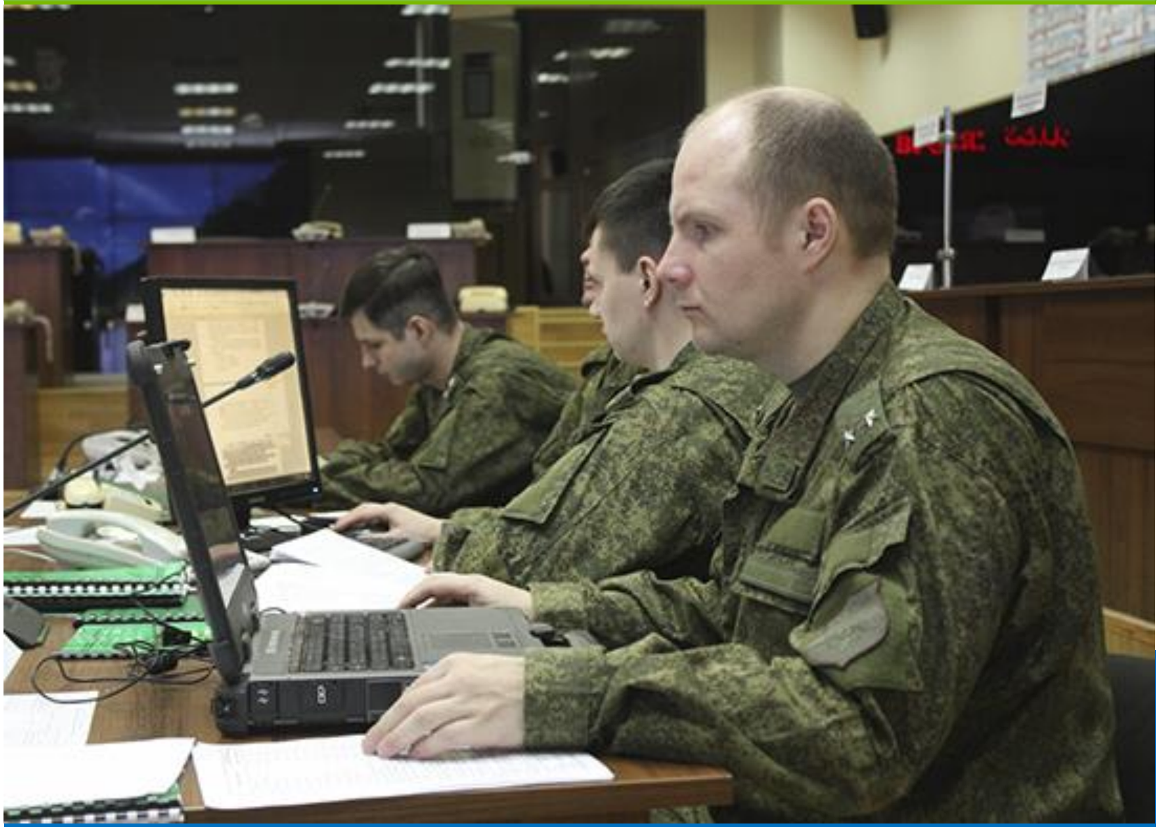
CNA

June 2021



# The Role of Russia's Military in Information Confrontation

Joe Cheravitch

IOP-2021-U-030078-Final

**Abstract**

In this CNA Occasional Paper, Joe Cheravitch, Doctoral Student at King's College London, traces the evolution of Russian military thought on computer network operations such as cyberattacks and espionage. Examining Russia's cyber capabilities, as well as changes in doctrine and strategy, Cheravitch analyzes the ways and means of Russia's unique approach to "information confrontation," which has caught the West by surprise on a number of recent occasions. The report also explores possible future scenarios of Russian military cyber operations and notes the need for continuous study of Russia's military and its approach to modern conflict.

This report is part of a series generously funded by a grant from the Carnegie Corporation of New York.

CNA's Occasional Paper series is published by CNA, but the opinions expressed are those of the author(s) and do not necessarily reflect the views of CNA or the Department of the Navy.

**Distribution**

**DISTRIBUTION STATEMENT A.** Approved for public release: distribution unlimited.

06/25/2021

This work was performed under Specific Authority Contract No. G-19-56503

**Cover image credit**: "Специалисты информационной безопасности ЦВО в ходе учения отразили хакерскую атаку условных террористов" [CVO information security specialists repelled a hacker attack from mock terrorists during an exercise], Ministry of Defence of the Russian Federation (Russian Defense Ministry), January 19, 2018, https://function.mil.ru/news_page/country/more.htm?id=12158781@egNews.

**Approved by**: **June 2021**

Michael Kofman, Research Program Director
Russia Studies Program
Strategy, Policy, Plans, and Programs Division

Request additional copies of this document through inquiries@cna.org.

# Executive Summary

Between the collapse of the Soviet Union in 1991 and Russia's annexation of Crimea over two decades later, international attention toward Russia's military waned significantly from its apogee during the Cold War. Russia's military, however, hardly remained static and underwent significant changes as it strove to adapt to perceived shifts in contemporary warfare. While rapid evolutions in digital communications technology during the late 20th and early 21st centuries were certainly seen as a critical threat in Russian defense circles, they also offered a new means of undermining adversaries from virtually unlimited distances. Conflicts of the future, according to many Russian analysts and observers, hinged on control of "information resources," which involved everything from jamming enemy battlefield communications to using mass media to turn a population against its leadership. The West was therefore caught by surprise in 2014, when Russia's military and security services began to use a wide array of computer network operations, electronic warfare, and digital influence platforms to help facilitate kinetic activities in Crimea and eastern Ukraine while disrupting Ukraine's new government and its international partners. Since then, a litany of cyberattacks—many of which have been attributed to Russian military intelligence—and seemingly novel approaches to military operations in Russia's periphery and abroad have reinvigorated studies in Russian military affairs, attracting a growing number of analysts tasked with deciphering Russia's motivations and methods.

This paper aims to trace Russian military thought related to the technical aspects of computer network operations, such as cyberattacks and espionage, from its early post-Soviet origins to current activity. Drawing on open source data, it will examine the Russian military's cyber capabilities, the forces and means behind notable operations, on top of evolutions in relevant strategy and doctrine. Throughout the paper, the term *information confrontation* defines these capabilities and conceptualizes their place in modern conflict. A brief section on terminology will describe the debate surrounding the Russian definition of cyber operations, explaining why the term "information confrontation" is most appropriate in this context. Finally, the paper concludes with potential future scenarios regarding the Russian military's approach to cyber operations. Probably the most important lesson this paper imparts is the need for continuous study of Russia's military and its approach to modern conflict, particularly its operations in the dimension between interstate harmony and overt conflict—the uneasy peace that currently defines relations between Moscow and the West.

This page is intentionally left blank.

# Contents

This page is intentionally left blank.

# Introduction

The Russian military's adoption of emerging technology related to computer network operations and signals intelligence, coupled with its continued improvisation with its largely Cold War–era electronic warfare arsenal, represents one of the most successful aspects of Russian military modernization since the collapse of the Soviet Union. Given the discrepancy in resources between Russia and its perceived adversaries, the ability to use constantly evolving digital communications and computing technology offered a means to help bridge the capabilities gap that continues to separate Moscow from many of its rivals. Additionally, Western militaries' increasing dependence on the same technological advances for enhanced communication and control presented potential weaknesses worth exploiting, which Russian defense officials and experts quickly recognized. In 1998, well aware of the difficult position facing Russia's military during its immediate post-Soviet nadir, Nikolai Mikhailov, a former deputy secretary on Russia's security council, was one of many defense officials to see potential in developing "asymmetric" technologies to "devalue the gigantic expenditures" of rivals' efforts to create a "new generation of weapons" in the 21st century.[1] Statements by government and military officials regarding the importance of cyber specialists, plus quasi-national holidays like Military Signalman's Day, established in 2006, or Electronic Warfare Specialist's Day, in 1999, accentuated the critical role these cadres would occupy in contemporary Russian national security.

Nevertheless, cyber capabilities have historically lagged behind Russian defense luminaries' conceptualization of their use. Incongruities not only between military thought and actual capabilities, but also between the Soviet Union and its adversaries during the Cold War, forced a culture of improvisation involving signals intelligence and computer-driven intelligence collection and analysis. Historian Jonathan Haslam described this situation in 2015:

> Stymied by backwardness in invention, Soviet engineers in the military-industrial complex proved their genius through mastering the art of improvisation. They applied the law of comparative advantage: making full use of what lay at hand rather than mimicking the other side, treating fundamental asymmetries not as reason for regret but as opportunities to exploit.[2]

[1] Nikolay Mikhailov, "Russia can preserve the status of great power" [Россия может сохранить статус великой державы], *Independent Military Review* [Независимое военное обозрение] No. 36 (1998).

[2] Jonathan Haslam, *Near and Distant Neighbors: A New History of Soviet Intelligence* (New York: Farrar, Straus and Giroux, 2015), p. 251.

As disparities between Moscow and its rivals became even more apparent in the late 1990s, the use of asymmetric means to exploit the weaknesses of, primarily, an expanding NATO became paramount. As offensive cyber operations attributed to Russian actors, particularly the military, have demonstrated, state-sponsored hackers have very much continued the "art of improvisation" of their Soviet predecessors, exhibited by their use of rival countries' malware for their own espionage and attacks and the inclusion of external partners—or the silent appropriation of their work[3]—into operations.

At the same time, other states' cyber operations and their corresponding doctrinal evolutions, primarily the United States, indelibly affected Russia's adoption of these capabilities.[4] While Russia languished financially and attempted to shore up its diminishing military potential, the experiences of the Persian Gulf War, NATO's intervention in the Balkans, and eventually the invasions and occupations of Iraq and Afghanistan afforded Russian defense officials and experts case studies in modern warfare, including cyber operations. Military campaigns of the 1990s and early 2000s demonstrated to Russian military onlookers the inseparability of the psychological and technical aspects of modern warfare and interstate competition, a notion reinforced by lessons from wars in the Caucasus and the chaos of the "color revolutions" along Russia's periphery. Russian military authors noted successful examples in others' operations, particularly the ability of US intelligence and military services to use the internet to launch remote attacks on communications infrastructure, control information, and disseminate propaganda through technical operations during the Persian Gulf War, NATO's bombing of Yugoslavia, and the Global War on Terror.[5] As cybersecurity researchers revealed more and more details about the Stuxnet cyberattack against Iran's Bushehr nuclear plant, uncovered in

[3] For example, malware used by Russian military intelligence as early as 2009 was directly rooted in criminal malware known as "BlackEnergy," originally created by a hacker—Dmytro Oleksiuk—around 2007. Source: Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, (New York: Doubleday, 2019), pp. 10-16.

[4] US national security scholar Dr. Martin Libicki's August 1995 publication "What is Information Warfare?" is an example of a US publication that influenced Russian counterparts' ruminating on Russia's approach to digital competition. See: Valery Baranov, "An instrument of political compulsion" [Инструмент политического принуждения], *Military-Industrial Courier* [Военно-промышленный курьер] No. 49 (2006); Aleksandr Tiranov, "Expertise. A puppet world" [Экспертиза. Марионеточный мир], *Independent Military Review* [Независимое военное обозрение] No. 033 (2002); A.V. Fedorov and V.N. Tsygichko, "Information challenges of national and international security" [Информационные вызовы национальной и международной безопасности], PIR Center, Aug. 2001, p. 111.

[5] Vladimir Platonov, "Expertise. Cyberspace under the gun of the Pentagon" [Экспертиза. Киберпространство под прицелом Пентагона], *Military-Industrial Courier* [Военно-промышленный курьер] No. 24 (2006); Pavel Shumilo, "Ongoing cyberattack on humanity" [Идет кибератака на человечество], *Army Digest* [Армейский сборник], No. 11 (2006).

2010, Russian military authors noted one of the first observed cases of cyber operations transcending espionage and disruptive attacks to cause physical damage and took note of its meaning for growing international cyber aggression.[6]

Russian military literature at the time also widely discussed weaknesses seen in others' approaches to cyber operations, largely emphasizing the psychological aspect of digital warfare. In 2003, a GRU psychological operations officer claimed that the difficulties US forces in Iraq faced resulted from the US military's overestimation of its "advanced information" technologies and its neglect of the psychological factors affecting the battlefield.[7] Two years later, the same officer (along with a coauthor) noted the "great interest" specialists paid to China's approach to the technical and psychological pillars of "information confrontation," which supplemented modern technology with China's millennia of experience in asymmetric warfare.[8] These early observations would help forge the Russian military's unique approach to digital competition in times of peace and war, "information confrontation" (*informatsionnoe protivoborstvo*), which rests on two equally important and mutually reinforcing pillars—psychological and technical effects.

[6] Vladimir Shcherbakov, "Virtual space, real struggle" [Пространство виртуальное, борьба реальная], *Military-Industrial Courier* [Военно-промышленный курьер] No. 40 (2010); E.N. Belov, A.A. Ponomarev, A.V. Semenov, and V.P. Fedorets, "Information security threats of armed and military technology, completed with electronic components of foreign manufacture" [Угрозы информационной безопасности вооружения и военной специальной техники, укомплектованных электронной компонентной базой иностранного производства], *Military Thought* [Военная мысль] No. 12 (2013); Aleksandr Shapovalov, "The USA's global cyber-domination" [Глобальное кибергосподство США], *Military-Industrial Courier* [Военно-промышленный курьер] No. 44 (2013).

[7] A.G. Starunskiy, "Psychological operations of the US armed forces in a modern stage" [Психологические операции вооруженных сил США на современном этапе], *Military Thought* [Военная мысль] No. 11 (2003); The author, Aleksandr G. Starunskiy, was named in a *New York Times* article from July 2020 that described his role in supporting GRU messages published on several GRU-linked websites. See: Julian E. Barnes and David E. Sanger, "Russian Intelligence Agencies Push Disinformation on Pandemic," *New York Times*, Jul. 28, 2020, https://www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html). Additionally, a recent decision to appoint Starunskiy to the Russian Security Council's Science Council revealed his position as the deputy commander of Military Unit 55111, which—according to Meduza, a Russia-focused investigative outlet—is tied to GRU information operations. See: Denis Dmitriev, Alexey Kovalev, and Lilia Yapparova, "Psy-ops in high places Putin's new science adviser to Russia's National Security Council is a military intelligence agent accused of spreading disinformation about the coronavirus," Meduza, May 17, 2021, https://meduza.io/en/feature/2021/05/17/psy-ops-in-high-places.

[8] A. Avramenko and A. Starunskiy, "General military problems. Psychological operations of China's People's Liberation Army" [Общие военные проблемы. Психологические операции народно-освободительной армии Китая], *Foreign Military Review* [Зарубежное военное обозрение] No. 4 (2005).

