CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

DECEMBER 2022 | CYBER CONFLICT IN THE RUSSIA-UKRAINE WAR

Cyber Operations in Ukraine: Russia's Unmet Expectations

Gavin Wilde

Cyber Operations in Ukraine: Russia's Unmet Expectations

Gavin Wilde

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Contents

Cyber Conflict in the Russia-Ukraine War

The war in Ukraine is the largest military conflict of the cyber age and the first to incorporate such significant levels of cyber operations on all sides. Carnegie's series "Cyber Conflict in the Russia-Ukraine War" represents our first offerings in what will be a long, global effort to understand and learn from the cyber elements of the Ukraine war. We welcome queries from other authors interested in contributing to this endeavor by having us publish their work. If you would like to learn more, please contact Arthur Nelson at arthur.nelson@ceip.org.

Publications in this series:

- "Evaluating the International Support to Ukrainian Cyber Defense," Nick Beecroft, November 3, 2022
- "Cyber Operations in Ukraine: Russia's Unmet Expectations," Gavin Wilde, December 12, 2022
- "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," Jon Bateman, forthcoming

Summary

A review of academic, doctrinal, and journalistic writing covering the last three decades of Russian military theorizing on cyber-related issues yields three hypotheses that may explain the mismatch between the expectations of many Western observers and the reported impact of Russian cyber operations in the 2022 invasion of Ukraine.[1] By exploring the unique and oft-overlooked facets of Moscow's conceptualization of "cyber," this paper provides a foundation for better assessing Russia's performance in cyberspace in Ukraine in early 2022, along with a more nuanced understanding of its capabilities and possible expectations going forward. These hypotheses are as follows:

- Russia's Information Operations Troops—a rough analog to Western military cyber commands—remains in its infancy and appears optimized more for counterpropaganda than for offensive cyber operations. The operational command structure over offensive cyber operations, meanwhile, remains murky and is possibly more political than military in nature.

- Russia's premier offensive cyber capacities are housed within agencies focused on intelligence and subversion—the key tool kits used against Ukraine since 2014—rather than combined-arms warfare.

- Moscow's secretive and poorly executed February 2022 invasion precluded optimal performance in the initial period of the war, which is particularly pivotal in Russian thinking about effectiveness in the information domain.

These are each examined through Russia's own information warfare prism, which differs in crucial ways from Western conceptions of "cyber"—foremost in that it is more expansive, encompassing and emphasizing the psychosocial impacts of information and communication technologies on both the polity and the public.

Introduction: Seeing Through Moscow's Own Lens

To better understand the cyber aspects of Russia's early 2022 military incursion into Ukraine, analysts should account for the unique way in which Moscow views cyber operations and doctrinally conceptualizes success or failure in the cyber domain.

First, the very concept of "cyber" widely used in the United States and West—which largely emphasizes the technical integrity of networks—is rarely if ever used in the official Russian strategic and military lexicon. Instead, Moscow refers to "information confrontation" or "information war/warfare" to describe the range of operations—both technical and psychological, code and content—that can be deployed against adversarial systems and decisionmaking. Drawing on Soviet fears of ideological encroachment, as well as the humiliation and siege mentality cultivated since the Soviet collapse, the preponderance of Russia's emphasis falls on what the U.S. military terms the cognitive dimension, within what U.S. officials would call information operations.[2] Under this construct, offensive cyber operations are a subset of broader operations in the information environment designed to achieve as much a psychological impact as a technological one.[3]

Ultimately, Russian doctrine does not make the same distinction as the West between cyber and information operations. Rather, Russia's concept entangles the physical and psychological features of interstate conflict—now heavily mediated by technology—throughout the entirety of the information space.[4] For example, a 2011 document released by the Russian defense ministry defined information war as:

> "conflict between two or more states in information space with the goal of inflicting damage to information systems, processes, and resources, as well as to critically important structures and other structures; undermining political, economic, and social systems; carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government; as well as forcing a State to make decisions in the interests of their opponents."[5]

This definition is far more expansive than what U.S. analysts call "cyber warfare." It also helps explain the self-reinforcing conspiratorialism and post-truth tendencies of Russian operations.[6] As one Russian academic put it:

> "The specific feature of "information warfare" is the implicitness of its actors. Who is the organizer of these actions? Against whom are they really directed? This ambiguity, regardless of the actors, serves to both mythologize and demonize "information warfare." One can trace, at will, a motivational chain, a "cunning plan" behind any news story or event attributable to "enemies." This, of course, does not rule out the development or execution of such plans and projects by various political and social forces—both foreign and domestic...However, the actors in "information wars" have largely become the product of interpretations and discursive practices, which, in turn, are then also regarded as "information warfare."[7]

This conception also blurs the lines between foreign and domestic threats, drawing on Leninist themes of perpetual political struggle and concern over penetration by fifth columnists. The cyber-enabled tools of online surveillance and censorship within Russia's borders—and efforts to isolate Russia from the global internet—are mutually reinforcing with those deployed beyond them.[8] Moscow's foreign policy battles are often indistinguishable from its struggle for domestic regime stability.[9] In this regard, much of what the West views as aggression in the information space would be couched by Moscow in counteroffensive terms—chaff to drown out or distort signals from abroad that run counter to the Kremlin's preferred narratives before they can penetrate and take root within Russian society.[10]

Indeed, the fear of—and thus belief in—the efficacy of subliminal messaging is rooted in another vestige of Soviet-era strategic thought, which feeds contemporary Russian views of information warfare: reflexive control.[11] This theory postulates that an enemy can be

induced to make decisions of its own volition that are in fact disadvantageous to itself and beneficial to Russia. By this logic, practitioners would be able to ascertain "where, when, or how to insert specially developed information for the enemy consumer to digest, process, and act on, according to a Russian plan."[12] In contrast to the traditional Western principle of deterrence, which aims to clearly signal insurmountable superiority, reflexive control relies more on disguised manipulation.[13]

Secondly, as regards information warfare, Russian strategic culture has never adopted the conceptual lines Westerners often have between peacetime and wartime,[14] making an assessment of Moscow's success in the latter a somewhat arbitrary exercise. Even the lexicon typically used—struggle (*protivoborstvo*)—connotes a consistent, continuous interaction that may be accompanied by periods of cooperation or armed conflict but is subordinate to neither.[15] This tendency of thought, however, may not always work in Russia's favor. As the Ukraine incursion demonstrates, the requirements for speed, impact, and control in cyberspace increase dramatically during periods of conventional war,[16] as events on the ground—rather than merely access or capability—drive tactical and operational requirements.[17] The deeper understanding of a target network—what scholar Max Smeets calls "tacit knowledge," typically the province of intelligence services—is not readily transferable to a military unit for purposes of attack.[18] In other words, cyber forces built for perpetual struggle likely lack the surge capacity necessary during wartime.

