Congressional Research Service
Informing the legislative debate since 1914

Russian Military Intelligence: Background and Issues for Congress

Updated November 15, 2021

Congressional Research Service
https://crsreports.congress.gov
R46616

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46616

November 15, 2021

Andrew S. Bowen
Analyst in Russian and European Affairs

Russian Military Intelligence: Background and Issues for Congress

Following Russia's occupation of Ukraine's Crimea region and invasion of eastern Ukraine in 2014, many observers have linked Russia to additional malicious acts abroad. U.S. and European officials and analysts have accused Russia of, among other things, interfering in U.S. elections in 2016; attempting a coup in Montenegro in 2016; conducting cyberattacks against the World Anti-Doping Agency and the Organization for the Prohibition of Chemical Weapons in 2016 and 2018, respectively; attempting to assassinate Russian intelligence defector Sergei Skripal in the United Kingdom in 2018; and offering "bounties" to Taliban-linked fighters to attack U.S. personnel in Afghanistan. Implicated in all these activities is Russia's military intelligence agency, the Main Directorate of the General Staff (GU), also known as the GRU.

The United States has indicted GRU officers and designated the GRU for sanctions in response to Russia's invasion of Ukraine, cybercrimes, and election interference. The Department of Justice has indicted GRU officers for cyber-related offenses against the World Anti-Doping Agency and the Organization for the Prohibition of Chemical Weapons, NotPetya malware attacks in 2017, various cyberattacks against the 2018 Olympics, and interference in the 2016 U.S. elections. The GRU as an agency has been designated for sanctions under Executive Order 13694, as amended, and Section 224 of the Countering Russian Influence in Europe and Eurasia Act of 2017 (CRIEEA; P.L. 115-44/H.R. 3364 Countering America's Adversaries Through Sanctions Act [CAATSA], Title II).

The GRU is a large, expansive organization under the command of Russia's Ministry of Defense and Defense Minister Sergei Shoigu. Headed since 2018 by Admiral Igor Kostyukov, the GRU plays an important role in Russia's foreign and national security policies. As an arm of the military, the GRU is responsible for all levels of military intelligence, from tactical to strategic. The GRU commands Russia's *spetsnaz* (special forces) brigades, which conduct battlefield reconnaissance, raiding, and sabotage missions, in addition to training and overseeing local proxies or mercenary units. Additionally, the GRU conducts traditional intelligence missions through the recruitment and collection of human, signals, and electronic assets. Beyond its traditional combat- and intelligence-related roles, the GRU conducts extensive cyber, disinformation, propaganda, and assassination operations. These operations are often aggressive and brazen, leading to publicity and the exposure of GRU culpability.

Congress and the executive branch continue to consider responses and countermeasures to malicious Russian activities. Because the GRU continues to conduct cyberattacks, election interference, assassinations, and disinformation, understanding the agency's structure and the position it occupies in Russian foreign and security policy can help identify what the GRU is capable of and why it conducts particular operations. Understanding the GRU also offers insight into Russia's wider use of cyber, disinformation, and influence operations and can inform broader discussions of potential U.S. responses and countermeasures.

This report addresses Russian military intelligence, including organizational structure and activities, and related U.S. policy. For further background on Russia, see CRS Report R46761, *Russia: Foreign Policy and U.S. Relations*, by Andrew S. Bowen and Cory Welt; CRS In Focus IF11718, *Russian Cyber Units*, by Andrew S. Bowen; CRS Report R46518, *Russia: Domestic Politics and Economy*, by Cory Welt and Rebecca M. Nelson; CRS In Focus IF11625, *Russian Armed Forces: Military Doctrine and Strategy*, by Andrew S. Bowen; CRS In Focus IF11589, *Russian Armed Forces: Capabilities*, by Andrew S. Bowen; and CRS Report R45415, *U.S. Sanctions on Russia*, coordinated by Cory Welt.

Contents

Contacts

Introduction

Russia's military intelligence agency is a large, expansive, and powerful organization responsible for the collection of foreign intelligence and the operation of Russia's military special forces (*spetsnaz*) units. Since 2010, its official title has been the Main Directorate (*Glavnoye upravleniye*) of the General Staff, formally referred to in abbreviated form as the GU, although commonly referred to as the GRU (*Glavnoye razvedyvatel'noye upravleniye*, or Main Intelligence Directorate).[1]

Due to its operations and responsibilities, the GRU is one of the most well-known of Russia's intelligence agencies. It plays a large role in Russian foreign and security policy. By understanding the GRU and its operations, Members of Congress may gain greater insight into the conduct of Russian foreign and security policy, including the use of disinformation, propaganda, and cyber strategies.

