 2020, pp. 80–85.

Sterlin, A., and A. Khriapin, "Ob osnovakh gosudarstvennoi politiki Rossiiskoi Federatsii v oblasti iadernogo sderzhivaniia," *Flag rodiny*, August 14, 2020.

Sterlin, A. E., A. A. Protasov, and S. V. Kreidin, "Sovremennye transformatsii kontseptsii i silovykh instrumentov strategicheskogo sderzhivaniia," *Voennaia mysl'*, Vol. 8, 2019.

"Strategic Operations in a Continental Theater of Strategic Military Action," *Journal of Slavic Military Studies*, Vol. 2, No. 2, 1989.

Sugden, Bruce M., "Nuclear Operations and Counter-Homeland Conventional Warfare: Navigating Between Nuclear Restraint and Escalation Risk," *Texas National Security Review*, Vol. 4, No. 4, Fall 2021, pp. 59–89.

Sukhanov, Sergei, "VKO – eto zadacha, a ne sistema," *Vozdushno-kosmicheskaya oborona*, March 29, 2010.

Sukhorutchenko, V. V., A. B. Zelvin, and V. A. Sobolevsky, "Napravleniye issledovaniy boyevykh vozmozhnostei vysokotochnogo oruzhiya bolshoi dalnosti v obychnom snaryazhenii," *Voennaia mysl'*, No. 8, 2009.

Sutton, H. I., "Russia Increasing Submarine Cruise Missile Capacity as US Navy Decreases Its Own," RUSI, August 19, 2021.

Svechin, Aleksandr A., *Strategy*, 2nd ed., trans. Kent Lee, ed., Minneapolis, Minn.: East View Publications, 1991.

"Syria Experience Prompts Need for Military Satellite Grouping, Says Russian Defense Chief," TASS, February 5, 2019.

Thomas, Timothy, "The Evolving Nature of Russia's Way of War," *Military Review*, July–August 2017, pp. 34–42.

Thompson, Allen, *The Altay Optical-Laser Center Sourcebook*, Federation of American Scientists, March 29, 2011.

————, *Sourcebook on the Okno, Okno-S, Krona and Krona-N Space Surveillance Sites*, Federation of American Scientists, November 19, 2014.

Tikhonov, Aleksandr, "Ministerstvo oborony RF otkryto k ravnopravnomu dialogu po obespecheniiu voennoi bezopasnosti," *Krasnaya Zvezda*, December 18, 2019.

Tirpak, John A., and Brian W. Everstine, "Syria Strike Marks Combat Debut for JASSM-ER," *Air Force Magazine*, April 15, 2018.

Tsymbalov, Aleksandr Georgiyevich, "O razvitii operativnikh form i sposobov deistvii voisk (sil) pri reshenii zadah VKO na sovremennom etape," *Vozdushno-kosmicheskaya oborona*, No. 3, 2012, pp. 32–40.

Tsyrendorzhiev, S. R., "O kolichestvennoi otsenke voennoi bezopasnosti," *Voennaia mysl'*, No. 10, 2014.

Turovsky, Daniil, *Vtorzhenie: Kratkaya istoriya russkikh khakerov*, 2019.

Unal, Beyza, *Cybersecurity of NATO's Space-Based Strategic Assets*, London: Chatham House, July 2019.

U.S. Air Force, "EC-130H Compass Call," webpage, last updated May 2015. As of January 20, 2022: https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104550/ec-130h-compass-call/

U.S. Congress, Office of Technology Assessment, *New Technology for NATO: Implementing Follow-On Forces Attack*, Washington, D.C.: U.S. Government Printing Office, OTA-ISC-309, June 1987.

U.S. Department of Defense, *Report to Congress: Kosovo/Operation Allied Force After-Action Report*, Washington, D.C., January 31, 2000.

————, *Nuclear Posture Review*, Washington, D.C., February 2018.

U.S. General Accounting Office, *Cruise Missiles: Proven Capability Should Affect Aircraft and Force Structure Requirements*, Washington, D.C., GAO/NSIAD-95-116, April 1995.

U.S. Space Command Public Affairs Office, "Russia Conducts Space-Based Anti-Satellite Weapons Test," July 23, 2020.

Ven Bruusgaard, Kristin, "Russian Nuclear Strategy and Conventional Inferiority," *Journal of Strategic Studies*, Vol. 44, No. 1, 2021, pp. 3–35.

Vershinin, Alex, "Feeding the Bear: A Closer Look at Russian Army Logistics and the Fait Accompli," *War on the Rocks*, November 23, 2021.

"Vertolet radioelektronnoy bor'by Mi-8MTPR1 na forume 'Armiya-2019,'" *Voyenno-tekhnicheskiy sbornik 'Bastion'*, January 29, 2020.