These dynamics underscore the third major factor that must be considered: what constitutes success in Russia's comparatively broad and nebulous concept of information war? The readily available data regarding Russian operations in cyberspace can tell a vastly different story when viewed in isolation than they would when contextualized, both within Moscow's thinking and within the target environment. Activity does not automatically translate into achievement, however, nor investment of effort into impact.[19]

Analysts should not make the mistake of attributing intentionality to chance nor foreign orchestration to chaos. They should, however, use the metrics Moscow has adopted for itself in doctrinal and strategic documents—not solely damage assessments from within the targeted country—as a lens through which to judge success. There is predictive utility in gauging Kremlin focus and threat perception in the information space.[20] As experts note, "a clear-eyed assessment of where and just how much resourcing is being directed by an aggressive adversary can help shape our own policies regarding where and how our strategic trade-offs are positioned."[21] Moreover, analysts should allow for the possibility that Moscow has overestimated the strategic utility of information warfare writ large.[22]

With these caveats in mind, analysts can make more precise and informed assessments regarding Russian cyber performance in Ukraine. In that vein, what follows are several hypotheses that might help explain the unmet expectations of many Western analysts on that score.

Hypothesis #1: Information Troops Remain in Infancy and Are Optimized Primarily for Counterpropaganda

Whereas the eventual establishment of United States Cyber Command (USCC) was already being deliberated in the mid-2000s,[23] the prospect for a general Russian analog was not publicly raised by senior officials in Moscow until the 2010s—well after the 2008 Russo-Georgian War, the Arab Spring, and warming relations between Kyiv and the EU. These developments in particular had galvanized Moscow's thinking about information and its role in conflict.[24] After reportedly being formally envisioned and established sometime in 2014–2015, the existence of a Russian cyber-focused unit under military command—separate and distinct from the intelligence services in structure and mission focus—was not formally acknowledged publicly until 2017. Russian Defense Minister Sergey Shoygu at that time alluded to the Information Operations Troops (Voyska Informatsionnykh Operatsiy, or VIO) in a speech to the Russian parliament. If even only roughly accurate, this chronology would make the Russian VIO somewhere between six and eight years old as of the February 2022 renewed incursion into Ukraine. (A detailed time line of key events is outlined below.) Even so, some observers are skeptical that the VIO constitutes a rough USCC analog and assert that Moscow's cyber operations are orchestrated via political channels through the Security Council and the Presidential Administration rather than via a traditional military command structure.[25]

As Smeets recently wrote, "cyber capacity is primarily about people."[26] VIO's relative infancy extends to the experience of its cadres. According to Russian investigative journalists, the initial hunt to staff the VIO focused on recent graduates from technical universities and young programmers, while netting roughly a hundred personnel from private sector companies nationwide.[27] This suggests, in addition to a high degree of competition among Russian agencies for a relatively small pool of technical talent, a relative lack of both service and operational experience.

Prior to 2008, Moscow had viewed information warfare through a largely defensive prism, dedicated to information security—"the state of protection of its national interests in the information sphere defined by the totality of balanced interests of the individual, society, and the state"[28]—and to information assurance for the networks used by the armed forces. Meanwhile, Russian doctrinal writings typically refer to offensive cyber capabilities mostly in accusatory terms toward the United States and its allies, whom they allege have militarized the domain.[29] Expert Keir Giles, in analyzing Russia's 2011 "Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space," notes that the document "echo[es] the defensive theme of other Russian documents relating to cyberspace. . . and cite[s] in [its] preamble a statement of the external threat to Russia's information

security arising from other states developing information warfare concepts."[30] Consequently, a diplomatic push for treaty and multilateral constraints likely belied Moscow's fears that Russia had lagged behind other powers in developing military cyber capacity.[31] National Security Concepts released under President Vladimir Putin have also emphasized concerns that "the domination of some states in global information space and the development of information warfare techniques have not abated, and Russia is still squeezed out of this process."[32] Fears have permeated among security officials of "logic bombs" being planted within Russia's networks and "special content" being piped into its public.

In the aftermath of the Russo-Georgian war, however, leading Russian theorists bemoaned Tbilisi's resiliency in sustaining communications with its public and ability to cultivate global sympathy, symbolizing Russia's "utter inability to champion our goals and interest in the world information arena."[33] Moreover, Moscow has long recognized that political support within the United States and Europe is key to Western cohesion on foreign and security policy. These theorists therefore recommended a cadre of diplomats, academics, public relations professionals, and technologists, not only to neutralize enemy command and control but also to degrade adversary moral and cultural values and very ways of life.[34] Pressure began to build for a more unified organizational construct to match this theory.

Despite already having a relatively unified theory of information war at that time, "expertise in sensors, emitters, content, and code . . . hardly resembled one another. Each called for different equipment and training; there was scant reason for them to be organized together."[35] Meanwhile, a major portion of Russian offensive cyber prowess likely resided not in the military and security services but in the murky world of cyber criminals—though the symbiotic relationship between these actors would frequently be drawn upon for its coercive and disruptive potential on the international stage.[36] The preponderance of sophisticated offensive cyber talent under state auspices, meanwhile, rested within the putatively domestic-focused Federal Security Service (FSB)[37]—which, alongside the General Staff's Main Intelligence Directorate (GRU)[38] and Ministry of Internal Affairs, had fiercely resisted the idea of an increased military role in the cyber arena as recently as 2014.[39] As Smeets notes, "there is an interaction effect between the day-to-day mission of the cyber command and its ability to develop and maintain a certain capability."[40] Whether the Russian military has been able to do so independently of, in competition with, or via wartime subordination of, those services is disputable.

Perhaps consequently, a range of reports suggest the VIO had an initial organizational emphasis on information assurance, counterpropaganda, and psychological operations—much less on technical effects. Indeed, the threat outlined in Moscow's strategy and doctrinal writings is less a military than a psychological one, undermining Russia's influence and status, particularly along its periphery.[41] After a string of popular revolutions in former Soviet states, the Arab Spring, and the Bolotnaya Square protests in 2011 and 2012—with social media playing an increasingly larger role in each—Moscow conclusively ruled out the idea that any organic wellspring of public discontent was possible absent high-level orchestration from

abroad. This line of thought recalls the conspiracist streak of the Joseph Stalin era, during which Moscow's leading daily newspaper once declared: "We know that engines do not stop by themselves, machine tools do not break down on their own, boilers do not explode on their own. Someone's hand is hidden behind these events."[42]

This strain of thought also carried through even into the most recent Russian National Security Strategy in 2021, which explicitly calls out the danger of narratives and value systems being imposed from abroad via information technologies.[43] The Russian military has focused on expanding and enhancing the less technically intensive operations that sow socio-political discontent, possibly to the detriment of the often more complex malware operations carried out by intelligence services.[44]