# Terminology: Information Warfare or Confrontation?

The cyber lexicon is not entirely new to Russia's military. Discussion about "cybernetics" and its application to the Soviet military date back at least to the mid-1960s, though this had almost nothing to do with penetrating adversarial networks and much more to do with improving command-and-control of Soviet forces.[9] As early as 1992, the Russian military's journal *Red Star* warned of impending "information confrontation" between Russia and Ukraine due to the latter's decision to refuse *Red Star* correspondents preferential treatment.[10] Between roughly the mid-1990s and the mid-2000s, Russian military literature experienced a proliferation in terms used to describe computer network operations, mostly those seemingly employed by other countries. Terms like *cyberwar* (*kibervoyna*), *cyber weapons* (*kiberoruzhie*), and *cyber terrorism* were used to varying extents by experts studying rapid advances in computing technology. But these references gradually became less prominent in the literature as Russia refined its own methods and means of waging digital battles and as defense officials and experts increasingly referred to these activities mostly as *information warfare* or *confrontation*. *Information struggle* (*informatsionnaya bor'ba*) also appears in military literature during the same timeframe and generally refers to the same operations and capabilities, but eventually became less prominent in Russian military literature starting in the early 2010s.[11]

Since roughly the early 2000s, descriptions of Russian cyber capabilities and strategy largely revolve around two terms: *information confrontation* and *information warfare* (*informatsionnaya voyna*). Russian military literature very often uses these terms interchangeably, creating an ambiguity that even Russian experts close to these issues recognize and frequently seek to correct. As a 2019 article published by the Russian Academy of Military Sciences claimed, "almost every author" maintained a separate definition for *information warfare* and *confrontation*, adding that *information warfare* should be excluded

[9] V. Rozhdestvenskiy, "Cybernetics in military affairs" [Кибернетика в военном деле], *Military Thought* [Военная мысль] No. 2 (1964).

[10] "Who needs a confrontation?" [Кому нужна конфронтация?], *Red Star* [Красная звезда] No. 136-7 (1992).

[11] There are, of course, exceptions: Konstantin Sivkov, a leading figure in the Russian Academy of Rocket and Artillery Sciences (RARAN), authored a 2018 article in *Military-Industrial Courier* titled "The Fourth Dimension of War," which made wide use of the term "information struggle" alongside confrontation and warfare. See: Konstantin Sivkov, "The fourth dimension of war" [Четвертое измерение войны], *Military-Industrial Courier* [Военно-промышленный курьер] No. 39 (2018).

from official documents, since the term *warfare* connotes armed conflict, which is absent in the kind of peacetime digital competition that Russian military authors usually reference.[12] As some Western experts have observed, there is no real distinction between concepts like "cyberwar" and "information war," which indivisibly blend the physical and psychological aspects of modern interstate competition through information technology.[13]

- *Information confrontation* – The Russian military's encyclopedia defines *information confrontation* as "an integral part of the relations and form of conflict between sides (government, societal-political, movements and organizations, armed forces and others), each of which strives to inflict defeat (destruction) through information."[14] According to this definition, defeat in the "information realm" is inflicted through "information weapons," including electronic warfare assets and "electronic-software" effects. Non-military authorities on information confrontation have defined it as a "contest of social systems" in which one side achieves predominance over the other and the main purpose of which is to "provide information-psychological security" to the state.[15] These experts add that information confrontation serves as an "asymmetric answer" to the "external influence of stronger subjects."
- *Information warfare* – According to the military encyclopedia, *information warfare* is the "open and sharp collision" between states that exploits one another's "information realms," which mainly consist of telecommunications networks, to "destabilize society and the government."[16] Nevertheless, leading non-military experts define information warfare as an open *and* covert struggle among competing information systems to achieve a determined victory in the "material realm."[17] Notably, Russian Minister of

[12] V.F. Lata, V.A. Annenkov, and V.F. Moiseev, "Information confrontation: a system of terms and definitions" [Информационное противоборство: система терминов и определений], *Bulletin of the Academy of military science*s [Вестник Академии военных наук] No. 2 (2019).

[13] Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, (New York: Doubleday, 2019), p. 241.

[14] "Information confrontation" [Информационное противоборство], *Encyclopedia of the Ministry of Defense of the Russian Federation*, undated, https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5221@morfDictionary.

[15] V.B. Veprintsev, A.V. Manoilo, A.I. Petrenko, and D.B. Frolov, *Operations of Information-Psychological Warfare* [Операции информационно-психологической войны], (Moscow: Goryachaya liniya, 2019), pp. 318-319.

[16] "Information warfare" [Информационная война], *Encyclopedia of the Ministry of Defense of the Russian Federation*, undated, https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5211@morfDictionary.

[17] V.B. Veprintsev, A.V. Manoilo, A.I. Petrenko, and D.B. Frolov, *Operations of Information-Psychological Warfare* [Операции информационно-психологической войны], (Moscow: Goryachaya liniya, 2019), p. 68.

> Defense Sergey Shoygu has characterized supposed Western efforts to undermine Russia through information technology as “information warfare,” often when describing the Russian military’s growing potential to respond.[18]

Russian military officials and experts also frequently use the term *information security* (*informatsionnaya bezopasnost’*) when discussing cyber operations, though mostly in a defensive or diplomatic context. For example, Russia’s 2016 Information Security Doctrine attempted to lay out a whole-of-government approach to protecting Russia against perceived threats in the “information realm” (*informatsionnaya sfera*), which included other states’ exploitation of “information infrastructure” to conduct espionage or launch cyberattacks.[19] In 2011, Russia’s Ministry of Defense released its conceptual framework on military activities in the “information space,” which defined information security as the “defensibility of information resources of the armed forces from the effects of information weapons.”[20] Russia participates in several multilateral organizations that aim to establish an “information security” framework regulating states’ activities on each other’s networks, including the Shanghai Cooperation Organization.[21]

The term seemingly used most often to refer to Russian forces and means involved in digital operations is *information confrontation*, which this paper will use to broadly define the computer network operations, psychological operations, electronic warfare, and signals intelligence capabilities that constitute this form of digital competition. The experts and officials closest to these issues and forces generally use *information confrontation* to describe them. Russia’s 2014 military doctrine called for the development of means of “information

[18] Mikhail Korostikov, “Sergey Lavrov and Sergey Shoygu presented Russia’s claims to the West” [Сергей Лавров и Сергей Шойгу предъявили Западу претензии России], Kommersant, Apr. 27, 2016, https://www.kommersant.ru/doc/2974569; “Shoygu called out the purpose of the West’s information war against Russia” [Шойгу азвал цель информационной войны Запада против России], TASS, Jun. 26, 2019, https://tass.ru/armiya-i-opk/6596144?utm_source=twitter.com&utm_medium=social&utm_campaign=smm_social_share.

[19] “Information Security Doctrine of the Russian Federation” [Доктрина информационной безопасности Российской Федерации], *Rossiyskaya gazeta*, Dec. 5, 2016, https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html.

[20] “Conceptual views on activities of the armed forces of the Russian Federation in the information space” [Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве], *Ministry of Defense of the Russian Federation*, 2011, http://www.pircenter.org/media/content/files/9/13480921870.pdf.

[21] A.E. Belyantsev, A.V. Lymar, and A.N. Kazachenko, “Information security as the chief factor of the state information policy of the Russian Federation” [Информационная безопасность как важнейший фактор государственной информационной политики Российской Федерации], *Bulletin of the Academy of Military Sciences* [Вестник Академии военных наук] No. 3 (2015).

confrontation" to address perceived challenges to national security, while—two years later—Chief of the General Staff Valery Gerasimov announced that the military successfully incorporated "information confrontation" into a strategic military exercise for the first time. [22] The GRU has similarly adopted *information confrontation* to refer to its computer network and psychological operations that constitute the bulk of Russia's approach to digital competition. The GRU's psychological operations forces, for instance, classify their work as a "component of information confrontation," the purpose of which is "forming and stimulating opinions, views, emotions, and behavior" that correspond to Russia's national security interests.[23] Vyacheslav Kondrashov, a former general in the GRU and professor of history, labelled operations in "cyberspace" (*kiberprostranstvo*) as an indispensable component of modern information confrontation and a key threat to Russia's national security that demanded "appropriate countermeasures" in an article he wrote a few weeks after a GRU online cutout, "Guccifer 2.0," delivered thousands of emails to Wikileaks for publication ahead of the US Democratic National Convention.[24]

Information confrontation is bifurcated into respective technical (*informatsionno-tekhnicheskiy*) and psychological (*informatsionno-psikhologicheskiy*) components. The former consists of operations like cyber espionage and attacks, electronic warfare at the tactical and operational levels, and—under more liberal interpretations—kinetic strikes against enemy "information resources," such as command-and-control systems. The latter consists of activities historically associated with psychological warfare, such as battlefield leaflet dissemination, though Russian experts certainly see technological breakthroughs as providing an unprecedented level of reach for these operations, like submitting pseudonymous articles intended to influence Western audiences to websites and social media platforms. The technical and psychological aspects of information confrontation do not necessarily garner the same level of attention from Russian decision-makers or experts. According to Oscar Jonsson, author of the 2019 book *The Russian Understanding of War*, cyberwarfare is seen "to have the potential

[22] "Military Doctrine of the Russian Federation" [Военная доктрина Российской федерации], *Rossiyskaya gazeta*, Dec. 30, 2014, https://rg.ru/2014/12/30/doktrina-dok.html; "'Information confrontation' was worked out for the first time at the 'Kavkaz-2016' exercises" [На учениях "Кавказ-2016" впервые отработали "информационное противоборство"], *RIA Novosti*, Sept. 14, 2016, https://ria.ru/20160914/1476902330.html.

[23] Michael Weiss, "Aquarium Leaks: Inside the GRU's Psychological Warfare Program," Free Russia Foundation, 2020, p. 63, https://www.4freerussia.org/aquarium-leaks-inside-the-gru-s-psychological-warfare-program/.

[24] Vyacheslav Viktorovich Kondrashov, "Information confrontation in the cybernetic space" [Информационное противоборство в кибернетическом пространстве], Scientific-Research Center for National Security Problems [Научно-исследовательский центр проблем национальной безопасности], Aug. 22, 2016, http://nic-pnb.ru/analytics/informatsionnoe-protivoborstvo-v-kiberneticheskom-prostranstve/.

for large-scale destruction," but Russian experts do not see it as significant enough to change "the nature of war." Jonsson adds the following:

> The fundamental novelty in the understanding of the nature of war is, rather, information-psychological warfare. As the information arena is key for domestic and international power, information-psychological warfare is seen to be so effective that it can alter the consciousness of a county, eroding its trust in public institutions and state policy to the degree that the citizens are prepared to revolt, creating color revolutions.[25]

[25] Oscar Jonsson, *The Russian Understanding of War: Blurring the Lines between War and Peace*, (Washington: Georgetown Press, 2019), pp. 120-122.

# Organizational Structure of Cyber Forces

As of 2021, virtually every Russian security organization has some sort of "cyber" capacity, though many are focused on defending Russia's internet from foreign subversion. Even the Federal Protective Service (FSO), popularly conceived as Putin's "praetorian guard," has a cyber-relevant component, including a mandate to surreptitiously monitor other ministries and agencies involved in national security.[26] Russia's Foreign Intelligence Service (SVR) directs Advanced Persistent Threat (APT) 29, a shadowy group of skilled hackers who seemingly focus on illicitly obtaining information through espionage while avoiding disruptive operations.[27] For its part, Russia's Federal Security Service (FSB) almost certainly has several components dedicated to offensive cyber operations, including Centers 16 and 18. Center 16 (known by different monikers across the cybersecurity industry), a direct descendant of the Soviet-era KGB's 16th Directorate,[28] is allegedly the most skilled of Russia's "hacking teams," according to the *Washington Post*. In 2020, Center 16 targeted dozens of state and local networks in the US.[29] Center 18, or the Center for Information Security (*Tsentr informatsionnoy bezopasnosty*), maintains a small cadre of official FSB officers and is known to expand its ranks by incorporating cybercriminals into its work. Center 18 even has the authority to bail out hackers

[26] Mark Galleotti, "In Moscow's Shadows 21: The Federal Protection Service (FSO) and Russian security politics; and Three Stories About the Opposition," *In Moscow's Shadows* (podcast), Jan. 11, 2021, https://www.buzzsprout.com/1026985/7237975-in-moscow-s-shadows-21-the-federal-protection-service-fso-and-russian-security-politics-and-three-stories-about-the-opposition.

[27] John Leyden, "Who is behind APT29? What we know about this nation-state cybercrime group," *The Daily Swig*, Jul. 24, 2020, https://portswigger.net/daily-swig/who-is-behind-apt29-what-we-know-about-this-nation-state-cybercrime-group; US Department of the Treasury, "Treasury Sanctions Russia with Sweeping New Sanctions Authority," Press Releases, Apr. 15, 2021, https://home.treasury.gov/news/press-releases/jy0127.

[28] The KGB's 16th Directorate was established in 1973 by KGB order No. 0056, which split signals interception from other duties as part of an assessed exigent need by the Soviets to establish cryptographic parity with the West. See: Jonathan Haslam, *Near and Distant Neighbors: A New History of Soviet Intelligence* (New York: Farrar, Straus and Giroux, 2015), p. 242.

[29] Ellen Nakashima, Shane Harris, and Devlin Barrett, "Russia remains more potent threat of election interference despite administration focus on Iran," *Washington Post*, Oct. 22, 2020, https://www.washingtonpost.com/national-security/iran-russia-election-interference/2020/10/22/e3c2fc1a-1496-11eb-ad6f-36c93e6e94fb_story.html.

detained by Russia's internal security services, according to an anonymous source in 2019, with the simple explanation "this isn't your business" (*ne vashe delo*).[30]

No other service or agency, however, has exhibited the same kind of aggression or the broad repertoire in digital activity as has the GRU, at least in terms of observed activity and attributed operations.[31] Reports published by Western governments, investigative journalists, and the cybersecurity industry have illustrated the GRU's role in waging information confrontation against Russia's perceived adversaries. The GRU relies on different formations to wage its furtive digital campaigns, such as Unit 54777, responsible for psychological operations, and Units 74455 and 26165, which—as revealed by the Mueller investigation—concentrate on cyberattacks, espionage, and support to online influence operations. The Information Operations Troops (*Voyska informatsionnykh operatsiy*; VIO), first publicly mentioned in 2014, seek to integrate and synthesize these activities, judging from Russian officials' statements. As described in US sanctions imposed against Russian malign influence actors in mid-April 2021, the VIO oversees Unit 54777 and is responsible for "cyber espionage, influence, and offensive cyber operations."[32] While most of these units are based in Moscow, the GRU also manages a nationwide network of regional psychological operations and signals intelligence units that support information confrontation.

## Historical overview

Following the collapse of the Soviet Union, the GRU possessed the forces and means that naturally led to its position in Russia's vanguard in waging digital war. In 1991, the GRU inherited the "special propaganda" department of the Soviet military's main political directorate, officially responsible for conducting psychological warfare since 1940.[33] Russian military intelligence has an even longer association with the technical aspects of information confrontation, including the use of "new" technology in waging early campaigns designed to disinform enemies or affect their communications. After the Red Army captured Fort

[30] Daniil Turovskiy, *Invasion: a short history of Russian hackers* [Вторжение: краткая история русских хакеров], (Moscow: Inviduum, 2019), p. 149.