Vikulov, S. F., ed., *Aktual'nye problemy realizatsii voenno-ekonomicheskogo potentsiala Rossii v pervoi chetverti XXI veka i osnovnye napravleniia voenno-ekonomicheskikh issledovanii*, 2019.

Vitko, A. V., "Chernomorskii flot: faktor rasshireniia boevykh vozmozhnostei v zone otvetstvennosti," *Voennaia mysl'*, No. 7, 2017.

Voloshin, L. I., "Teoriia glubokoi operatsii i tendentsii ee razvititiia," *Voennaia mysl'*, No. 8, 1978, pp. 14–26.

"Vozrozhdeniye 'Belogo lebedya': kak obnovili boyevoy bombardirovshchik Rossii," TASS, January 25, 2018.

Watts, Barry D., *Six Decades of Guided Munitions and Battle Networks: Progress and Prospects*, Washington, D.C.: Center for Strategic and Budgetary Assessments, March 2007.

Weeden, Brian, and Victoria Sampson, eds., *Global Counterspace Capabilities: An Open Source Assessment*, Broomfield, Colo.: Secure World Foundation, April 2021.

Westerlund, Fredrik, and Susanne Oxenstierna, eds., and Gudrun Persson, Jonas Kjellén, Johan Norberg, Jakob Hedenskog, Tomas Malmlöf, Martin Goliath, Johan Engvall, and Nils Dahlqvist, *Russian Military Capability in a Ten-Year Perspective—2019*, Stockholm: Swedish Defence Research Agency, FOI-R--4758--SE, December 2019.

Whisler, Greg, "Strategic Command and Control in the Russian Armed Forces: Untangling the General Staff, Military Districts, and Service Main Commands (Part Two)," *Journal of Slavic Military Studies*, Vol. 33, No. 1, 2020, pp. 89–112.

Wood, Dakota L., ed., *2022 Index of U.S. Military Strength*, Washington, D.C.: Heritage Foundation, 2022. As of January 4, 2022: https://www.heritage.org/sites/default/files/2021-09/2022_IndexOfUSMilitaryStrength.pdf

Zak, Anatoly, *Russian Military and Dual-Purpose Spacecraft: Latest Status and Operational Overview*, Arlington, Va.: CNA, June 2019.

Zakvasin, Alexei, "Kozyr' v rukave: kakie perspektivnye vidy protivosputnikovogo vooruzheniia razrabatyvaiutsia v Rossii," RT, November 29, 2018.

Zarudnitskii, V. B., "Faktory dostizheniia pobedy v voennykh konfliktakh budushchego," *Voennaia mysl'*, No. 8, 2021a.

———, "Kharakter i soderzhanie voennykh konfliktov v sovremennykh usloviiakh i obozrimoi perspective," *Voennaia mysl'*, No. 1, 2021b.

Zolotarev, V. A., ed., *Istoriia voennoi strategii Rossii*, Moscow: Kuchkovo Pole/Poligrafresursy, 2000.

Zubov, N. P., "Sovershenstvovanie form primeneniia i sposobov deistvii aviatsionnykh formirovanii voenno-vozdushnykh sil," *Vestnik Akademii voennykh nauk*, Vol. 3, No. 76, 2021.

RAND NATIONAL DEFENSE RESEARCH INSTITUTE

For decades, the Russian military has been faced with the same problem: how to overcome the North Atlantic Treaty Organization's (NATO's) strategic depth in a time of strategic nuclear parity. In the late Soviet era, this was done by building up massive numbers of ground forces to overcome prepared defenses. In 2008, Russia drastically reduced its land forces in the hopes that long-range strike could compensate for a lack of mass on the ground in a regional war. Russian strategists have since focused on the ways and means through which Russia can conduct offensive actions throughout the entire depth of NATO without large numbers of ground forces.

As of 2021, Russia was still reliant to some degree on nonstrategic nuclear weapons (NSNW) for regional warfighting. Recent evidence suggests that Russian planning for regional war is trending toward a unified strategic operation. This notional concept is intended to more effectively organize and allocate Russia's conventional strike and nonkinetic attack capacity as it fills the role of Russian NSNW in regional war over the coming decades.

To understand why this trend is occurring, this report examined Russia's evolution toward a unified strategic operation and associated capability development, focusing on four areas: long-range conventional strikes against critical military and civilian targets; electronic warfare to disrupt NATO command, control, communications, computers, intelligence, surveillance, and reconnaissance; counterspace actions; and cyberattacks against critical infrastructure.

$48.00

ISBN-10 1-9774-0935-0
ISBN-13 978-1-9774-0935-5

54800

9 781977 409355

www.rand.org

RR-A1233-8