Russia has relatively limited experience in framing doctrines and strategies around offensive cyber operations for the military, fewer and less experienced personnel in place to conduct them, and an emphasis on psychological rather than technical effects in the information space. This fact likely limited its ability to effectively incorporate such operations into a combined arms campaign in Ukraine. Meanwhile, even the most cunningly devised information operations are unlikely to yield capitulation by an enemy government, military, and population, however much Moscow has codified this as a strategic objective.[45]

Table 1. Time Line of Russia's Information Operations Troops

October 2008	In the aftermath of the Russo-Georgian War, information warfare theorist Igor Panarin details the need to "renew the mechanism for foreign policy propaganda."[46]
February 2010	Russia's military doctrine underscores that future conflicts will have an informational component. Information warfare will be essential for pre-conflict shaping of the political space and for "shaping a favorable response from the world community to the utilization of military force."[47]
January 2011	The Russian Ministry of Defense's (MOD) "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space" defines cyber operations in a defensive manner and information war as "actions that may damage information systems and resources; undermine political, economic, and social systems; brainwash the population; or coerce the victim government."[48]
March 2012	Then deputy prime minister Dmitry Rogozin alludes to discussions about the creation of a military command "to ensure the information security of both the armed forces and all the state infrastructure as a whole."[49]
Summer 2013	Rogozin calls social media "an element of 'cyberwar,' including against Russia."[50] Shoygu announces a "hunt" for young programmers.[51] Sources within MOD claim the establishment of an information troops unit is underway, with stand-up planned by the end of the year.[52] The primary tasks will be "processing outside information and combating cyber threats"; recruits are required to learn English.[53]

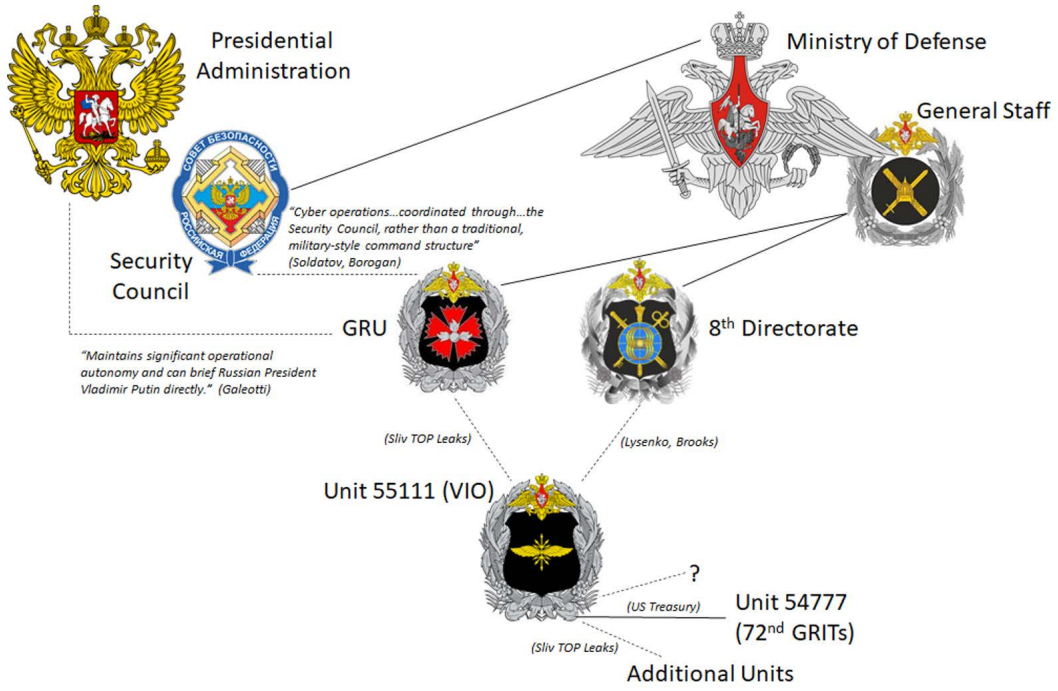
Table 1. Time Line of Russia's Information Operations Troops Continued

Spring 2014	The VIO is formally planned; a primary task is to defend military communications and control systems.[54] A Defense Ministry document, "Cybernetic Confrontation With a Potential Adversary," mentions the VIO, and sources explain its intent to "disrupt information networks."[55]
Late 2014	Authorities begin assigning conscripts to newly established army "research companies" of sixty troops each. They are expected to focus on cyber, information warfare, and propaganda. The companies putatively fall under the General Staff's Eighth Directorate and are located throughout the services, including within the GRU.[56] Russia's military doctrine emphasizes information warfare capabilities to withstand external influence.[57]
January 2015	The Eighth Directorate (Unit 31659) announces a major new tender for network protection services.[58]
October–November 2015	Reported time frame of the planned VIO stand-up.[59]
September 2016	The VIO reportedly participates in Kavkaz-2016 military exercises.[60]
February–March 2017	Shoygu confirms the VIO publicly. Commercial analysis alleges roughly 1,000 total troops across twelve to fourteen units, with a budget of $300 million.[61] Shoygu cites the VIO's Soviet-era "counterpropaganda" pedigree and the similarities of its tasking.[62] Reports surface of the VIO's remit over "traditional counterpropaganda."[63]
December 2020	The memoirs of an officer of the GRU's 72nd Main Intelligence Information Center (GRITs, or Unit 54777)[64] indicate that the unit was responsible for the overall planning of military psychological warfare.[65]
April 2021	Ukrainian Foreign Ministry spokesperson Oleg Nikolenko asserts that the Russian VIO "is creating the media backdrop to justify the crimes of the Russian army";[66] U.S. Treasury sanctions allege that the VIO oversees the GRU's key psychological warfare Unit 54777.[67]
May 2021	Unverified leaks to Russian activists also indicate that the VIO is designated as Unit 55111, which oversees Unit 54777.[68]
July 2022	Unverified leaks to Russian activists detail localized "information confrontation centers" subordinate to Unit 55111; departments include "disinformation," "counterpropaganda," "photo-video documentation," and "linguistic support." Reports conflict as to the ultimate chain of command over the VIO—whether it falls under the GRU, the General Staff's Eighth Directorate, or is possibly a mere amalgamation of extant GRU units that perhaps fall under an operational military command structure during wartime.[69]

Hypothesis #2: Bureaucratic Remit and Rivalry Favors Subversion Over War

After the Soviet collapse, the shared KGB pedigree among many senior figures in Kyiv and Moscow came to underpin what would become the FSB's primary purview over the

Figure 1. The VIO's Possible Command Structure



Note: See endnotes for sources.