[31] Technically, Russian military intelligence's proper title is the Main Directorate of the General Staff of the Ministry of Defense of the Russian Federation (ГУ ГШ МО РФ). Nonetheless, this paper uses the far more familiar acronym, GRU, to refer to Russian military intelligence.

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

[33] "A special front" [Особый фронт], *Arguments of time* [Аргументы времены], Oct. 1, 2018, https://svgbdvr.ru/voina/osobyi-front.

Aleksandrovskiy on the Caspian Sea from the Whites in 1919, for instance, specialists used captured radio equipment to pose as the latter and receive their uninterrupted intelligence updates, all while issuing disinformation that led to ambushes and capture.[34]

The ever-increasing intelligence requirements of the Cold War necessitated increasingly sophisticated signals intelligence capabilities. In 1954, signals intelligence forces within the Soviet military were transferred to the GRU's Second Department, dividing some of these specialists into "Separate Special Surveillance" (OSNAZ) units.[35] The GRU's 6th Directorate was established the following year to better organize these units. Aside from controlling a growing network of "radio intercept" and "electronic intelligence" units on Soviet territory, the 6th Directorate also gained intelligence from international centers based in Cuba, Vietnam, Burma, China, and Mongolia.[36] Between 1963 and 1987, the GRU's signals intelligence apparatus grew into new fields for intelligence gathering, including air and space programs, largely because of Ivan Ivashutin—the head of the GRU at the time—and his interest in expanding technical capabilities.[37]

## Unit 26165, the Main Special Service Center

To further expand its signals intelligence capacity, the GRU stood up the 85th Main Special Service Center (*Glavniy tsentr spetsial'noy sluzhby,* GTsSS), or Unit 26165, the same unit implicated in modern GRU information confrontation efforts that range from cyber espionage to election influence.[38] The 85th suffered reductions in the immediate post-Soviet period, but

[34] D.A. Larin, *Russia's Cryptographic Service: Studies of History* [Криптографическая служба России: очерки истории], (Moscow: Helios ARV, 2017), p. 26.

[35] Vadim Viktorovich Grebennikov, *Radio-intellligence of Russia. Intercepting Information* [Радиоразведка России. Перехват информации], (Moscow: Ridero, 2019), p. 74.

[36] Aleksandr Shevyakin, *The KGB: Security System of the Soviet Union* [КГБ: система безопасности СССР], (Moscow: Algoritm, 2014), p. 103

[37] Vadim Viktorovich Grebennikov, *Radio-intellligence of Russia. Intercepting Information* [Радиоразведка России. Перехват информации], (Moscow: Ridero, 2019), p. 82.

[38] Shortly after its inception, the 85th used the Soviet Union's most powerful computer at the time, the "Bulat," named after a famous performer—Bulat Okudzhava—and developed by the predecessor to Kvant, a state research institution sanctioned by the US in 2018 for its "material and technological" support to Russia's FSB. See: Jonathan Haslam, *Near and Distant Neighbors: A New History of Soviet Intelligence* (New York: Farrar, Straus and Giroux, 2015), p. 244; Aleksandr Shevyakin, *The KGB: Security System of the Soviet Union* [КГБ: система безопасности СССР], (Moscow: Algoritm, 2014), p. 103.

continued its main mission to decrypt communications.[39] Many prominent GRU officers involved in computer network operations likely passed through the 85th's ranks or worked closely with the unit. Perhaps most important among them is Sergey Gizunov, who led the 85th prior to his ascension to GRU central leadership and after he became a "scientific laureate" of Russia for science and technological research in 2009.[40] According to a 2018 *Washington Post* article, the 85th, alongside the FSB, sought to recruit from Russian high schools, in part by promoting "cadet classes" that focused on math and computer skills.[41] Judging by its attributed operations, the unit has a broad mandate, but concentrates on cyber espionage. In 2018, one of the unit's officers used fake personas to pose as UK journalists to gain information about the investigation into the poisoning of former Russian spy Sergei Skripal.[42] The unit has a clear and consistent interest in going after European political targets, including national legislatures, possibly for intelligence or subsequent influence operations.[43] Between late 2019 and late 2020, the unit targeted over 200 organizations affiliated with the US Democratic and Republican parties, likely in an attempt to support election influence activities similar to the unit's work in 2016.[44]

[39] Irek Murtazin, "Military unit No. 26165 again" [Опять войсковая часть № 26165], *Novaya gazeta*, May 30, 2020, https://novayagazeta.ru/articles/2020/05/30/85620-opyat-voyskovaya-chast-26165.

[40] "Intelligence among their own" [Разведка среди своих], *Kommersant*, Jan. 12, 2016, https://www.kommersant.ru/doc/2890274.

[41] Anton Troianovski and Ellen Nakashima, "How Russia's military intelligence agency became the covert muscle in Putin's duels with the West," *Washington Post*, Dec. 28, 2018, https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html.

[42] Robert Mendick, "Novichok hacker is US poll suspect," *Yahoo News*, Dec. 5, 2020, https://www.yahoo.com/news/russian-spy-imitated-telegraph-journalists-163033385.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAHDysKyoei0M6vfy7dsFjo3GeW5yeqxWv1b52oSkK8RLNzghI0gQmTzMLymytJOPihYeJWIn89EXD7hY5rcUxsG9gwxLe4pIdzla0WEdqZ3px0hkWJk1tZbPOELSc4eOG5kRVlPiQo5fnM0QepMkV9grfrrR8XGQY0CdyAkbpadn.

[43] "Norway accuses Russian hackers of parliament attack." *France 24*, Aug. 12, 2020, https://www.france24.com/en/live-news/20201208-norway-accuses-russian-hackers-of-parliament-attack; Bill Toulas, "Russian Hackers Had Managed to Access Angela Merkel's Emails," *TechNadu*, May 9, 2020, https://www.technadu.com/russian-hackers-access-angela-merkel-emails/101468/.

[44] Andy Greenberg, "Russia's Fancy Bear Hackers Are Hitting US Campaign Targets Again," *WIRED*, Oct. 9, 2020, https://www.wired.com/story/russias-fancy-bear-hackers-are-hitting-us-campaign-targets-again/.

# Unit 11135, the 18th Central Scientific Research Institute

Research and development of cyber capabilities within the GRU rests on both old and newer institutions. Among the older is the 18th Central Scientific Research Institute (*Tsentral'niy nauchno-issledovatel'skiy institut,* TsNII), or Unit 11135, which was established in 1938 and historically worked on "radio reconnaissance," satellite communications, and coding for the GRU's Operational-Technical Directorate.[45] According to Meduza, a Russia-focused investigative journalism agency, there is no public information about the 18th TsNII; Russians joke online that the unit's basement holds a UFO that crash landed in Moscow in 1959.[46] The 18th likely expanded into computer network operations research as early as the 1990s, judging from a conference hosted by the unit and its interest in a 2004 dissertation on the "research and development of mathematical and software tools for effective parallelization of applied problems on high-performance computing systems."[47] Dr. Ilya Levin, the deputy director of the computing institute at Russia's Southern Federal University, published three articles for the unit in the mid-2000s, the titles of which were redacted in a list of Levin's work from 2017.[48] As of 2013, the 18th concentrated on "secret communications systems" and coding for long-distance and satellite "radio-reconnaissance." A 2017 corruption case involving the unit

[45] Valentin Mzareulov, "The 18th TsNII" [18-й ЦНИИ], *Shield and Sword*, undated, http://shieldandsword.mozohin.ru/mi/gru4992/nii/18.htm; Images and commemorative memorabilia surrounding the 18th TsNII date the unit to 1938 and demonstrate an emblematic connection to signals intelligence.

[46] Daniil Turovskiy, "The GRU – what is it? Whom do they take as spies? And why are they revealed so often?" [ГРУ — это вообще что? Кого берут в шпионы? И почему их так часто раскрывают?], Meduza, Oct. 15, 2018, https://meduza.io/feature/2018/10/15/gru-eto-voobsche-chto-kogo-berut-v-shpiony-i-pochemu-ih-tak-chasto-raskryvayut.

[47] S. A. Vyalykh, "Raising the effectiveness of automated operational control system defence from the impact of malicious software" [Повышение эффективности защиты автоматизированных систем оперативного управления от вредоносных программных воздействий], 5th Central Scientific Research Test Institute (dissertation), 1999; I.I. Levin, "Methods and software and hardware for parallel structural-procedural computations" [Методы и програмнно-аппаратные средства параллелных структурно-процедурных вычисленний], Taganrog State Radio-Technical University (dissertation), 2004.

[48] "List of scientific works of the deputy director of the Scientific-research institute of multiprocessor computing systems A.V. Kalyaev of Southern federal university Doctor of sciences Il'ya Izrailevich Levin, published between 1985 and 2017" [Список научных трудов заместителя директора Научно-исследовательского института многопроцессорных вычислительных систем имени академика А.В. Каляева Южного федерального университета доктора технических наук Левина Ильи Израилевича, изданных в 1985 - 2017 годах], Southern Federal University, 2017, https://sfedu.ru/files/upload/per/15873 Список%20научных%20трудов_Левин_02.2017.pdf.

revealed its development of "radio electronic special technology" for the GRU, according to Russian press.[49]

## Unit 74455, the Main Center for Special Technologies

Not all of the GRU's cyber formations have deep historical roots. The GRU's Center for Special Technologies (*Glavniy tsentr spetsial'noy tekhnologiy,* GTsST), or Unit 74455, has not only accompanied the 85th in notable cyber operations, but launched the costliest cyberattack in history with the "NotPetya" wiperware of 2017 that temporarily disabled a large swath of global shipping. The GTsST has no apparent predecessor and is most likely the product of Russian military efforts to develop an offensive cyber capability within the military in the late 2000s. One of the earliest mentions of the GTsST comes from official military documents from 2010 examining the possibility of transferring an officer from the strategic rocket forces to the GTsST.[50] A 2012 document details specialist pay for the GTsST and another highly secretive GRU unit, Unit 29155, which—per recent disclosures—has been implicated in sabotage and assassination operations in Europe between 2014 and 2018.[51] In 2012, then-Deputy Prime Minister Dmitriy Rogozin announced to a group of military scientists that Russian officials discussed establishing a "cyber command" (*kiberkomandovanie*) that would provide "information security" for the army and state infrastructure, though whether this was a reference to the GTsST remains unclear.[52]

[49] German Petelin and Vladimir Barinov, "Military intelligence demands a 30-million-ruble penalty from scientists" [Разведка Минобороны требует от ученых неустойку в 30 млн рублей], *Izvestiya*, Mar. 15, 2013, https://iz.ru/news/546680; "A former coworker of a military research facility was convicted of stealing radio-equipment worth 40 million" [Бывший сотрудник военного НИИ осужден за хищение радиодеталей на 40 миллионов], *Lenta.ru*, Jan. 31, 2017, https://lenta.ru/news/2017/01/31/radiodetali/.

[50] Anna Kovalenko, "The NYT revealed a secret GRU unit for 'destabilizing Europe'" [NYT рассказала о секретном подразделении ГРУ по «дестабилизации Европы»], *The Bell*, Oct. 9, 2019, https://thebell.io/nyt-rasskazala-o-sekretnom-podrazdelenii-gru-po-destabilizatsii-evropy.

[51] Christo Grozev, Pieter van Huis, Yordan Tsalov, The Insider Russia, and Respekt, "How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine," *Bellingcat*, Apr. 26, 2021, https://www.bellingcat.com/news/uk-and-europe/2021/04/26/how-gru-sabotage-and-assassination-operations-in-czechia-and-bulgaria-sought-to-undermine-ukraine/.

[52] "Rogozin described plans to create a cyber command" [Рогозин рассказал о планах создать киберкомандование], *Vedomosti*, Mar. 12, 2012, https://www.vedomosti.ru/technology/news/2012/03/21/rogozin_rasskazal_o_planah_sozdat_kiberkomandovanie.

## The Main Center for Special Developments

A seemingly newer addition to the GRU's network of research institutes is the Center for Special Developments (*Tsentr spetsial'nykh razrobotok*, TsSR), which—according to investigative journalists—as of late 2016 was collocated at the same facility in Moscow as the GTsST's hackers.[53] The unit's official webpage on the Russian Ministry of Defense website describes the purpose of the TsSR as providing for "the security of communications and information systems," with other tasks listed as "the design and construction of high-performance problem-oriented computing systems" and "applied research in the field of microelectronics."[54] The TsSR likely has connections to the GRU's 85th as well; one of the GRU hackers detained as part of a team from the 85th deployed to the Hague to hack into the Organisation for the Prohibition of Chemical Weapons, Evgeniy Serebryakov, previously worked in the TsSR. Serebryakov also listed the TsSR as his place of employment when he wrote a 2014 article in *Applied Discrete Mathematics*. Moreover, Georgiy Roshka, a hacker with the 85th who took part in the GRU's 2017 effort to affect the French presidential elections through hack-and-leak operations, traveled in 2014 with a specialist from the TsSR, Sergey Zaitsev, to an IT-conference in Rostov-on-Don.[55] While as of late May 2021, the TsSR had no listed vacancies on Habr.ru, a popular Russian site for IT specialists, 26 specialists listed the TsSR as their place of employment, including two graduates of the A.F. Mozhaiskiy Military Engineering-Space Academy, with specialties ranging from IT recruiting to backend development.[56]

[53] Sergey Dobrynin and Mark Krutov, "'The Center for Special Developments'. How the Russians expelled from the Netherlands are tied to the GRU" ["Центр специальных разработок". Как высланные из Голландии россияне связаны с ГРУ] *Radio Svoboda*, Oct. 4, 2018, https://www.svoboda.org/a/29525612.html.

[54] "The Center for Special Developments of the Ministry of Defense of the Russian Federation" [Центр специальных разработок Министерства обороны Российской Федерации], Ministry of Defense of the Russian Federation, undated, https://ens.mil.ru/science/SRI/information.htm?id=11739@morfOrgScience.

[55] Roman Dobrokhotov, "Roshka and Myshka. GRU associates broke into the French president's mail" [Рошка и мышка. Почту президента Франции взломали сотрудники ГРУ], *The Insider*, Jun. 1, 2017, https://theins.ru/politika/58803; "A new connection between the hacker who hacked Macron and the Ministry of Defense has been discovered. In 'Erika', everyone denies it" [Обнаружена новая связь взломавшего Макрона хакера с Минобороны. В "Эврике" все отрицают], *The Insider*, May 12, 2017, https://theins.ru/news/55749.

[56] Search for "ЦСР МО РФ" on habr.ru, May 26, 2021.

## The GRU's Military Science Unit, ERA Technopolis

Probably to help recruit specialists for its increasingly important cyber units, in 2013, the GRU established a "military science unit" (*voennaya nauchnaya rota*) as part of Defense Minister Sergey Shoygu's "big hunt" for "young programmers" inaugurated that year to help military modernization.[57] These units would offer special accommodations to graduates of technical programs in Russian universities who are subject to mandatory military service, but would conduct research related to their fields as opposed to serving in less cerebral, more spartan roles, like in combat arms. The GRU manages the 4th Military Science Unit (MSU), one of four original MSUs established in 2013, though their number has grown to 16. Based in the northeast suburbs of Moscow,[58] the 4th MSU very likely concentrates on cyber research; the unit held an exhibit in 2015 at the Ministry of Defense's "Innovation Day" that revealed the unit's foci as the development of "special software" and the "software implementation of special mathematical algorithms."[59] Beyond its MSU, the GRU almost certainly can pull from other military services to fulfill its cyber staffing needs. Photos of some of the GRU hackers indicted by the United States in 2018, for instance, include insignias on their uniforms from the aerospace defense forces, the navy, the air force, and the signals branch.[60] As of 2016, the head of a division under the GTsST was a member of the "Special IT" faculty at A.F. Mozhaisky Academy.[61]

[57] Sergey Popsulin, "Sergey Shoygu announced a 'big hunt' for young programmers" [Сергей Шойгу объявил о «большой охоте» на молодых программистов], *Cnews.ru*, Jul. 4, 2013, https://www.cnews.ru/news/top/sergej_shojgu_obyavil_o_bolshoj_ohote.

[58] "Science companies" [Nauchnye roty], Faculty of Machine Construction Technology, N.E. Bauman Moscow State Technical University, undated, http://mt.bmstu.ru/2019.12.25.php.

[59] Bmpd, "Innovation day of Russia's Ministry of Defense" [День инноваций Министерства обороны России], *LiveJournal* (blog), Oct. 6, 2015, https://bmpd.livejournal.com/1505576.html.

[60] "Aleksey Aleksandrovich Potemkin," US Federal Bureau of Investigation, undated, https://www.fbi.gov/wanted/cyber/aleksey-aleksandrovich-potemkin; "Nikolay Yuryevich Kozachek," US Federal Bureau of Investigation, undated, https://www.fbi.gov/wanted/cyber/nikolay-yuryevich-kozachek; "Artem Andreyevich Malyshev," US Federal Bureau of Investigation, undated, https://www.fbi.gov/wanted/cyber/artem-andreyevich-malyshev.

[61] Peter Mironenko and Anastasia Yakoreva, "Cryptographers from military units: what we know about the accused Russian hackers," *The Bell*, Jul. 14, 2018, https://thebell.io/en/cryptographers-from-military-units-what-we-know-about-the-accused-russian-hackers/.

Russia’s Ministry of Defense nonetheless has other institutions that conduct research and development related to cyber and digital influence capabilities. As early as 2009, former President Dmitriy Medvedev directed the Ministry of Defense to establish an “information confrontation center,” which would boost the “information-propagandistic” potential of Russia’s military.[62] The center’s exact role was unclear, but it was allegedly sparked by the Russian military’s supposed inability to explain to Belarusian farmers that a large-scale joint exercise that year, Zapad 2009, would not harm their crops.[63] Unverified sources point to “information confrontation centers” in Russia’s southern military district that conduct psychological operations against Ukraine, though their relationship to the Medvedev-era initiative is unclear.[64] More recently, the Ministry of Defense has established the “Elite of the Russian Army” (ERA) Technopolis in Anapa, along the Black Sea coast. As of its inception in 2017, the ERA Technopolis planned to host 18 laboratories and a staff of 2,000 scientists, who would focus on four research areas: IT and automated control systems; information security; robotics; and energy, technology, and life support machines.[65] In early 2021, the Ministry of Defense announced that three MSUs had been transferred to ERA Technopolis, which would support several defense organizations, including the Ministry of Defense IT Department.[66] US sanctions against Russian cyber actors in April 2021 stated that the ERA Technopolis “houses and supports” GRU units responsible for offensive cyber operations and uses “the personnel and expertise” of Russia’s IT sector for military and dual-use technology.[67]

[62] “An information confrontation center will be established in the defense ministry” [В Минобороны будет создан центр информационного противоборства], *Oruzhie rossii*, Oct. 8, 2009, https://www.arms-expo.ru/news/archive/v-minoborony-budet-sozdan-centr-informacionnogo-protivoborstva08-10-2009-09-38-00/.

[63] The Russian military’s difficulties in conducting strategic messaging during the war with Georgia a year prior very likely provided more significant motivation for this initiative.

[64] Armia_spasenia, “Our young ‘psychos’” [Наши южные “психи”], *LiveJournal* (blog), Jul. 29, 2020, https://armia-spasenia.livejournal.com/13865.html; Vladimir84, “Information about Russian ‘psycho’ forces became known” [Стали известны данные о войсках «психов» России.], *Tribun*, Feb. 6, 2018, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiV6NmFiP7vAhXNGs0KHSH0CcgQFjAJegQIChAD&url=https%3A%2F%2Ftribun.com.ua%2F47273&usg=AOvVaw0gtlV5apHT9JDxq2jybqgY.

[65] Aleksandr Golts, “Russian Scientists in Military Uniforms,” The Jamestown Foundation, Jul. 19, 2018, https://jamestown.org/program/russian-scientists-in-military-uniforms/.

[66] “Three scientific companies arrive in Era technopolis in Anapa,” TASS, Jan. 19, 2021, https://tass.com/science/1246691.

[67] US Department of the Treasury, “Treasury Sanctions Russia with Sweeping New Sanctions Authority,” Press Releases, Apr. 15, 2021, https://home.treasury.gov/news/press-releases/jy0127.

## The Information Operations Troops

In 2014, a year after Shoygu announced a "big hunt" for military programmers to staff MSUs, the General Staff inaugurated the "Information Operations Troops" (*Voyska informatsionnykh operatsiy*; VIO), which would control units responsible for defending against cyberattacks and "hacker exploits," incorporating lessons observed from past NATO activities that allowed Russia's military to avoid some (unspecified) mistakes and economize resources.[68] Observers presumed the VIO would incorporate special engineers, cryptographers, translators, OSNAZ officers, and electronic warfare specialists.[69] Three years later, Minister of Defense Sergey Shoygu revealed the operational status of the VIO to Russia's national legislature, saying that it would be "more powerful and effective" than the Soviet military's psychological warfare department in addressing the "information-psychological" attacks from the West.[70] While the 2014 discussion of the VIO apparently focused more on technical capabilities and countering cyberattacks, Shoygu's 2017 presentation to the Duma seemingly concentrated on the psychological aspect of the VIO's mandate. The VIO likely has both technical and psychological operations roles, and the VIO's creation probably represents the most significant organizational change related to Russian military cyber capabilities since the collapse of the Soviet Union. According to recent US sanctions, the VIO conducts cyber espionage, influence, and offensive cyber operations, and the 72nd Main Intelligence and Information Center (GRITs; Unit 54777) is a component of the VIO.[71] An August 2020 article published in *Atomic Strategy XXI* about "raising the innovative potential" of Russia's State Atomic Energy Corporation (Rosatom) involving "foreign intelligence and the defense of state secrets" claimed that the creation of the VIO offered "new possibilities" for Rosatom, which traditionally works with Russian intelligence services—including the GRU—on important issues.[72] According to Ukrainian sources, during the early stages of the Ukraine crisis, the VIO was commanded by

[68] Yuriy Gavrilov and Sergey Ptichkin, "Cyborgs won't break through" [Киборги не прорвутся], *Rossiyskaya gazeta*, May 13, 2014, https://rg.ru/2014/05/13/kiber.html.

[69] "Information Operations Troops are being created in the armed forces" [В Вооруженных силах создают войска информационных операций], *Independent Military Review* [Независимое военное обозрение], May 16, 2014, https://nvo.ng.ru/nvo/2014-05-16/2_red.html.

[70] "Shoygu described the tasks of the Information Operations Troops" [Шойгу рассказал о задачах войск информационных операций], *Ria.ru*, Feb. 22, 2017, https://ria.ru/20170222/1488617708.html.

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

[72] Yuriy Bobylov, "Specific factors of raising the innovative potential of 'Rosatom': foreign intelligence and defending state secrets" [Особые факторы повышения инновационного потенциала ГК «Росатом»: внешняя разведка и защита гостайн], *Atomic Strategy* [Атомная стратегия], No. 158 (2020).

Major General P.M. Kovoval'chik, who oversaw the unit's "information-psychological operations."[73] As of 2011, Konoval'chik led a GRU OSNAZ unit based near St. Petersburg.[74] A year earlier, Konoval'chik served as the scientific advisor for a dissertation on "formalization and information processing algorithms for expert technical diagnostic systems of hybrid objects."[75] Earlier in his career, Konoval'chik was affiliated with the GRU's 85th TsSS, according to a 2004 article he coauthored in *Artificial Intelligence*.[76]

## General Staff role

While the GRU serves as the "muscle" behind the Russian military's contemporary information confrontation efforts, the military's General Staff very likely functions as the nerve center for the military's cyber operations—particularly at the strategic level—organizing relevant forces and generating the doctrine that guides them. Probably the most obvious form of General Staff control is the direct subordination of the GRU to the former, despite intermittent successes by the GRU to "jump the chain" and communicate directly with senior political leadership. Independent of the GRU, the General Staff's sub-directorate for electronic warfare similarly conducts planning and organization as well as directs technological development relevant to electronic warfare requirements.[77]

[73] Aleksandr Kovalenko, "Who conducts information warfare against Ukraine or about the secret of unit 76836" [Кто курирует информационной войной против Украины или про секреты В\Ч 76836], *Odessa Courier* [Одесский Курьер], Nov. 27, 2020, https://uc.od.ua/columns/1533/1231160.

[74] "Military unit 61913" [Войсковая Часть 61913], *Rusprofile*, undated, https://www.rusprofile.ru/id/7130884; Osnaz_cikle, "Military unit 61913 – a military town" [В/ч 61913 - военный городок], *LiveJournal* (blog), Dec. 8, 2012, https://osnaz-cikle.livejournal.com/36111.html. https://www.rusprofile.ru/id/7130884.

[75] Aleksandr Yur'evich Romanenko, "Formalization and information processing algorithms for expert technical diagnostic system hybrid objects" [Формализация и алгоритмы обработки информации для экспертной системы технического диагностирования гибридных объектов], *Institute of Engineering Physics* (dissertation) [Институт инженерной физики], 2010, https://iifrf.ru/files/sections/154/avto_romanenko.pdf.

[76] Interestingly, one of Konoval'chik's coauthors for this paper, I.I. Levin, also authored a dissertation in 2004 (mentioned earlier) that was of interest to the GRU's 18th TsNII; I.I. Levin, P.M. Konoval'chik, A.I. Ivanov, and A.D. Malevanchuk, "Multiprocessor system, adaptable under the information structure of tasks different classes" [Многопроцессорная система, адаптируемая под информационную структуру задач различных классов], *Artificial Intelligence* [Искусственный интеллект], No. 3 (2004), http://iai.dn.ua/public/JournalAI_2004_3/Razdel2/04_Luvin_Koval'chik_Ivanov.pdf.

[77] "Directorate of the head of the electronic warfare forces of the Armed forces of the Russian Federation" [Управление начальника войск радиоэлектронной борьбы Вооруженных Сил Российской Федерации], Ministry of Defense of the Russian Federation, undated, https://structure.mil.ru/structure/ministry_of_defence/details.htm?id=9713@egOrganization.

Additionally, the General Staff's 8th Directorate, which is responsible for securing the military's networks and protecting classified information, is organizationally independent from other information confrontation forces and bodies.[78] Both the network defenders and electronic warfare forces have their own MSUs: the 7th MSU based at the Military Communications Academy in St. Petersburg is responsible for network security and the 9th MSU, based in Tambov, is responsible for electronic warfare research. The task of corralling these directorates and ensuring their adherence to plans falls on the Chief of the General Staff and his deputies. Nevertheless, US intelligence assessments about Russian influence and interference during the 2016 and 2020 US presidential elections claim President Putin personally approved the broad campaigns that aimed to affect those elections' outcomes, suggesting that strategic information confrontation efforts involving the military require approval by the presidential administration.

Among the General Staff's sub-directorates responsible for planning, coordinating, and organizing information confrontation, the Main Operational Directorate (*Glavnoe operativnoe upravlenie*; GOU) probably plays an important role. The GOU's mandate consists of identifying emerging national security threats, organizing and developing defense planning, liaising with other Russian government security services, and supporting military cooperation within multilateral institutions that are important to Moscow.[79] The GOU's current leader, Colonel-General Sergey Rudskoy, defined the GOU as the military's incubator of ideas, adding in 2018 that its officers were critical to the changing nature of conflict, including "cyberspace."[80] Russian security analyst Aleksandr Golts identified the GOU as one of the Russian military's leading participants in its "perpetual information war" related to the Syria conflict.[81] The transition of former GOU leader Colonel-General Andrey Kartapolov to head of the Russian military's new Main Military-Political Directorate (GVPU), a Soviet-era formation responsible for ensuring morale and ideological adherence, could further indicate the GOU's ties to

[78] "History of the establishment of the service of defending state secrets in the Armed Forces of the Russian Federation" [История создания и развития службы защиты государственной тайны в Вооруженных Силах Российской Федерации], Ministry of Defense of the Russian Federation, Nov. 13, 2018, https://function.mil.ru/news_page/country/more.htm?id=12203742@egNews.

[79] "Main operational directorate of the General staff of the Armed Forces of the Russian Federation" [Главное оперативное управление Генерального штаба Вооруженных Сил Российской Федерации], Ministry of Defense of the Russian Federation, undated, https://structure.mil.ru/structure/ministry_of_defence/details.htm?id=9710@egOrganization.

[80] Sergey Rudskoy, "A generator of ideas and plans" [Генератор идей и замыслов], *Red Star* [Красная звезда], No. 18 (2018).

[81] Aleksandr Golts, "The big war has so far been avoided" [Большой вонйы пока избежали], *New Times* [Новое время], Apr. 16, 2018, https://newtimes.ru/articles/detail/158473/.

information confrontation, though in the case of the GVPU, these activities would be defensive in nature, since the directorate's stated purpose is to improve the morale of Russian forces.