Ukraine portfolio.[70] The service played key roles in attempting to prop up former Ukrainian president Viktor Yanukovych's regime in 2014,[71] oversaw political incursions in the United States throughout Donald Trump's presidency,[72] and plotted to depose Ukrainian President Volodymyr Zelenskyy's administration and install friendly forces in Kyiv in February 2022.[73] Only in May, after reportedly laying the latter catastrophic failure at the feet of the FSB, did Putin put the GRU in charge of intelligence on Ukraine.[74] However, even this shift could not alter some of the underlying dynamics that put the Russian services at a distinct disadvantage, especially their failure to evolve into a warfighting support apparatus. While Western intelligence agencies underwent foundational changes in the post-9/11 environment—including a shift toward greater sharing, integrated intelligence, surveillance, and reconnaissance (ISR), and open-source intelligence (OSINT) collection and analysis—Russia's "special services" largely further entrenched their KGB legacy tasks: covert surveillance, paramilitary action, and "active measures." Russia's leadership thus "entered the conflict almost entirely unprepared for the capabilities and uses of . . . 21st century intelligence."[75]

The two Russian state entities with demonstrated track records in such subversion—including through offensive cyber means—are the GRU and FSB.[76] Both have historically operated permissively in Ukrainian cyberspace, including a string of disruptive attacks in 2022.[77]

The two share a long-standing rivalry,[78] however, which has been rendered even more acute since the 2016 hacks of the U.S. Democratic National Committee and subsequent intrigues in Moscow, where several FSB officers were arrested for treason, ostensibly for implicating the GRU to Western contacts.[79] There are also grounds to suspect that the FSB maintains the competitive edge in offensive cyber tradecraft, technology, experience, and talent and is possibly loath to cede it in support of military objectives.[80] The FSB likely held an institutional view of Ukraine as part of its own home turf, potentially disinclining it from damaging crucial Ukrainian infrastructure that Russia would itself require in an invasion and occupation.[81] As the war dragged on and Russia's political aims shifted from seizing Kyiv outright,[82] the FSB may also have been reluctant to expend whatever crown jewels remained in its formidable stock of exploits.[83] Coordination and cooperation between the two are thus unlikely.

Meanwhile, what appeared to be preemptive Western advisories in spring 2022 regarding GRU-linked exploits Industroyer2 and Pipedream—apparently designed to disrupt Ukrainian electrical grids, industrial control systems, and supervisory control and data acquisition systems—may have neutralized two major arrows in Moscow's cyber quiver.[84] Whether any remain in reserve, or Russia's well of sophisticated exploits has largely run dry, remains an open question.

In both cases, the preponderance of Russian offensive cyber capability appears to belong to those Russian agencies servicing traditional intelligence, counterintelligence, and subversion (as opposed to warfighting) roles following a long Soviet-era legacy. As the doctrinal thinking outlined above suggests, even the most brazen and destructive cyber attacks historically unleashed in Ukraine appear to be part of a sociopolitical pressure campaign, not particularly intended to achieve any discrete, time-bound, or geographic objectives.[85] Meanwhile, available insights from 2022 (particularly the hack of U.S. satellite company Viasat)[86] potentially indicate Russian intent to divert Ukrainian operational communications into more surveillable channels rather than to merely block them outright—reflecting "a different set of priorities . . . that cyber espionage is playing a more important role than disruptive or degradative cyber-attacks."[87]

Chief of the General Staff Valery Gerasimov has notoriously opined about the need to emphasize nonmilitary means of conflict, highlighting the information environment as a vehicle for "long-range, hidden action upon not only critically important information infrastructure, but also upon the population of a country, directly influencing the condition of national security of a state."[88] The war in Ukraine may signify that Russia has overinvested in the latter at the expense of the former—by choice, constraint, inertia, or all three.[89] Moscow's consistent drumbeat of disruptive cyber attacks, as well as propaganda, disinformation, and online influence campaigns in the post–Maidan Uprising era, point toward a strategy of subversive erosion, wherein:

> "The goal is to maintain or achieve a favorable balance of power over the longer term rather than to fulfil a specific short-term objective . . . to erode

> the pillars of an adversary's strength, namely public support for the government, economic and industrial capacity, and, as a riskier option, military capabilities. . . . Establishing and maintaining exploitation of adversary systems at the scope and scale necessary to achieve strategic impact requires significant organizational capacity and, particularly, highly-skilled labor. As in traditional subversion, only the largest intelligence agencies will have enough of both to attempt this strategy."[90]

The FSB and the GRU appear to have done so independently of, if periodically concurrent with, the Russian military's kinetic operations.

Hypothesis #3: Falling Short in the Crucial Initial Period of War

The Russian conception postures the whole of the information space—including adversary forces, leadership, and society writ large—as an ecosystem to be decisively dominated, particularly in the run-up to kinetic exchange. It is precisely this period, however, where Moscow's efforts—across several domains—fell short. Timothy Thomas, an expert on Russian military thought, explained: "A state that is planning aggression will use peacetime or a period of threat to plant viruses, disorganize systems of the country it wants to attack, and launch wide-scale targeted information operations and intense reconnaissance activity."[91] Russia scholar Maria Snegovaya also recently noted: "A Russian information campaign is most effective at the early stages of a combat operation, when it provides cover for rapid military actions. . . . However, Russia lost this opportunity in its operations in the Luhansk and Donetsk regions. Russian troops were unable to penetrate these regions as promptly as in Crimea due both to the lack of military resources (the best forces were kept in Crimea) and to Russia's overestimation of the support it would receive in eastern Ukraine."[92]

Russian information warfare theorists have therefore underscored that the initial phase of an armed conflict is pivotal. The legendary General Makhmut Gareyev was convinced that information operations had the potential to blunt the onset of overt armed conflict.[93] At the same time, other generals specializing in the discipline have highlighted the importance of unleashing it in advance of armed conflict as a way of preparing the battlespace:[94]

> "Prior to an 'information strike,' all targets should be identified (including

> enemy information systems), enemy access to external information should be denied, credit and monetary circulation should be disrupted, and the populace should be subjected to a massive psychological operation—including disinformation and propaganda. This would be accomplished by careful pre-strike planning and long-term investments in reconnaissance and covert penetration into enemy systems."[95]

First emphasized in the early Soviet era, the initial period of war was defined in 2012 as the point when warring states conduct military operations involving armed formations that are "deployed before the start of war to achieve short-range strategic objectives, or to create favorable conditions for committing their main forces and continuing with more operations," while national information sources were protected from adversary influence.[96] During that period, military, economic, and technological measures should be taken in combination with psychological campaigns.[97] Some of this emphasis likely stems from the fact that Russian war-planning has long been underpinned by the assumption that it would be "the militarily inferior party in a regional or large-scale war against a technologically superior adversary."[98] This tendency, alongside overly secretive and ill-informed pre-invasion planning, appears to have been in effect as Moscow (and the West) overestimated its own abilities and underestimated Ukraine's—precisely during the period that its own doctrines deemed as most pivotal for information warfare.[99]

The wave of GRU-linked cyber attacks during the first week of Russia's renewed February 2022 incursion,[100] and the later exposure of two ominous but as-yet-unused exploits,[101] suggest Moscow at least attempted adherence to this doctrine. Alternatively, however, the spectrum of Moscow's long-running information warfare efforts against Ukraine dating as far back as 2013 raises the prospect that Ukraine's resilience and defenses had matured sufficiently over time to largely blunt whatever cyber and information operations Moscow's "special military operation" entailed.[102] This dynamic also underscores a major conceptual inconsistency: the demands of preparation for a combined-arms campaign do not lend themselves well to Moscow's more nebulous notions of information warfare as an ongoing, unending struggle.