The career of Igor Dylevskiy provides a look into the GOU's potential role in conceptualizing information confrontation. Between 2008 and 2020, Dylevskiy—along with coauthors, some from the General Staff—published 10 articles in the General Staff's leading journal, *Military Thought* (*Voennaya mysl'*), all related to information confrontation. These articles examined the US and Russian approaches to information confrontation, but mostly advocated for strengthening international norms and agreements that would constrain the use of information technology in interstate conflict.[82] Dylevskiy was designated head of the GOU's 5th Directorate in 2010.[83] In 2017, Dylevskiy—by then a Major General—served on an expert panel hosted by the General Staff Academy on "security in the information space and free access to information: a contradictory relationship."[84]

Theater-level information confrontation, like that targeting Ukraine since 2014, has largely been delegated to Russia's military districts. General Gerasimov revealed as much in a military exercise in 2016, when he stated that "information confrontation centers" had been established in the military districts, which worked alongside the General Staff's GOU, electronic

[82] For example, see: S.A. Komov, S.V. Korotkov, and I.N. Dylevskiy, "On the evolution of modern American doctrine of 'information operations'" [Об эволюции современной американской доктрины "информационных операций"], *Military Thought* [Военная мысль], No. 6 (2008); C.I. Bazylev, I.N. Dylevskiy, S.A. Komov, and A.N. Petrunin, "Activity of the Armed Forces of the Russian Federation in the information space: principles, rules, confidence building measures" [Деятельность Вооруженных Сил Российской Федерации в информационном пространстве: принципы, правила, меры доверия], *Military Thought* [Военная мысль], No. 6 (2012); I.N. Dylevskiy, V.O. Zapivakhin, S.A. Komov, S.V. Korotkov, and A.N. Petrunin, "An international regime of information weapons non-proliferation: utopia or reality?" [Международный режим нераспространения информационного оружия: утопия или реальность?], *Military Thought* [Военная мысль], No. 10 (2014).

[83] "Dylevskiy Igor' Nikolaevich - biography" [Дылевский Игорь Николаевич – биография], *VIPerson* [ВИПЕРСОН], Apr. 20, 2021, http://viperson.ru/people/dylevskiy-igor-nikolaevich; "New appointments" [Новые назначения], *Red Star* [Красная звезда], Dec. 14, 2006, available at: http://old.memo.ru/d/63196.html.

[84] "Representatives of the General Staff Academy took part in the Sixth Moscow Conference on international security" [Представители ВАГШ ВС РФ приняли участие в работе VI Москов-ской конференции по международной безопасности], Ministry of Defense of the Russian Federation, May 2, 2017, https://function.mil.ru/news_page/world/more.htm?id=12121426@egNews; Dylevskiy attracted brief attention from Russian press in 2017, when he—after receiving direction from Rudskoy—allegedly provided a fake video of Russian airstrikes in Syria that was eventually showcased by Putin as evidence of Russian military prowess against Islamic extremists and appeared in a documentary by Oliver Stone. See: "RBC: footage of operations in Syria shown to Stone was prepared for Putin at the General Staff" [РБК: показанные Стоуну кадры операции в Сирии для Путина подготовили в Генштабе], *Kommersant*, Jun. 23, 2017, https://www.kommersant.ru/doc/3332425.

warfare units, and the service for protecting state secrets.[85] Planning and coordinating at this level very likely occurs between military district headquarters and the regional psychological warfare and signals intelligence units (*otdely spetsial'nykh naznachenii*; OSNAZ) under the GRU, as well as other formations outside of military intelligence, such as electronic warfare units.[86] The regional networks of psychological and electronic warfare and signals intelligence units are a legacy of the Soviet era, when military districts, armies and fleets, and lower-echelon units maintained operational control over what are now considered forces relevant to information confrontation.

## Locations of relevant GRU units

The Russian military's Moscow-based and regional psychological operations units faced their first significant post-Soviet challenge during the First Chechen War, when the military used psychological operations groups based in all of Russia's military districts.[87] While more information has come to light about the role of Russia's leading psychological warfare unit, Unit 54777, in recent years, less is known about regional formations. According to Ukrainian sources, the 2140th Psychological Operations Group has been particularly active in Ukraine since 2014, conducting internet-based operations, physical leaflet distribution, and face-to-face communication with target audiences.[88] As of the early 2010s, senior GRU psychological operations specialists were attached to service branches, military districts, and fleets through intelligence departments at headquarters, with each military district or fleet having as many as nine specialists, according to a GRU document detailing this hierarchy.[89] The same document revealed that Unit 54777 was the highest echelon for psychological warfare.

*Please see Figure 1 and data in Appendix A for locations.*

[85] "'Information confrontation' was worked out for the first time at the 'Kavkaz-2016' exercises" [На учениях "Кавказ-2016" впервые отработали "информационное противоборство"], *Ria.ru*, Sept. 14, 2016, https://ria.ru/20160914/1476902330.html.

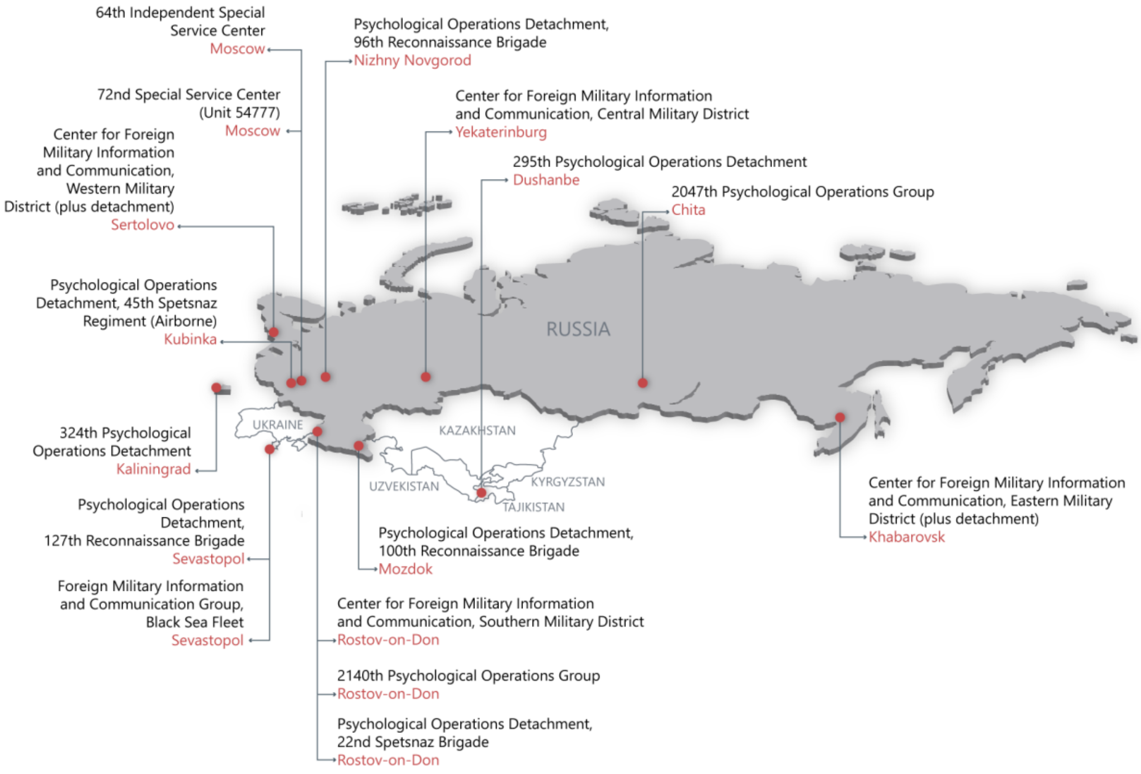
[86] Michael Weiss, "Aquarium Leaks: Inside the GRU's Psychological Warfare Program," Free Russia Foundation, 2020, p. 46, https://www.4freerussia.org/aquarium-leaks-inside-the-gru-s-psychological-warfare-program/.

[87] S.V. Kozlov, *Spetsnaz GRU: Eternal 1989-1999* [Спецназ ГРУ: Безвременные], (Moscow: Russkaya Panorama, 2010), p. 176.

[88] "Locked N' Loaded: Russian Federation psychological operations units" [Locked N' Loaded: подразделения психологических операций Российской Федерации], *Inform Napalm*, Oct. 7, 2020, https://informnapalm.org/49314-podrazdelenii-a-psikhologicheskikh-operat-sii-rossii/.

[89] "Structure of the psychological warfare service of the armed forces of the Russian Federation" [Структура службы психологической борьбы ВС РФ], GRU, 2012.

**Figure 1. Locations of main GRU psychological operations units**


64th Independent Special Service Center
Moscow
72nd Special Service Center (Unit 54777)
Moscow
Center for Foreign Military Information and Communication, Western Military District (plus detachment)
Sertolovo
Psychological Operations Detachment, 45th Spetsnaz Regiment (Airborne)
Kubinka
324th Psychological Operations Detachment
Kaliningrad
Psychological Operations Detachment, 127th Reconnaissance Brigade
Sevastopol
Foreign Military Information and Communication Group, Black Sea Fleet
Sevastopol
Psychological Operations Detachment, 96th Reconnaissance Brigade
Nizhny Novgorod
Center for Foreign Military Information and Communication, Central Military District
Yekaterinburg
295th Psychological Operations Detachment
Dushanbe
2047th Psychological Operations Group
Chita
RUSSIA
UKRAINE
KAZAKHSTAN
UZVEKISTAN
KYRGYZSTAN
TAJIKISTAN
Center for Foreign Military Information and Communication, Eastern Military District (plus detachment)
Khabarovsk
Psychological Operations Detachment, 100th Reconnaissance Brigade
Mozdok
Center for Foreign Military Information and Communication, Southern Military District
Rostov-on-Don
2140th Psychological Operations Group
Rostov-on-Don
Psychological Operations Detachment, 22nd Spetsnaz Brigade
Rostov-on-Don

Source: See Appendix A.

Russian military intelligence signals units (*otdeleniya spetsial'novo naznacheniya*; OSNAZ) have firmly established roots in Russian military history. During the First World War, the Imperial military established the Service for Observation and Networks (*Sluzhby nablyudeniya i svyazy*), which consisted of a central radio intercept station, 10 peripheral radio intercept stations, and 10 more radio direction-finding stations.[90] During the Cold War, the Soviets expanded the ranks of OSNAZ specialists; by the 1980s, there were 40 such regiments and 170 battalions.[91] Since the onset of the Ukraine crisis, independent researchers have revealed some details

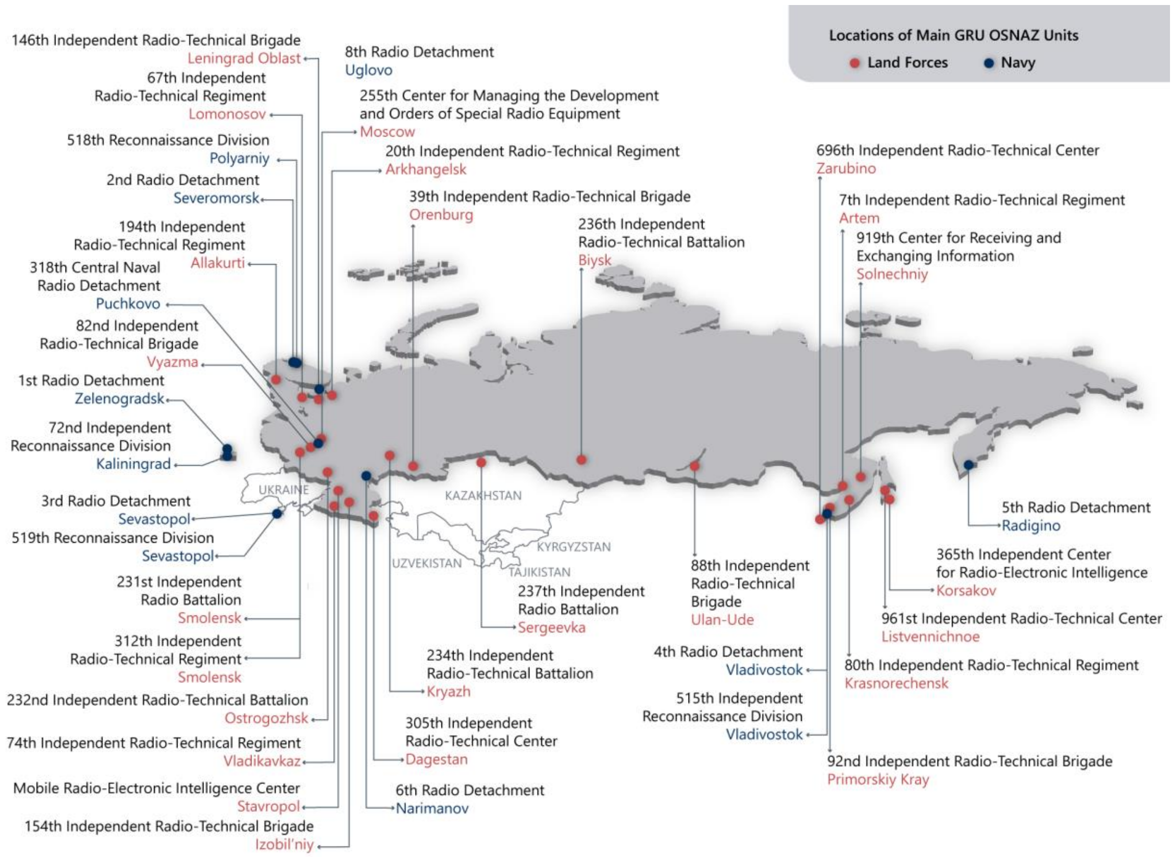
[90] D.A. Larin, *Russia's cryptographic service: studies of history* [Криптографическая служба России: очерки истории], (Moscow: Helios ARV, 2017), p. 24.

[91] Christopher Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*, (New York: Basic Books, 1999), p. 353.

about contemporary OSNAZ activities. The GRU's "Center S" conducts operations in Syria, for instance; as of late 2014, it recorded and decrypted rebel communications in Syria on behalf of Assad's regime.[92] Ukrainian researchers discovered via social media that an OSNAZ specialist with the 82nd Independent Radio-Technical Brigade had probably deployed to Ukraine in late 2014.[93]

*Please see Figure 2 and data in Appendix B for locations*.

### Figure 2. Locations of main GRU OSNAZ units


Locations of Main GRU OSNAZ Units
● Land Forces
● Navy
146th Independent Radio-Technical Brigade
Leningrad Oblast
8th Radio Detachment
Uglovo
67th Independent Radio-Technical Regiment
Lomonosov
255th Center for Managing the Development and Orders of Special Radio Equipment
Moscow
518th Reconnaissance Division
Polyarniy
20th Independent Radio-Technical Regiment
Arkhangelsk
2nd Radio Detachment
Severomorsk
39th Independent Radio-Technical Brigade
Orenburg
194th Independent Radio-Technical Regiment
Allakurti
236th Independent Radio-Technical Battalion
Biysk
318th Central Naval Radio Detachment
Puchkovo
82nd Independent Radio-Technical Brigade
Vyazma
1st Radio Detachment
Zelenogradsk
72nd Independent Reconnaissance Division
Kaliningrad
3rd Radio Detachment
Sevastopol
519th Reconnaissance Division
Sevastopol
231st Independent Radio Battalion
Smolensk
312th Independent Radio-Technical Regiment
Smolensk
232nd Independent Radio-Technical Battalion
Ostrogozhsk
74th Independent Radio-Technical Regiment
Vladikavkaz
Mobile Radio-Electronic Intelligence Center
Stavropol
154th Independent Radio-Technical Brigade
Izobil'niy
234th Independent Radio-Technical Battalion
Kryazh
305th Independent Radio-Technical Center
Dagestan
6th Radio Detachment
Narimanov
237th Independent Radio Battalion
Sergeevka
88th Independent Radio-Technical Brigade
Ulan-Ude
4th Radio Detachment
Vladivostok
515th Independent Reconnaissance Division
Vladivostok
696th Independent Radio-Technical Center
Zarubino
7th Independent Radio-Technical Regiment
Artem
919th Center for Receiving and Exchanging Information
Solnechniy
5th Radio Detachment
Radigino
365th Independent Center for Radio-Electronic Intelligence
Korsakov
961st Independent Radio-Technical Center
Listvennichnoe
80th Independent Radio-Technical Regiment
Krasnorechensk
92nd Independent Radio-Technical Brigade
Primorskiy Kray
UKRAINE
KAZAKHSTAN
UZVEKISTAN
KYRGYZSTAN
TAJIKISTAN

Source: See Appendix B.

[92] Oryx, "Captured Russian Spy Facility Reveals the Extent of Russian Aid to the Assad Regime," *Bellingcat*, Oct. 6, 2014, https://www.bellingcat.com/news/mena/2014/10/06/captured-russian-spy-facility-reveals-the-extent-of-russian-aid-to-the-assad-regime-2/.

[93] Irakli Komaxidze, "Annushka from OsNaz," *Inform Napalm*, Apr. 3, 2015, https://informnapalm.org/en/annushka-from-osnaz/.

# Implementing Information Confrontation

While defense experts and military officers reflected on the application of rapidly evolving digital communications technology to contemporary conflict, Russia's military quietly built new capabilities to meet the challenges and opportunities of a progressively interconnected world. The GRU, for instance, likely initially grafted new computer network operations specialists onto signals intelligence units founded during the Cold War. Beginning in the mid-2000s, malware that cybersecurity researchers would eventually link to GRU operators began penetrating targeted networks from the Caucasus to NATO countries to exfiltrate sensitive data. Russia's military likely worked with Russia's Federal Security Service (FSB) to channel patriotic sentiment into cyberattacks against Georgian government websites during the brief war in late 2008.

Simultaneously, those responsible for psychological operations adapted to the same technological shifts, gradually employing blogs, websites, and even SMS text messages (similar to traditional printed leaflets and journals). Denis Tyurin, a former GRU officer who manages an information agency called InfoRos that spreads disinformation on the GRU's behalf, registered InfoRos-affiliated websites as early as 1999.[94] In the wake of Russia's war with Georgia, an official at the GRU's psychological warfare academy worked to incorporate new methods of digital "information-psychological effects," such as "machine translations" and computer-based audio and video production, into the curriculum. These new methods were coupled with age-old techniques like disinformation, the use of stereotypes, and "statement and repetition."[95] By the time the GRU attempted to affect the outcome of the 2016 US presidential election, it had thoroughly rehearsed these tactics in information confrontation operations aimed at Russia's self-proclaimed "near abroad" and more distant targets in the West.

[94] Tyurin was sanctioned by the US Department of Treasury on April 15, 2021, for his role in managing InfoRos on behalf of the GRU, specifically the 72nd Main Intelligence Information Center. See: "Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections," US Department of the Treasury, Apr. 15, 2021, https://home.treasury.gov/news/press-releases/jy0126). Interestingly, according to domain registration history, Tyurin and a colleague named David Rudman in 1999 registered a domain focused on Russian martial arts, "sambo.com," under a server belonging to InfoRos.

[95] S.A. Cheshuin, "Specifics of contemporary information confrontation and accounting for them when training specialists of foreign military information in the Military university" [Особенности современного информационного противоборства и их учёт при подготовке специалистов зарубежной военной информации в Военном университете], *Pandia.ru*, 2009.

# Conceptualizing, building, and organizing, 1990s to 2013

The role of information confrontation within Russia's defense community has solidified since the uncertainty of the immediate post-Soviet era, when many defense officials and pundits observed rapid advances in modern communications technology with a mix of apprehension and cautious optimism. Russia's then-defense minister, Igor Sergeev, claimed in 1999 that "cyber-weapons," among other emerging defense technologies, were a "main priority" in developing the Russian military's future potential, but he warned the military was falling far behind on these critical developments.[96] In an 2003 article titled "Information Confrontation and Maskirovka of the Forces," two former senior military officers, in light of other countries' increasing attention to bolstering the "methods and means" of conducting information confrontation, suggested combing *maskirovka* (military deception) elements, psychological operations, intelligence, electronic warfare, and computer network operations into a single "information confrontation system" within the military; the authors added that such a system should start at lower levels until it could gradually be integrated into a unified staff structure.[97] The article loosely presaged the eventual creation of the Information Operations Troops and Gerasimov's integration of an information confrontation staff into a district-level exercise. Cyber confrontation between the West and China reinforced emerging concepts associated with computer network operations, such as attribution challenges and "patriotic" hackers, the potential of computer espionage, and the inherent link between technical and psychological effects.[98]

At the same time, outsized fears and expectations occasionally drove outlandish conclusions about the role of computer networks (and even holographic technology) in future conflicts. A former Soviet psychological operations officer, for example, stated in 1999 that hackers could

[96] "Minister of defense of the Russian Federation I.D. Sergeev. Fundamentals of Russian military-technical politics at the start of the 21st century" [Министр обороны РФ Маршал Российской Федерации И.Д.Сергеев. Основы военно-технической политики России в начале XXI века], *Urals Military News* [Уральские Военные Вести], No. 099 (1999).

[97] A.N. Limno and M.F. Krysanov, "Information confrontation and maskirovka of the forces" [Информационное противоборство и маскировка войск], *Military Thought* [Военная мысль], No. 5 (2003).

[98] A. Kirovets, "Organs of propaganda and information confrontation of the PRC" [Органы пропаганды и информационной войны кнр], *Foreign Military Review* [Зарубежное военное обозрение], No. 9 (2013); Vladimir Shcherbakov, "Cyber-spetsnaz attacks from the heavens" [Киберспецназ атакует с территории поднебесной], *Independent Military Review* [Независимое военное обозрение], No. 22 (2008); T. Aitakaeva, "PRC: concepts of information operations" [КНР: концепции информационных операций], *Foreign Military Review* [Зарубежное военное обозрение], No. 6 (2008).

incapacitate internet users by inserting a special color pattern that subconsciously and dramatically increased a victim's heart rate, dubbed "Virus 666," a claim repeated in several Russian military publications in the 2000s and 2010s.[99] Another claim, often mentioned in tandem with Virus 666, is the supposed appearance of an image of Jesus Christ in the sky above Mogadishu in February 1993, which some Russian authors indirectly attributed to US psychological operations forces and even captured the imagination of Igor Panarin, an ex-KGB analyst turned political scientist and Russian luminary on information confrontation, who wrote about the supposed apparition in a 1995 article published in *Red Star*.[100] Panarin, who also posited the economic collapse and eventual partition of the United States, helped to write Russia's 2000 Information Security Doctrine and urged Russia to defend itself against an "information war" from the West, partly by creating its own information warfare system.[101] A member of Russia's Academy of Military Sciences in 2005 described the internet as an "open field" where viruses could "destroy information bases" while "zombifying" populations."[102]

[99] Vladimir Gavrilovich Krysko, *The Secrets of Psychological Warfare* [Секреты психологической войны], (Minsk: Kharvest, 1999), p. 11; V. Belous, "Weapons of the 21st Century," *International Affairs*, No. 2 (2009); "Topic: main directions of providing information security in the activities of troops (forces)" [Тема: основные направления обеспечения информационной безопасности в деятельности войск (сил)], *Military Watch* [Боевая вахта], No. 99 (2001); N.P. Shekhovtsov and Yu. E. Kuleshov, "Information weapon: the theory and practice of its application in information warfare" [Информационное оружие: теория и практика применения в информационном противоборстве], *Bulletin of the Academy of Military Sciences* [Вестник Академии военных наук], No. 1 (2012); One of the rare mentions of Virus 666 is a post by a cybersecurity research firm, F-Secure, which cites a US Army journal in describing the supposed virus: "...computer virus capable of affecting a person's psyche is Russian Virus 666. It manifests itself in every 25th frame of a visual display, where it produces a combination of colors that allegedly put computer users into a trance. The subconscious perception of the new pattern eventually results in arrhythmia of the heart." F-Secure, however, adds that Virus 666 "is nonsense," and one should "ignore it." See: "Russian Virus 666," F-Secure, undated, https://www.f-secure.com/v-descs/russv666.shtml.

[100] Gennadiy Zhilin, "Information-psychological weapons: yesterday and today" [Информационно-психологическое оружие: вчера и сегодня], *Soldier of the Fatherland* [Солдат Отечества], No. 57 (2004); Igor Panarin, "'Trojan horse' of the 21st century. Information weapons: realities and possibilities" ["Троянский конь" XXI века. Информационное оружие: реалии и возможности], *Red Star* [Красная звезда], No. 282 (1995); R. Zukulis, "Information weapons. Shock-inducing, or victory without a single shot" [Информационное оружие. Повергающее в шок, или победа без единого выстрела], *Flag of the Motherland* [Флаг Родины], No. 155 (1999); Claims of an image of Christ appearing in the sky above Mogadishu in early 1993 were published in an American tabloid, *Weekly World News*, that closed in 2007. See: Becky Granger, "Face of Jesus Photographed over Somalia!" *Weekly World News*, Mar. 2, 1993.

[101] Dmitriy Shlapentokh, "How the Putin Regime Perceives US Protests," Institute of Modern Russia, Jul. 29, 2020, https://imrussia.org/en/analysis/3144-how-the-putin-regime-perceives-us-protests; Oscar Jonsson, *The Russian Understanding of War: Blurring the Lines between War and Peace* (Washington: Georgetown Press, 2019), pp. 115-116.

[102] Viktor Khudoleev, "Information confrontation. When they fire words" [Информационное противоборство. когда стреляют словом], *Red Star* [Красная звезда], No. 193 (2005).

To be sure, assigning an almost paranormal dimension to the psychological aspects of conflict, however, is not exclusive to contemporary Russian defense thinkers. Pyotr Nikolaevich Krasnov, a Cossack commander during World War One and anti-Bolshevik author-in-exile following the Russian Civil War, claimed in his book *Soul of an Army* that "mass hallucinations" could, however infrequently, determine a battle. Krasnov gave the example of the surrender of Austro-Hungarian soldiers to Russian forces in Galicia in 1914 who claimed to have seen the Virgin Mary overhead providing cover to the Tsar's troops.[103] Nevertheless, authors with Russia's PIR-Center presented a more sober view on information confrontation in 2001, claiming that despite "serious discussions" about the concept in scientific circles, in reality, its full potential was in the distant future.[104]

It took the experiences of the early 2010s, such as the Arab Spring and the Bolotnaya protests in Russia, to fully galvanize Russian leadership against perceived information threats. Putin remarked in 2012 that military capabilities in the fields of space, information confrontation, and cyberspace would have "great, if not decisive, significance" in future conflicts.[105] Then-deputy director of the FSB Sergey Smirnov warned that "Western special services" were forming secret units to use modern communications technology to destabilize societies, and that Russia's 2012 presidential election demonstrated the potential of the "blogosphere" to disrupt Russia.[106] This period inaugurated an unprecedented congruence between Russian senior leadership and mid-level officials within the military, who had been warning about information confrontation for well over a decade.

Limited cases of cyber activity attributable to Russian military actors in the 2000s demonstrate early efforts to meet these challenges and harness the potential of rapid advances in digital communications technology. Between 2004 and 2013, APT28—a hacker outfit attributed to the GRU's Unit 26165[107]—used fake NATO correspondence and imitated pro-Chechen websites

[103] P.N. Krasnov, *Soul of an Army* [Душа армии], (YOYO Media: Moscow, 2016), p. 51.

[104] A.V. Fedorov and V.N. Tsygichko, "Information challenges of national and international security" [Информационные вызовы национальной и международной безопасности], *PIR Center*, Aug. 2001, p. 110.

[105] Vladimir Putin, "Vladimir Putin: 'Being strong: guarantees of Russia's national security" [Владимир Путин: "Быть сильными: гарантии национальной безопасности для России"], *Rossiyskaya Gazeta*, Feb. 20, 2012, https://rg.ru/2012/02/20/putin-armiya.html.

[106] "The FSB vows to clear foreign special services from Russia's internet" [ФСБ обещает очистить рунет от воздействия зарубежных спецслужб], *Vedomosti*, Mar. 27, 2012, https://www.vedomosti.ru/technology/news/2012/03/27/fsb_obeschaet_ochistit_runet_ot_vozdejstviya_zarubezhnyh.

[107] "APT28," *MITRE*, Apr. 19, 2021, https://attack.mitre.org/groups/G0007/.

to exploit networks to gain intelligence on adversaries.[108] The IP address used to host the "stopgeorgia" website during Russia's war with Georgia in 2008 belonged to a small company, Steadyhost, that was essentially collocated with a large GRU complex on Khoroshevskoe Highway in Moscow.[109] For their part, GRU psychological operations specialists exhibited burgeoning efforts to use the internet for their work. As early as 2004, psychological operations specialists based in Russia's Eastern Military District maintained a website somewhat akin to the Central Intelligence Agency's World Factbook that provided information about countries in the region, but also "specialist commentary" that included articles about human rights abuses in China, organized crime in Japan, "suicide through the internet," and other regional and international topics.[110]

## Ukraine crisis to present

Operations targeting Ukraine beginning in 2014 demonstrated the practical application of over a decade's worth of observations and the comparatively experimental efforts of the 2000s. GRU psychological operations specialists used social media on an unprecedented scale to influence Ukrainian and international audiences throughout the conflict, beginning after Russia's annexation of Crimea.[111] According to Ukrainian intelligence, GRU specialists and their proxies coupled modern methods of psychological warfare, like disseminating SMS messages, with traditional ones, such as leaflets, to "demoralize, confuse, and intimidate" Ukraine's armed forces.[112] In 2014, "Cyber Berkut"—an ostensibly pro-Russian Ukrainian hacktivist group now attributed to the GRU—began a years-long campaign involving defacing Ukrainian government websites, cyberattacks against Ukrainian and regional targets, and election interference.[113]

[108] "APT28: A Window into Russia's Cyber Espionage Operations?" *FireEye*, 2014, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf.

[109] Daniil Turovskiy, *Invasion: a short history of Russian hackers* [Вторжение: краткая история русских хакеров], (Moscow: Inviduum, 2019), p. 138.

[110] "Archive" [Архив], Center for Foreign Military Information and Communication, Far East Military District, Russian Federation, Jul. 29, 2004, https://web.archive.org/web/20041026135744/http://www.atrinfo.ru/archive/archive%20main.htm.

[111] Ellen Nakashima, "Inside a Russian disinformation campaign in Ukraine in 2014," *Washington Post*, Dec. 25, 2017, https://www.washingtonpost.com/world/national-security/inside-a-russian-disinformation-campaign-in-ukraine-in-2014/2017/12/25/f55b0408-e71d-11e7-ab50-621fe0588340_story.html?utm_term=.2a5196bd1120.