Conclusion

By practicing strategic empathy for Moscow's historical views of the information space and the contest within it—particularly in the context of conventional armed conflict—analysts can avoid the false mirroring and faulty signaling that tends to plague discussions about offensive cyber operations and thus frame distorted expectations.[103] With regards to the cyber aspects of Russia's war on Ukraine, more robust insights into Moscow's thinking may also help explain why these operations fell short of the strategic impact that Moscow envisioned.[104] These three hypotheses—the infancy and putative focus of the VIO, the preponderance of cyber talent in the Russian national security ecosystem, and the pivotal nature of the initial period of war—share a common theme. Moscow's information warfare thinking, its offensive cyber capabilities, and its organizational construct proved simply unfit for purpose in an event-driven, combined-arms campaign of the sort undertaken in February 2022.

About the Author

Gavin Wilde is a senior fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace, where he applies his expertise on Russia and information warfare to examine the strategic challenges posed by cyber and influence operations, propaganda, and emerging technologies.

Acknowledgments

The author is grateful for generous contributions of time and expertise from Jon Bateman, Andrew Bowen, Michael van Landingham, Eli Levite, Arthur Nelson, George Perkovich, and Max Smeets.

Notes

1 Much remains unknown (and unknowable) about Russian cyber operations, including in Ukraine in 2022. This piece seeks solely to address an apparent mismatch between some Westerners' expectations and the unique features of Russian strategic thought on offensive cyber operations, particularly during a period of conventional war.

2 See Joint Publications 3-12 and 3-13 at "Joint Publications Operations Series: 3-0 Operations Series," U.S. Joint Chiefs of Staff, June 8, 2018, https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series; and "Joint Publication 3-13: Information Operations," U.S. Joint Chiefs of Staff, November 20, 2014, https://irp.fas.org/doddir/dod/jp3_13.pdf.

3 Niels Bo Poulsen and Jørgen Staun, eds., *Russia's Military Might: A Portrait of Its Armed Forces*, (Copenhagen: Djøf Forlag, 2021), 328, https://pure.diis.dk/ws/files/4534518/Russia_s_Military_Migth.pdf.

4 Greg Austin, Kai Lin Tay, and Munish Sharma, "Great-Power Offensive Cyber Campaigns: Experiments in Strategy," International Institute for Strategic Studies, February 24, 2022, 55, https://www.iiss.org/blogs/research-paper/2022/02/great-power-offensive-cyber-campaigns.

5 Timothy Thomas, "Russian Military Thought: Concepts and Elements," MITRE Corporation, August 26, 2019, 188, https://www.mitre.org/news-insights/publication/russian-military-thought-concepts-and-elements.

6 Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model," RAND Corporation, July 11, 2016, https://www.rand.org/pubs/perspectives/PE198.html.

7 Grigory L. Tulchinsky, "Information Wars as a Conflict of Interpretations: Activating the 'Third Party,'" *Russian Journal of Communication* 5, no. 3 (December 1, 2013): 244–51, https://doi.org/10.1080/19409419.2013.822054.

8 Justin Sherman, "Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior," Atlantic Council, July 12, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior.

9 Stephen Blank, "Russian Information Warfare as Domestic Counterinsurgency," *American Foreign Policy Interests* 35, no. 1 (January 1, 2013): 31–44, https://doi.org/10.1080/10803920.2013.757946.

10 "Russia Needs To Counter Mainstream Media, Head of RT Network Says," National Public Radio (NPR), June 9, 2017, https://www.npr.org/2017/06/09/532196946/russia-needs-to-counter-mainstream-media-head-of-rt-network-says.

11 Maria Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare," Institute for the Study of War, September 2015, 10-12, https://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf.

12 Thomas, "Russian Military Thought."

13 Dmitry Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy," Institut Français des Relations Internationales (IFRI) Security Studies Center, November 2015, http://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf.

14 Most notably by Russian Chief of the General Staff Valeriy Gerasimov, as detailed in Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows* (blog), July 6, 2014, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war.

15 Blagovest Tashev, Michael Purcell, and Brian McLaughlin, "Russia's Information Warfare: Exploring the Cognitive Dimension," *MCU Journal* 10, no. 2 (December 10, 2019): 129–47, https://doi.org/10.21140/mcuj.2019100208.

16 Lennart Maschmeyer, "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations," *International Security* 46, no. 2 (October 25, 2021): 51–90, https://doi.org/10.1162/isec_a_00418.

17 Daniel Moore (@ILDannyMoore), "3rd bit from the "Offensive Cyber Operations" book! On distinguishing between op types. * Presence-based ops: intel ops ending with an attack (e.g. Industroyer, Viasat op) * Event-based ops: field-ready, robust abilities (e.g. EW pods, CEMA teams, some wipers)" Tweet, June 5, 2022, https://twitter.com/ILDannyMoore/status/1533471115208802305/photo/1.

18 Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (London, UK: Hurst Publishers, 2022), 89.

19 Michael Kofman, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer, "Lessons From Russia's Operations in Crimea and Eastern Ukraine," RAND Corporation, May 9, 2017, https://www.rand.org/pubs/research_reports/RR1498.html.

20 Gavin Wilde, "Assess Russia's Cyber Performance Without Repeating Its Past Mistakes," War on the Rocks, July 21, 2022, https://warontherocks.com/2022/07/assess-russias-cyber-performance-without-repeating-its-past-mistakes.

21 Nina A. Kollars and Michael B. Petersen, "Feed the Bears, Starve the Trolls," *The Cyber Defense Review*, Special Edition (2019): 145–58.

22 Timothy Thomas, "Information Weapons: Russia's Nonnuclear Strategic Weapons of Choice," *The Cyber Defense Review* 5, no. 2 (Summer 2020): 125–141.

23 John C.K. Daly, "US Air Force Prepares for Cyber Warfare," Space Daily, October 9, 2006, https://www.spacedaily.com/reports/US_Air_Force_Prepares_For_Cyber_Warfare_999.html.

24 Austin, Tay, and Sharma, "Great-Power Offensive Cyber Campaigns," chap. 3.

25 Andrei Soldatov and Irina Borogan, "Russian Cyberwarfare: Unpacking the Kremlin's Capabilities," Center for European Policy Analysis (CEPA), September 8, 2022, https://cepa.org/wp-content/uploads/2022/09/Unpacking-Russian-Cyber-Operations-9.2.22.pdf.