[112] "SBU exposes psy-ops group working for Russia's GRU," UNIAN Information Agency, Mar. 12, 2019, https://www.unian.info/politics/10477047-sbu-exposes-psy-ops-group-working-for-russia-s-gru.html.

[113] Vitaly Shevchenko, "Ukraine conflict: Hackers take sides in virtual war," BBC, Dec. 20, 2014, https://www.bbc.com/news/world-europe-30453069.

During a late-November 2014 trip to Kyiv by then-Vice President Joe Biden, the group claimed to have illicitly obtained confidential documents from Biden's staff, which were posted to vk.com, Russia's rough equivalent to Facebook.[114] A year later, GRU hackers with the GTsST launched a cyberattack against Kyiv's power grid that temporarily left 230,000 people without power. A similar attack against Kyiv's energy infrastructure in 2016 led some researchers to conclude that Ukraine served as a "testbed" for evolving Russian cyber warfare capabilities.[115]

The GRU simultaneously gained experience in conducting the kind of cyber-enabled influence operations that would eventually gain significant international attention, especially after the GRU's effort to affect the US presidential election in 2016. Operations in 2015 attributed to or suspected to have been conducted by Russian military actors solidified the link between the technical and psychological aspects of computer network operations that Russian defense experts had long envisioned. Beginning in January of that year, GRU cyber and psychological operations specialists posed as an ISIS-affiliated hacking group, CyberCaliphate, as part of a campaign involving hack-and-leak tactics, cyberattacks against French and US news networks, and threatening the physical safety of spouses of US service members through social media.[116] The CyberCaliphate campaign was most likely part of an effort to divert international attention from Russia's intervention in east Ukraine and redirect it toward the threat posed by ISIS, possibly paving the way for Russian intervention in Syria later that year. Also in 2015, a pseudonymous blog published a claim based on "confidential sources" that Washington armed ISIS to sow regional chaos.[117] The author of Drakula's Blog claimed to be a Romanian with access to confidential sources and leaked documents. Between early 2015 and late 2016, the blog posted allegations in stilted English that included local authorities downplaying an Ebola outbreak in Texas,[118] NATO's use of combat drones in the Arctic under false pretenses to

[114] Vitaly Shevchenko, "Ukraine conflict: Hackers take sides in virtual war," BBC, Dec. 20, 2014, https://www.bbc.com/news/world-europe-30453069.

[115] Kim Zetter, "The Ukrainian Power Grid Was Hacked Again," *VICE Motherboard*, Jan. 10, 2017, https://www.vice.com/en/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report.

[116] Raphael Satter, "Russian hackers posed as IS to threaten military wives," AP News, May 8, 2018, https://apnews.com/article/mi-state-wire-or-state-wire-russia-co-state-wire-north-america-4d174e45ef5843a0ba82e804f080988f.

[117] "U.S. and its struggle against ISIL," *DrakulaBlogZ*, Mar. 30, 2015, https://drakulablogdotcom3.wordpress.com/2015/03/30/u-s-and-its-struggle-against-isil/.

[118] "Exciting trip to the USA," *DrakulaBlogZ*, Apr. 2, 2015, https://drakulablogdotcom3.wordpress.com/2015/04/02/exciting-trip-to-the-usa/.

establish control over vital resources,[119] and corruption rings that linked the US Democratic Party to Azerbaijan's President Ilham Aliyev.[120] In July 2015, the blog leaked details of a meeting at NATO's Center of Excellence for Strategic Communication in Riga, subtly doctoring the information by adding points about the supposed growing popularity of Russian leadership among Ukrainians.[121] While the blog seemingly gained little traction, "Drakula's" work was mentioned in several Russian military journals, including a 2015 article in *Foreign Military Review* that repeated the blog's claim about a supposed plan by NATO to undermine Moscow by inducing panic and defeatism within Russia's population.[122] A separate article published in *Independent Military Review* called Drakula's Blog an analogue to Wikileaks, concluding that—because of Western "information attacks"—Russia's military would "learn how to wield such a weapon."[123]

Many GRU cyber operations with no clear digital influence component still have a discernible motivation to inflict "information-psychological" effects on their targets, reflecting the continued importance of influencing foreign audiences. The "NotPetya" attack in 2017, for instance, occurred on Ukraine's Constitution Day. A study by Booz Allen Hamilton of GRU cyber activity found that the GRU selected dates for some of its operations "on or around days related to Ukrainian identity and independence," and—on certain occasions—the choice of target "strongly aligned with the operation's symbolic significance."[124] A "massive" cyberattack launched by the GRU against Georgia in late 2019, despite affecting a wide range of targets, also included website defacement and follow-on attacks against two television broadcasters, which Adam Meyers, the vice president of intelligence for CrowdStrike, described as indicative of

[119] "What is the purpose of combat drones in the Arctic?" *DrakulaBlogZ*, Aug. 10, 2015, https://drakulablogdotcom3.wordpress.com/2015/08/10/drones_arctic/.

[120] "Democrats don't care a pin about their principles! They are under the thumb of lobbying companies funded by oil magnates," *DrakulaBlogZ*, Jun. 8, 2016, https://drakulablogdotcom3.wordpress.com/2016/06/08/democrats-funded-by/.

[121] Steve Tatham, "The Solution to Russian Propaganda is not EU or NATO Propaganda but Advanced Social Science to Understand and Mitigate its Effect in Targeted Populations," *IO Sphere* (Fall 2015), p. 29.

[122] "Information wars" [Информационные войны] *Foreign Military Review* [Зарубежное военное обозрение], No. 5 (2015).

[123] Vladimir Mukhin, "Headquarters to an information spetsnaz" [Ставка на информационный спецназ], *Independent Military Review* [Независимое военное обозрение], No. 14 (2015).

[124] "Bearing Witness: Uncovering the Logic behind Russian Military Cyber Operations," Booz Allen Hamilton, 2020, p. 18, https://www.boozallen.com/content/dam/boozallen_site/ccg/pdf/publications/bearing-witness-uncovering-the-logic-behind-russian-military-cyber-operations-2020.pdf.

Russian tactics: “The specific outcome is less important than causing upheaval and conflict between different groups in the country.”[125]

## GRU cyber espionage

International attention surrounding some of GRU hackers’ most notorious operations risks overlooking the psychological nature of GRU cyber activity and eclipsing the GRU’s more routine—but important—cyber espionage efforts. Russian military hackers’ target government and civilian networks that span the globe to illicitly gain valuable information. Non-military targets for espionage, such as the US Democratic Party in 2016, or even the Patriarch of the Orthodox Church in 2015, however, demonstrate the GRU’s willingness to target civilian and political networks, likely producing not only political intelligence, but possible material for subsequent online influence operations. In September 2020, GRU hackers used a “hard to detect” strand of the GRU’s Zebrocy malware to gain access to NATO networks through ostensible NATO training documents infected by malicious code.[126] GRU cyber espionage is the most common activity in the organization’s digital repertoire, and cybersecurity research on GRU espionage campaigns shows continued attempts to breach defense industrial networks, likely to boost Russia’s own military development. Moreover, NATO networks offer intelligence on deployments, exercises, force postures, and other operational and strategic issues that would prove valuable to any country’s military intelligence. Interestingly, in 2017, GRU hackers shifted from traditional NATO targets to ones based in Central and East Asia, particularly networks owned by diplomatic and defense organizations, demonstrating that GRU cyber espionage does not exclusively target the West.[127]

## Battlefield hacking?

Judging from known activity, GRU cyber operators are probably less concerned with directly affecting tactical conditions in places like eastern Ukraine or Syria than they are with broader

[125] Andy Greenberg, “The US Blames Russia's GRU for Sweeping Cyberattacks in Georgia,” *WIRED*, Feb. 20, 2020, https://www.wired.com/story/us-blames-russia-gru-sweeping-cyberattacks-georgia/.

[126] Ax Sharma, “Russian hackers use fake NATO training docs to breach govt networks,” *Bleeping Computer*, Sept. 22, 2020, https://www.bleepingcomputer.com/news/security/russian-hackers-use-fake-nato-training-docs-to-breach-govt-networks/.

[127] “Sofacy shifts focus to include Far East defense and diplomacy, overlaps with advanced cyber espionage groups,” Kaspersky, Mar. 9, 2018, https://www.kaspersky.com/about/press-releases/2018_sofacy.

cyberattacks, digital influence, and espionage. Nevertheless, a handful of cases reveal potential attempts to achieve tactical effects. CrowdStrike analysts, for example, identified and attributed a GRU effort that occurred between 2014 and 2016 to target Ukrainian artillerists by infecting an Android phone application that helped specialists process data and fire more quickly.[128] A Ukrainian military officer at a 2019 symposium on electronic warfare claimed that unidentified Russian actors used a "virus" to infect Ukrainian radio repeaters to suppress communications.[129] Although several Russian defense officials and experts wrote about the potential of frontline hackers to disrupt local enemy command-and-control networks or even generate physical effects on enemy equipment through computer networks, these kinds of tactical efforts probably fall under the remit of the electronic warfare forces (versus GRU hackers). Roger McDermott, a specialist in Russian security issues, in 2017 found a "close link" between signals intelligence, air defense, artillery, and electronic warfare in Russian operations in southeastern Ukraine.[130] Of course, GRU hackers do not focus only on strategic effects and electronic warfare units do not focus only on tactical effects; instead, military leadership probably usually uses them for different effects in different environments.

## Large-scale, destructive cyberattacks

Russia's military has, with notable exceptions, refrained from launching large-scale cyberattacks devoid of any intended psychological effect against Russia's perceived Western adversaries, indicating that military planners reserve these operations for war (or the run up to it). Since the early 2000s, Russian military authors have frequently written about the destructive potential of cyberattacks aimed at an opponent's "soft underbelly"—its increasingly networked critical infrastructure, such as transportation and energy targets.[131]

[128] Adam Meyers, "Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units," CrowdStrike, Dec. 22, 2016, https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/.

[129] Shawn Snow, "US forces could learn from intense electronic war battle in Ukraine," *Military Times*, Oct. 30, 2019, https://www.militarytimes.com/flashpoints/2019/10/30/us-forces-could-learn-from-intense-electronic-war-battle-in-ukraine/.

[130] Roger N. McDermott, "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum," International Centre for Defence and Security, Sept. 2017, p. 5, https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf.

[131] Nikolay Novichkov, "The U.S. is not fully ready to repel serious cyberattacks" [США пока полностью не готовы к отражению серьезной кибератаки], *Military-Industrial Courier* [Военно-промышленный курьер], No. 31 (2012); Yu.O. Yashchenko, "The internet and information confrontation" [Интернет и информационное противоборство], *Military Thought* [Военная мысль], No. 3 (2003); Yu.I. Starodubtsev, P.V. Zakalkin, and S.A. Ivanov, "Technosphere warfare as a fundamental method of deciding conflicts in the conditions of globalization"

Undoubtedly, cyberattacks against critical infrastructure factor heavily into the Russian military's "strategic operation to destroy critically important targets" (SODCIT) concept. SODCIT, according to Dave Jonson, a NATO staff officer and expert on Russian national security, "is a multidomain operation intended to destroy critical enemy facilities in order to achieve a strategic objective."[132] As Timothy Thomas, a longstanding expert on Russian information operations, further explained in 2019:

> Cyber operations, which seemingly are without borders, are most likely one aspect of Russia's SODCIT concept, as it allows Russia to affect an enemy to the full depth of his territory in global information space. The SODCIT concept implies deep reach into an opponent's rear area and threats there to political, economic, military, and information infrastructures and targets of strategic significance. There is very little in the open military literature about this concept, but it has apparently been discussed in Russia for several years and, due to its strategic implications, is extremely important yet close hold.[133]

Nevertheless, in a hypothetical future conflict, the Russian military is likely to exhibit whatever ability it has to digitally incapacitate an adversary's critical infrastructure to increase the potential cost to NATO of overt conflict and deter NATO's less enthusiastic members. A 2017 cyberattack on a petrochemical facility in the Middle East, attributed to the Russian government's Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM), demonstrated the capability "to cause significant physical damage and loss of life."[134] The fact that the attack had no clear motivation and underscores the difficulty in predicting Russian state-sponsored cyber activity, including attacks with physical effects.

More recent revelations about GRU-affiliated hackers' supposed presence in US critical infrastructure since as early as 2017 could suggest that Russia's military is preparing for a contingency that calls for direct cyberattacks against the West, though there was no evidence

[Техносферная война как основной способ разрешения конфликтов в условиях глобализации], *Military Thought* [Военная мысль], No. 10 (2020).

[132] Dave Jonson, "Russia's Conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds," Lawrence Livermore National Laboratory Center for Global Security Research, Feb. 2018, p. 52, https://cgsr.llnl.gov/content/assets/docs/Precision-Strike-Capabilities-report-v3-7.pdf.

[133] Timothy L. Thomas, "Russian Military Thought: Concepts and Elements," MITRE, Aug. 2019, p. 8-6, https://www.mitre.org/sites/default/files/publications/pr-19-1004-russian-military-thought-concepts-elements.pdf.

[134] Additionally, according to the US Department of the Treasury, "In 2019, the attackers behind the Triton malware were also reported to be scanning and probing at least 20 electric utilities in the United States for vulnerabilities;" US Department of the Treasury, "Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware," Press Releases, Oct. 23, 2020, https://home.treasury.gov/news/press-releases/sm1162.

of this intent in the malware itself.[135] The Soviet military long messaged that its strategic rockets "were always at the ready" (*vsegda na postu*); a modern interpretation of this idea is that the GRU's hackers are "always near their keyboards," though no serious observer of Russia's military would equate cyber capabilities with the potentially apocalyptic capabilities of strategic nuclear forces.

[135] Andy Greenberg, "Hackers Tied to Russia's GRU Targeted the US Grid for Years, Researchers Warn," *WIRED*, Feb. 24, 2021, https://www.wired.com/story/russia-gru-hackers-us-grid/.

# Looking Forward

The assessment on 2020 election interference and influence released by the US intelligence community in early March this year describes a mostly negligible role played by the GRU, a stark departure from the 2016 campaign surrounding the US presidential election. The GRU, for example, unsuccessfully targeted "US political actors" in 2019 and 2020.[136] Although the GRU did apparently penetrate networks belonging to Burisma, the Ukrainian energy firm that Russian actors seek to associate with corruption on the part of US President Joe Biden and his family, the operation was quickly discovered and eventually attributed—amid controversy within the cybersecurity community—before the election.[137] Indeed, officials and analysts of Russian influence and cyber activity generally view 2020 as a failure by Russian actors "to mount any major hacking or disinformation operations to interfere in the presidential election."[138] This failure probably stems from several different factors, some of which are extrinsic to Russian hackers, such as an increasingly divided American political culture and an accelerating, cacophonic news cycle. Russian limitations, however, very likely also factored into the seemingly muted effort in 2020.