26 Smeets, *No Shortcuts*, 168.

27 "ГРУ — это вообще что? Кого берут в шпионы? И почему их так часто раскрывают? Даниил Туровский отвечает на главные вопросы про российскую разведку," Meduza, accessed July 11, 2022, https://meduza.io/feature/2018/10/15/gru-eto-voobsche-chto-kogo-berut-v-shpiony-i-pochemu-ih-tak-chasto-raskryvayut; Даниил Туровский, "Российские вооруженные киберсилы Как государство создает военные отряды хакеров," Meduza, 2016, https://meduza.io/feature/2016/11/07/rossiyskie-vooruzhennye-kibersily.

28 Timothy L. Thomas, "Information Security Thinking: A Comparison of U.S., Russian, and Chinese Concepts," in Proceedings of the International Seminar on Nuclear War and Planetary Emergencies — 26th Session (Erice, Italy: WORLD SCIENTIFIC, 2002), 344–56, https://doi.org/10.1142/9789812776945_0032.

29 Charles Billo and Welton Chang, *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States* (Hanover: Institute for Security Technology Studies at Dartmouth College, 2004); Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol, CA: O'Reilly Media, 2012), 161–177.

30 Keir Giles, "Russia's Public Stance on Cyberspace Issues," in *2012 International Conference on Cyber Conflict* (Tallinn, Estonia: NATO CCD COE Publications, 2012), 1–13, https://www.researchgate.net/publication/261044707_Russia's_public_stance_on_cyberspace_issues.

31 Sergei Medvedev, "Offense-Defense Theory Analysis of Russian Cyber Capability" (master's thesis, Naval Postgraduate School, 2015), https://calhoun.nps.edu/handle/10945/45225; and Keir Giles, "'Information Troops' - A Russian Cyber Command?" (2011 3rd International Conference on Cyber Conflict, Tallinn, Estonia: NATO CCD COE Publications, 2011), 45–60, http://195.222.11.251/uploads/2018/10/InformationTroopsARussianCyberCommand-Giles.pdf.

32 Dmitry Polikanov, "Russia's Perception and Hierarchy of Security Threats," *Connections* 4, no. 2 (2005): 85–92; and "Doctrine of Information Security of the Russian Federation," Ministry of Foreign Affairs of the Russian Federation, December 5, 2016, https://mid.ru/en/foreign_policy/fundamental_documents/1539546.

33 Stephen J. Blank and Richard Weitz, eds., *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald* (Fort Belvoir, VA: Defense Technical Information Center, 2010), 279, 282, https://apps.dtic.mil/sti/pdfs/ADA525166.pdf.

34 Ibid.

35 Martin C. Libicki, "The Convergence of Information Warfare," in *Information Warfare in the Age of Cyber Conflict*, ed. Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec, (Abingdon: Routledge, 2020), 15–26, https://doi.org/10.4324/9780429470509-2. While there is a natural symbiosis between cyber and electronic warfare, the latter is beyond the scope of this paper. Additional insights can be found at Bryan Clark, "The Fall and Rise of Russian Electronic Warfare," IEEE Spectrum, July 30, 2022, https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare.

36 Peter Warren, "Hunt for Russia's Web Criminals," *Guardian*, November 15, 2007, https://www.theguardian.com/technology/2007/nov/15/news.crime.

37 Kevin P. Riehle, *Russian Intelligence: A Case-Based Study of Russian Services and Missions Past and Present* (Bethesda, Maryland: National Intelligence University Press, 2022), https://www.scuolafilosofica.com/10883/kgb-gru-fsb-russian-intelligence-history-and-present; "Как Минобороны России планирует участвовать в информационных войнах," Главные события в России и мире | RTVI, accessed July 11, 2022, https://rtvi.com/stories/minfovoyna.

38 While it falls under the Ministry of Defense organizational and military command structure, the GRU enjoys a great deal of operational autonomy, political clout, and broad purview over battlefield reconnaissance and signals intelligence. Even within that shared structure, it likely guards these remits jealously. See Andrew Bowen, "Russian Military Intelligence: Background and Issues for Congress," Congressional Research Service, November 16, 2021, https://www.everycrsreport.com/reports/R46616.html.

39 Keir Giles and Anthony Seaboyer, "Russian Special Forces and Intelligence Information Effects," Royal Military College of Canada, March 2019, 60, https://cradpdf.drdc-rddc.gc.ca/PDFS/unc340/p810875_A1b.pdf.

40 Smeets, *No Shortcuts*, 168.

41 Stephen Blank, "Threats to and from Russia: An Assessment," *The Journal of Slavic Military Studies* 21, no. 3 (September 3, 2008): 491–526, https://doi.org/10.1080/13518040802313746; and Joe Cheravitch, "The Role of Russia's Military in Information Confrontation," Center for Naval Analyses, June 25, 2021, 54, https://www.cna.org/reports/2021/06/The-Role-of-Russia%27s-Military-in-Information-Confrontation.pdf.

42 Gabor Rittersporn, *Anguish, Anger, and Folkways in Soviet Russia* (Pittsburgh: University of Pittsburgh Press, 2014), 34.

43 "What You Need to Know about Russia's 2021 National Security Strategy," Meduza, July 5, 2021, https://meduza.io/en/feature/2021/07/05/what-you-need-to-know-about-russia-s-2021-national-security-strategy.

44 Joe Cheravitch and Bilyana Lilly, "Russia's Cyber Limitations in Personnel Recruitment and Innovation, Their Potential Impact on Future Operations and How NATO and Its Members Can Respond," in *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, ed. Amy Ertan, Kathryn Floyd, Piret Pernik, and Tim Stevens (Tallin: NATO CCDCOE Publications, 2020), 29, https://ccdcoe.org/uploads/2020/12/2-Russias-Cyber-Limitations-in-Personnel-Recruitment-and-Innovation_ebook.pdf.

45 Timothy Thomas, "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?," *The Journal of Slavic Military Studies* 27, no. 1 (January 2, 2014): 101–30, https://doi.org/10.1080/13518046.2014.874845.

46 "Система Информационного Противоборства | Еженедельник «Военно-Промышленный Курьер," August 4, 2018, https://dzen.ru/media/id/5a737163a86731b1a50d037f/sistema-informacionnogo-protivoborstva--5b65616db3263300a9c76480; and Emilio J. Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," US Army War College Quarterly: Parameters 47, no. 2 (June 1, 2017), https://doi.org/10.55540/0031-1723.2931.

47 Stephen Blank, ed., *Russian Military Politics and Russia's 2010 Defense Doctrine* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2011).

48 Ministry of Defense of the Russian Federation, "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space," NATO CCDCOE, January 1, 2011, https://ccdcoe.org/uploads/2018/10/Russian_Federation_unofficial_translation.pdf.

49 "Кибервойска Федерации," Актуальные комментарии, March 21, 2012, http://actualcomment.ru/kibervoyska_federatsii.html.

50 Р. И. А. Новости, "Рогозин счел соцсети элементом современной кибервойны," РИА Новости, last updated January 3, 2020, https://ria.ru/20130607/942041898.html.

51 "Сергей Шойгу объявил о «большой охоте» на молодых программистов," CNews.ru, July 4, 2013, https://www.cnews.ru/news/top/sergej_shojgu_obyavil_o_bolshoj_ohote.

52 "В 2013 Году России Появятся Свои Кибервойска - Российская Газета," July 5, 2013, https://rg.ru/2013/07/05/cyberwar-site-anons.html.

53 Туровский, "Российские вооруженные киберсилы Как государство создает военные отряды хакеров."

54 "Источник в Минобороны: В Вооруженных Силах РФ Созданы Войска Информационных Операций - ТАСС," ТАСС, May 12, 2014, https://tass.ru/politika/1179830.

55 "В России созданы кибервойска," vesti.ru, March 12, 2014, https://www.vesti.ru/article/1840746.

56 Volodymyr Lysenko and Catherine Brooks, "Russian Information Troops, Disinformation, and Democracy," *First Monday* 23, no. 5 (April 30, 2018), https://doi.org/10.5210/fm.v22i5.8176.

57 Dmitri Trenin, "2014: Russia's New Military Doctrine Tells It All," Carnegie Endowment for International Peace, December 29, 2014, https://carnegiemoscow.org/commentary/57607.

58 РИА Новости, "Минобороны РФ направит почти 43,5 млн руб на защиту от кибервирусов," РИА Новости, last updated March 2, 2020, https://ria.ru/20150127/1044570661.html.

59 "Минобороны РФ создаст в Крыму отдельную часть войск информационных операций," Meduza, April 17, 2015, https://meduza.io/news/2015/04/17/minoborony-rf-sozdast-v-krymu-otdelnuyu-chast-voysk-informatsionnyh-operatsiy.

60 "Военные РФ Впервые Отработали Информационное Противоборство На Учениях 'Кавказ' - ТАСС," ТАСС, September 14, 2016, https://tass.ru/armiya-i-opk/3619816?.

61 "В российской армии официально созданы кибервойска," vesti.ru, February 22, 2017, https://www.vesti.ru/article/1694456; "В российской армии официально созданы кибервойска," vesti.ru, February 22, 2017, https://www.vesti.ru/article/1694456.

62 РИА Новости, "Шойгу рассказал о задачах войск информационных операций," РИА Новости, February 22, 2017, https://ria.ru/20170222/1488617708.html.

63 Alexander Stepanov, "Кибермрмия - В Минобороны созданы подразделения для информационных спецопераций в Интернете," versia.ru, last updated March 16, 2017, https://versia.ru/v-minoborony-sozdany-podrazdeleniya-dlya-informacionnyx-specoperacij-v-internete; "Стали известны данные о войсках «психов» России.," Трибун, February 6, 2018, https://tribun.com.ua/47273.

64 "Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections," U.S. Department of the Treasury, April 15, 2021, https://home.treasury.gov/news/press-releases/jy0126.

65 Michael Weiss, "Aquarium Leaks: Inside the GRU's Psychological Warfare Program," Free Russia Foundation, December 7, 2020, 70–71, https://www.4freerussia.org/aquarium-leaks-inside-the-gru-s-psychological-warfare-program.

66 "Информационные войска РФ формируют медийный 'фон' для оправдания преступлений российской армии - МИД," Информационное агентство Украинские Национальные Новости (УНН), April 6, 2021, https://www.unn.com.ua/ru/news/1923859-informatsiyni-viyska-rf-formuyut-mediyniy-fon-dlya-vipravdannya-zlochiniv-rosiyskoyi-armiyi-mzs.

67 Jazlyn Melnychuk and Janne Hakala, "Russia's Strategy in Cyberspace," NATO Strategic Communications Centre of Excellence, June 11, 2021, https://stratcomcoe.org/publications/russias-strategy-in-cyberspace/210.

68 Sliv TOP, "Как ГРУ и ФСБ по приказу Путина вербуют молодежь в постсоветских странах," July 5, 2021, https://sliv.top/2021/07/05/kak-gru-i-fsb-po-prikazu-putina-verbuyut-molodezh-v-postsovetskih-stranah.

69 For additional details, see Weiss, "Aquarium Leaks"; Soldatov and Borogan, "Russian Cyberwarfare"; Lysenko and Brooks, "Russian Information Troops"; and Sliv TOP, "Центры информационных операций ГРУ ГШ в ваших руках," July 22, 2022, https://sliv.top/2022/07/22/czentry-informaczionnyh-operaczij-gru-gsh-v-vashih-rukah.

70 Юлия Самсонова, "Агенты влияния. Кто управлял Службой безопасности Украины," ФОКУС, July 3, 2015, https://focus.ua/politics/332609; and Andrei Soldatov, "The True Role of the FSB in the Ukrainian Crisis," Moscow Times, April 15, 2014, https://www.themoscowtimes.com/2014/04/15/the-true-role-of-the-fsb-in-the-ukrainian-crisis-a33985.

71 Andrei Soldatov, "Департамент оперативной информации (ДОИ)," Agentura.ru, December 27, 2021, https://agentura.ru/profile/federalnaja-sluzhba-bezopasnosti-rossii-fsb/departament-operativnoj-informacii-doi.

72 Gavin Wilde and Justin Sherman, "Targeting Ukraine Through Washington: Russian Election Interference, Ukraine, and the 2024 US Election," Atlantic Council, March 14, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/targeting-ukraine-through-washington.

73 Isaac Chotiner, "Putin's Pivot to a 'Really Big War' in Ukraine," *New Yorker*, May 24, 2022, https://www.newyorker.com/news/q-and-a/putins-pivot-to-a-really-big-war-in-ukraine.

74 "Putin Gives GRU Boosted Role in Ukraine – Report," *Moscow Times*, May 11, 2022, https://www.themoscowtimes.com/2022/05/11/putin-elevates-gru-in-ukraine-intelligence-gathering-report-a77632.

75 Philip Davies and Toby Steward, "No War for Old Spies: Putin, the Kremlin and Intelligence," Royal United Services Institute for Defense (RUSI), May 20, 2022, https://rusi.org/explore-our-research/publications/commentary/no-war-old-spies-putin-kremlin-and-intelligence.

76 Andrew Bowen, "In Focus: Russian Cyber Units," Congressional Research Service, February 2, 2022, https://crsreports.congress.gov/product/pdf/IF/IF11718.

77 Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired*, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine; and "Timeline of Cyberattacks and Operations," CyberPeace Institute, accessed July 14, 2022, https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline.

78 Mark Galeotti, "Putin's Hydra: Inside Russia's Intelligence Services," European Council on Foreign Relations (ECFR), 2016, https://ecfr.eu/wp-content/uploads/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf; Poulsen and Staun, *Russia's Military Might*, 342.