GRU hackers, for one, face far more operational scrutiny now than they did prior to 2016—an extensive network of cybersecurity firms have since increasingly sought to expose their activities. Before the 2018 US midterm elections, Microsoft disabled six internet domains used by GRU hackers that targeted US political organizations and affiliates.[139] Western governments publish operational details about units like the 85th GTsSS and GTsST. In August 2020, the US National Security Agency (NSA) and Federal Bureau of Investigation (FBI) published a report on malware used by the 85th GTsSS called "*drovorub*" (lumberjack); the report included

[136] "Foreign Threats to the 2020 US Federal Elections," Office of the Director of National Intelligence, Mar. 15, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

[137] Nicole Perloth and Matthew Rosenberg, "Russians Hacked Ukrainian Gas Company at Center of Impeachment," *New York Times*, Jan. 13, 2020, https://www.nytimes.com/2020/01/13/us/politics/russian-hackers-burisma-ukraine.html.

[138] Ellen Nakashima, "Fewer opportunities and a changed political environment in the U.S. may have curbed Moscow's election interference this year, analysts say," *Washington Post*, Nov. 17, 2020, https://www.washingtonpost.com/national-security/russia-failed-to-mount-major-election-interference-operations-in-2020-analysts-say/2020/11/16/72c62b0c-1880-11eb-82db-60b15c874105_story.html.

[139] Kelly Jackson Higgins, "Microsoft Sinkholes 6 Fancy Bear/APT28 Internet Domains," *DARKReading*, Aug. 21, 2018, https://www.darkreading.com/attacks-breaches/microsoft-sinkholes-6-fancy-bear-apt28-internet-domains/d/d-id/1332628

valuable information about how to detect and mitigate the activity.[140] Even on the "information-psychological" side of operations, the GRU seems to have recently experienced mostly setbacks. In September 2020, Facebook dismantled a network linked to the GRU consisting of 224 accounts, 35 pages, 18 groups, and 34 Instagram accounts.[141] In July 2020, US officials revealed that the GRU covertly managed InfoRos and OneWorld.Press; another, "Rebel Inside," was exposed in March 2021.[142] Identifications, attributions, removals, sanctions, and unrelenting scrutiny from a range of public and private partners have dramatically changed the environment that GRU digital specialists knew several years ago, suggesting that the GRU's cyber capabilities may fail to meet the theoretical and doctrinal importance of information confrontation. Given the consistent and alarming threat posed by NATO from Moscow's perspective, plus the zero-sum world of Russian bureaucratic rivalry, failure—or even stagnation—could spell a diminishing importance for the Russian military vis-à-vis other intelligence and security agencies that would enthusiastically usurp parts of the GRU's cyber mandate should senior officials' potential disappointment with the GRU seek to empower others at the expense of military intelligence. No real evidence, however, suggests this to be the case. Indeed, affirmation of the GRU's work from Putin during the organization's centennial anniversary in 2018 showed no signs that the public attribution of cyber operations to the GRU that year, or even its exposed involvement in the poisoning of GRU defector Sergei Skripal, shook the president's confidence in its "professionalism, courage, and determination."[143]

Moscow could, of course, work to ease the bitter, longstanding feuds between Russia's intelligence services, allowing it to better marshal available resources and personnel, including those within the military. Malware associated with both Russia's Foreign Intelligence Service (SVR) and the GRU simultaneously breached and sought to expand their respective accesses to a network belonging to the US Democratic National Committee in early 2016; cybersecurity researchers believe the two agencies did so as parallel, uncoordinated efforts and were largely

[140] "Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware," National Security Agency and Federal Bureau of Investigation, Aug. 2020, https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF.

[141] Nathaniel Gleicher, "Removing Coordinated Inauthentic Behavior, Facebook, Sept. 24, 2020, https://about.fb.com/news/2020/09/removing-coordinated-inauthentic-behavior-russia/

[142] "U.S. Accuses Russia Of Spreading Disinformation About Western COVID Vaccines," Radio Free Europe/Radio Liberty, Mar. 7, 2021, https://www.rferl.org/a/us-accuses-russia-covid-vaccine-disinformation/31138444.html; Julian E. Barnes and David E. Sanger, "Russian Intelligence Agencies Push Disinformation on Pandemic," *New York Times*, Jul. 28, 2020, https://www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html.

[143] "Putin Praises Russian GRU Military Intel for Its 100 Years," *Voice of America*, Nov. 2, 2018, https://www.voanews.com/europe/putin-praises-russian-gru-military-intel-its-100-years.

unaware of each other’s activity.[144] Fostering a more collaborative relationship between the two agencies might eventually lead to a more effective division of labor that avoids such redundancies. After all, the director of the SVR, Sergey Naryshkin, declared in late 2018 that the GRU and SVR both consisted of “talented people” that “share experience” and “intelligence information,” and that the two services assisted—rather than competed against—one another.[145] Meanwhile, the FSB has continued quiet and successful cyber espionage against a wide array of targets and remains a key player in offensive cyber operations. Despite its deep rivalry with the GRU, which may have even driven FSB hackers to disclose the GRU’s role in 2016 election hacking to Western officials, the benefits of collaborating on cyber operations might be enough to eventually bridge the bureaucratic divides between these actors, or at least get them to stop actively undermining one another. [146]

Whatever challenges they face, the GRU’s hackers show no signs of reducing the volume or frequency of their operations. In some cases, they are continuing to use the “art of improvisation” as their Soviet predecessors did. As NSA and FBI revealed the GRU’s drovorub malware, GRU hackers used far less sophisticated tactics to aggressively pursue its cyber espionage agenda, including a successful penetration of Norway’s parliament using methods that were “so common that they may seem like background noise that can be ignored.”[147] Another set of GRU malware in late 2020 used COVID-19 themes to launch a broad phishing campaign, indicating GRU hackers’ adeptness at “repurposing current world events to their advantage.”[148] A recent statement by the French Information Security Agency revealed a successful effort by GTsST hackers to exploit an IT monitoring system that lasted from 2017 to 2020, while an NSA advisory in May 2020 claimed the unit had successfully exploited

[144] “CrowdStrike’s work with the Democratic National Committee: Setting the record straight,” CrowdStrike, Jun. 5, 2020, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

[145] “Naryshkin described the cooperation between the SVR and GRU” [Нарышкин рассказал о взаимодействии СВР и ГРУ], *RIA Novosti*, Dec. 9, 2018, https://ria.ru/20181209/1547688565.html.

[146] Kimberly Zenz, “Infighting Among Russian Security Services in the Cyber Sphere,” Presentation at Black Hat USA (2019), https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjZ4O39jPHvAhWmB50JHQylBUUQFjAGegQIBhAD&url=https%3A%2F%2Fi.blackhat.com%2FUSA-19%2FThursday%2Fus-19-Zenz-Infighting-Among-Russian-Security-Services-in-the-Cyber-Sphere.pdf&usg=AOvVaw0tA9FR5ND4A50RQz0KJdGu.

[147] Feike Hacquebord, “Pawn Storm’s Lack of Sophistication as a Strategy,” *Trend Micro*, Dec. 17, 2020, https://www.trendmicro.com/en_us/research/20/l/pawn-storm-lack-of-sophistication-as-a-strategy.html.

[148] Ravie Lakshaman, “Russian APT28 Hackers Using COVID-19 as Bait to Deliver Zebrocy Malware,” *The Hacker News*, Dec. 9, 2020, https://thehackernews.com/2020/12/russian-apt28-hackers-using-covid-19-as.html.

vulnerable email servers for several months.[149] The perpetual arms race between cybersecurity specialists and GRU hackers has demonstrated that any setbacks suffered by the latter are likely to be temporary and that, as long as the motive exists, these units will continue to penetrate targeted networks, the ultimate effects of which are often only revealed after the fact, if they are discovered at all.

[149] Andy Greenberg, "NSA: Russia's Sandworm Hackers Have Hijacked Mail Servers," *WIRED*, May 20, 2020, https://www.wired.com/story/nsa-sandworm-exim-mail-server-warning/; Andy Greenberg, "France Ties Russia's Sandworm to a Multiyear Hacking Spree," *WIRED*, Feb. 15, 2021, https://www.wired.com/story/sandworm-centreon-russia-hack/.

# Appendix A: Locations of Main GRU Psychological Operations Units

Table 1. Main GRU Psychological Operations Units

| | |
|---|---|
| 72nd Special Service Center (Unit 54777) | Moscow |
| 64th Independent Special Service Center | Moscow |
| 295th Psychological Operations Detachment | Dushanbe |
| 324th Psychological Operations Detachment | Kaliningrad |
| Psychological Operations Detachment, 96th Reconnaissance Brigade | Nizhny Novgorod |
| Psychological Operations Detachment, 100th Reconnaissance Brigade | Mozdok |
| Psychological Operations Detachment, 127th Reconnaissance Brigade | Sevastopol |
| Foreign Military Information and Communication Group, Black Sea Fleet | Sevastopol |
| Center for Foreign Military Information and Communication, Central Military District | Yekaterinburg |
| Center for Foreign Military Information and Communication, Southern Military District | Rostov-on-Don |
| 2140th Psychological Operations Group | Rostov-on-Don |
| Psychological Operations Detachment, 22nd Spetsnaz Brigade | Rostov-on-Don |
| Psychological Operations Detachment, 45th Spetsnaz Regiment (Airborne) | Kubinka |
| Center for Foreign Military Information and Communication, Western Military District (plus detachment) | Sertolovo |
| 2047th Psychological Operations Group | Chita |

| | |
|---|---|
| Center for Foreign Military Information and Communication, Eastern Military District (plus detachment) | Khabarovsk |

Sources: “GRU General Staff: Structure” [ГРУ ГШ: структура], Warfare.be, 2012, archived at: http://archive.li/gncZ1; Ari Pesonen, “Russian psychological warfare units were created in the Defense Forces reform” [Venäjän psykologisen sodankäynnin yksiköt luotiin puolustusvoimauudistuksessa], Uusi Suomi (blog), Mar. 1, 2018, https://puheenvuoro.uusisuomi.fi/aripesonen1/251571-venajan-psykologisen-sodankaynnin-yksikot-luotiin-puolustusvoimauudistuksessa/; Vladimir84, “Information about Russian ‘psycho’ forces became known” [Стали известны данные о войсках «психов» России.], Tribun, Feb. 6, 2018; Mariner, “Pscyhological operations units of the Russian army” [Підрозділи психологічних операцій російської армії], Mil.in.ua, May 18, 2020, https://mil.in.ua/uk/articles/pidrozdily-psyhologichnyh-operatsij-rosijskoyi-armiyi/?fbclid=IwAR0KSPgdVpWCSaH3SV-Q6jNqKV0sJ_5nH_QlJElrmHOjFATTbAvkYLvY;  “22nd Independent spetsnaz brigade GRU” [22 ГВ. ОБРСПН ГРУ], Govserv.org, undated, https://www.govserv.org/RU/Bataysk/1413473168676015/22-гв.-ОБрСпН-ГРУ; “The Chinese language – my future!” [Китайский язык – мое будущее!], Transbaikal State University, Mar. 19, 2015, http://www.zabgu.ru/php/open_news.php?query=kitajskij_yazy%27k&news_page=1.

# Appendix B: Locations of Main GRU OSNAZ Units

Table 2. Main GRU OSNAZ Units

| **Land Forces** | |
|---|---|
| 92nd Independent Radio-Technical Brigade | Primorskiy Kray |
| 82nd Independent Radio-Technical Brigade | Vyazma |
| 146th Independent Radio-Technical Brigade | Leningrad Oblast |
| 88th Independent Radio-Technical Brigade | Ulan-Ude |
| 39th Independent Radio-Technical Brigade | Orenburg |
| 154th Independent Radio-Technical Brigade | Izobil'niy |
| 20th Independent Radio-Technical Regiment | Arkhangelsk |
| 7th Independent Radio-Technical Regiment | Artem |
| 74th Independent Radio-Technical Regiment | Vladikavkaz |
| 236th Independent Radio-Technical Battalion | Biysk |
| 237th Independent Radio Battalion | Sergeevka |
| 231st Independent Radio Battalion | Smolensk |
| 232nd Independent Radio-Technical Battalion | Ostrogozhsk |
| 234th Independent Radio-Technical Battalion | Kryazh |
| 305th Independent Radio-Technical Center | Dagestan |
| 312th Independent Radio-Technical Regiment | Smolensk |
| 67th Independent Radio-Technical Regiment | Lomonosov |
| 80th Independent Radio-Technical Regiment | Krasnorechensk |
| Mobile Radio-Electronic Intelligence Center | Stavropol |

| | |
|---|---|
| 255th Center for Managing the Development and Orders of Special Radio Equipment | Moscow |
| 919th Center for Receiving and Exchanging Information | Solnechniy |
| 365th Independent Center for Radio-Electronic Intelligence | Korsakov |
| 696th Independent Radio-Technical Center | Zarubino |
| 961st Independent Radio-Technical Center | Listvennichnoe |
| 194th Independent Radio-Technical Regiment | Allakurti |
| **Navy** | |
| 1st Radio Detachment | Zelenogradsk |
| 2nd Radio Detachment | Severomorsk |
| 3rd Radio Detachment | Sevastopol |
| 4th Radio Detachment | Vladivostok |
| 5th Radio Detachment | Radigino |
| 6th Radio Detachment | Narimanov |
| 8th Radio Detachment | Uglovo |
| 318th Central Naval Radio Detachment | Puchkovo |
| 72nd Independent Reconnaissance Division | Kaliningrad |
| 515th Independent Reconnaissance Division | Vladivostok |
| 518th Reconnaissance Division | Polyarniy |
| 519th Reconnaissance Division | Sevastopol |

Sources: “GRU General Staff: Structure” [ГРУ ГШ: структура], Warfare.be, 2012, archived at: http://archive.li/gncZ1; “Military units of Krasnodar and Krasnodar region” [Воинские части Краснодара и Краснодарского края], Vlad-expert.ru, undated, https://vlad-expert.ru/setevaja-voennaja-chast-v-kazanskoj-kropotkin-10309/; Elena Vasilieva, “Shoygu continued Serdyukov’s initiatives or what became of the unbeatable” [Шойгу продолжил начинания Сердюкова или что стало с непобедимой], Evasiljeva.ru (blog), Apr. 30, 2014, http://www.evasiljeva.ru/2015/11/blog-post_427.html.

# Figures

# Tables

This page is intentionally left blank.

**This report was written by CNA's Strategy, Policy, Plans, and Programs Division (SP3).**

SP3 provides strategic and political-military analysis informed by regional expertise to support operational and policy-level decision-makers across the Department of the Navy, the Office of the Secretary of Defense, the unified combatant commands, the intelligence community, and domestic agencies. The division leverages social science research methods, field research, regional expertise, primary language skills, Track 1.5 partnerships, and policy and operational experience to support senior decision-makers.

CNA is a not-for-profit research organization that serves the public interest by providing in-depth analysis and result-oriented solutions to help government leaders choose the  best course of action in setting policy and managing operations.

CNA

Dedicated to the Safety and Security of the Nation

IOP-2021-U-030078-Final

3003 Washington Boulevard, Arlington, VA 22201
www.cna.org ● 703-824-2000