79 Mark Galeotti, "NATO Review - Russian Intelligence Is at (Political) War," NATO Review, May 12, 2017, https://www.nato.int/docu/review/articles/2017/05/12/russian-intelligence-is-at-political-war/index.html; Amy Knight, "This Russian Spy Agency Is in the Middle of Everything," *Daily Beast*, last updated August 8, 2018, https://www.thedailybeast.com/this-russian-spy-agency-is-in-the-middle-of-everything; Editorial Team, "CrowdStrike's Work With the DNC: Setting the Record Straight," CrowdStrike, June 5, 2020, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee; and Cheravitch and Lilly, "Russia's Cyber Limitations," 43.

80 РТВИ, "Как Минобороны России планирует участвовать в информационных войнах," August 28, 2018, https://rtvi.com/stories/minfovoyna; Giles, "'Information Troops' - A Russian Cyber Command?"; Riehle, Russian Intelligence; Bilyana Lilly and Joe Cheravitch, "The Past, Present, and Future of Russia's Cyber Strategy and Forces," in 2020 12th International Conference on Cyber Conflict (CyCon) (2020 12th International Conference on Cyber Conflict (CyCon), Estonia: IEEE, 2020), 129–55, https://ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf; Cheravitch and Lilly, "Russia's Cyber Limitations," 44; Antonio Villalón, "The Russian ICC (V): FSB," Security Art Work, December 20, 2016, https://www.securityartwork.es/2016/12/20/the-russian-icc-v-fsb; and RFE/RL Russian Service, "Investigative Report: On the Trail of the 12 Indicted Russian Intelligence Officers," Radio Free Europe/Radio Liberty, July 19, 2018, https://www.rferl.org/a/investigative-report-on-the-trail-of-the-12-indicted-russian-intelligence-officers/29376821.html.

81 Tara Copp, "Why Is Ukraine's Internet Still Up? Perhaps Because the Invaders Need It," Defense One, March 7, 2022, https://www.defenseone.com/threats/2022/03/why-ukraines-internet-still-perhaps-because-invaders-need-it/362854.

82 Michael Kofman and Rob Lee, "Not Built for Purpose: The Russian Military's Ill-Fated Force Design," War on the Rocks, June 2, 2022, https://warontherocks.com/2022/06/not-built-for-purpose-the-russian-militarys-ill-fated-force-design.

83 Andrew Greenberg, "The Russian Hackers Playing 'Chekhov's Gun' With US Infrastructure," Wired, October 26, 2020, https://www.wired.com/story/berserk-bear-russia-infrastructure-hacking.

84 Daniel Pereira, "Industroyer2 and Pipedream ICS/SCADA Malware: DOE, CISA, NSA, and the FBI Release Joint Cybersecurity Advisory," OODA Loop, April 15, 2022, https://www.oodaloop.com/ooda-original/2022/04/15/industroyer2-and-pipedream-ics-scada-malware-doe-cisa-nsa-and-the-fbi-release-joint-cybersecurity-advisory.

85 Austin, Tay, and Sharma, "Great-Power Offensive Cyber Campaigns," 57.

86 Sam Cohen, "AcidRain Malware and Viasat Network Downtime in Ukraine: Assessing the Cyber War Threat," Just Security, September 12, 2022, https://www.justsecurity.org/83021/acidrain-malware-and-viasat-network-downtime-in-ukraine-assessing-the-cyber-war-threat.

87 Nadiya Kostyuk and Aaron Brantly, "War in the Borderland Through Cyberspace: Limits of Defending Ukraine Through Interstate Cooperation," *Contemporary Security Policy* 3, vol. 43 (June 29, 2022): 1–18, https://doi.org/10.1080/13523260.2022.2093587.

88 Dave Johnson, "General Gerasimov on the Vectors of the Development of Military Strategy," Russian Studies Series, NATO Defense College, last updated March 30, 2019, https://www.ndc.nato.int/research/research.php?icode=585.

89 Cheravitch and Lilly, "Russia's Cyber Limitations" 46; and Cheravitch, "The Role of Russia's Military in Information Confrontation," 1–2, 7–8.

90 Lennart Maschmeyer, "A New and Better Quiet Option? Strategies of Subversion and Cyber Conflict," *Journal of Strategic Studies* (July 27, 2022): 1–25, https://doi.org/10.1080/01402390.2022.2104253.

91 Thomas, "Russian Military Thought," 7–5.

92 Snegovaya, "Putin's Information Warfare in Ukraine."

93 Jacob W. Kipp, "Confronting the RMA in Russia," U.S. Foreign Military Studies Office, June 1997, 4–5.

94 Sergei G. Chekinov and Sergei A. Bogdanov, "The Art of War in the Early 21st Century: Issues and Opinions," Voyennaya Mysl (Military Thought), 2015.

95 Billo and Chang, *Cyber Warfare*, 115.

96 Thomas, "Russian Military Thought," 7–5.

97 Timothy Thomas, "The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking," *Journal of Slavic Military Studies* 29, no. 4, October 14, 2016, 554–575.

98 Michael Kofman, Anya Fink, Dmitry Gorenburg, Mary Chesnut, Jeffrey Edmonds, and Julian Waller, "Russian Military Strategy: Core Tenets and Operational Concepts," Center for Naval Analyses, August 2021, ii, https://www.cna.org/archive/CNA_Files/pdf/russian-military-strategy-core-tenets-and-operational-concepts.pdf.

99 Greg Miller and Catherine Belton, "Russia's Spies Misread Ukraine and Misled Kremlin as War Loomed," *Washington Post*, August 19, 2022, https://www.washingtonpost.com/world/interactive/2022/russia-fsb-intelligence-ukraine-war.

100 CyberPeace Institute, "Timeline of Cyberattacks and Operations."

101 Pereira, "Industroyer2 and Pipedream ICS/SCADA Malware."

102 Lionel Beehner, Liam Collins, and Robert Person, "The Fog of Russian Information Warfare," in *Perceptions Are Reality: Historical Case Studies of Information Operations in Large-Scale Combat Operations*, ed. Mark D. Vertuli and Bradley S. Loudon (Leavenworth: Army University Press, 2018), 207, 39–43.

103 Erica Borghard, "The 'Known Unknowns' of Russian Cyber Signaling," Council on Foreign Relations, April 2, 2018, https://www.cfr.org/blog/known-unknowns-russian-cyber-signaling.

104 Also see Nick Beecroft, "Evaluating the International Support to Ukrainian Cyber Defense," Carnegie Endowment for International Peace, November 3, 2022, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322.

Carnegie Endowment for International Peace

The Carnegie Endowment for International Peace is a unique global network of policy research centers around the world. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

Program

The Carnegie Technology and International Affairs Program (TIA) helps governments and industries reduce large-scale international risks of new technologies and related services. Recognizing that commercial actors control many of the most germane technologies, TIA identifies best practices and incentives that can motivate industry stakeholders to pursue growth by enhancing rather than undermining international relations.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org