In recent years, reports have linked the GRU to some of Russia's most aggressive and public intelligence operations. Reportedly, the GRU played a key role in Russia's occupation of Ukraine's Crimea region and invasion of eastern Ukraine, the attempted assassination of former Russian intelligence officer Sergei Skripal in the United Kingdom (UK), interference in the 2016 U.S. presidential elections, disinformation and propaganda operations, and some of the world's most damaging cyberattacks. The GRU operates both as an intelligence agency, collecting human, cyber, and signals intelligence, and as a military organization responsible for battlefield reconnaissance and the operation of Russia's main *spetsnaz* forces.[2]

Analysts note the GRU has a distinct organizational identity due to its dual status as an intelligence and military organization. Additionally, from its inception, the GRU has competed with other Russian security organs for resources and responsibilities. Other intelligence agencies have continually sought to take over the GRU's missions and responsibilities, leading to intense competition and often a duplication of efforts. Analysts and researchers have noted that the GRU's unique organizational culture and competition with other agencies may factor into its willingness to conduct aggressive and often reckless operations, as a way to justify the GRU's utility to Russia's political leadership.[3]

This report focuses on the GRU's origins, missions, documented or reported operations, and related U.S. policy. It first addresses the GRU's history and background to provide context for understanding its organizational mindset and traditional responsibilities. It then examines the GRU's organizational structure; analyzes the GRU's various missions, including intelligence collection, control of *spetsnaz* units, and cyber capabilities and operations; and addresses related U.S. policy and congressional action. The report concludes with a brief assessment of the GRU's future outlook.

[1] This report uses the abbreviation *GRU*.

[2] *Spetsnaz* in this report refers to the military spetsnaz brigades under GRU command. There are numerous other elite units in Russia often referred to as *spetsnaz* that are not under the control of the GRU.

[3] Mark Galeotti, "Putin's Hydra: Inside Russia's Intelligence Services," *European Council on Foreign Relations*, May 11, 2016, p. 2

Background and History

Russian military intelligence traces its lineage to 1918 under Russian leader Leon Trotsky.[4] Similar to civilian intelligence agencies created by the Bolsheviks (Communists) during the Russian Civil War, Russian military intelligence initially focused on protecting the regime from "counterrevolutionaries" from abroad. First known as the Registration Department (*Razvedupravlenie*, or *Razvedupr*), Russia's military intelligence soon became known as the Fourth Directorate of the Red Army. It gradually expanded its focus to collecting intelligence abroad and supporting Soviet foreign policy.[5] Its activities included running human intelligence assets, conducting propaganda and disinformation operations, and conducting sabotage operations (also known as *active operations*). During the 1920s and 1930s, the Fourth Directorate developed a reputation for aggressive and often careless operations, which led to numerous diplomatic incidents.

The Fourth Department also developed rivalries with other Soviet intelligence agencies, competing for missions, influence, and responsibilities.[6] For instance, Felix Dzerzhinsky, founder of the *Cheka*, a predecessor to the Committee for State Security (KGB), complained about "the irresponsible activities of the *Razvedupr*, dragging us into conflict with neighboring states."[7] The Fourth Directorate's close connection with the *Comintern* (Communist International), through which it conducted many activities and recruited agents, created friction with the Soviet Union's People's Commissariat for Foreign Affairs due to blowback from exposed operations and activities.[8]

Due to continued infighting and the need to streamline operations, the Main Intelligence Directorate of the General Staff (GRU) was created in 1942. During World War II, the GRU supervised sabotage, resistance, and guerrilla actions against the Nazis.[9] After the war, the GRU was placed under the direct command of the General Staff and, alongside the KGB's First Directorate, given responsibility for conducting both legal (under diplomatic cover) and illegal/nonofficial (without diplomatic cover) intelligence operations abroad, primarily focused on militarily relevant intelligence (such as acquiring Western technology and assessing strategic military capabilities).[10]

[4] Trotsky was a key leader of the Bolsheviks (the precursor to the Communist Party of the Soviet Union) and member of the Bolshevik (later Communist) Politburo. He also was the People's Commissar of Military and Naval Affairs from 1918 to 1925, and he was responsible for the creation of the Red Army. Raymond W. Leonard, "Studying the Kremlin's Secret Soldiers: A Historiographical Essay on the GRU, 1918–1945," *Journal of Military History*, vol. 56, no. 3 (1992), pp. 403–422; Jonathan Haslam, *Near and Distant Neighbors: A New History of Soviet Intelligence* (New York: Farrar, Straus and Giroux, 2015).

[5] Raymond W. Leonard, *Secret Soldiers of the Revolution: Soviet Military Intelligence, 1918-1933* (Westport, CT: Greenwood Press, 1999).

[6] Leonard, *Secret Soldiers*, pp. 7, 17-19.

[7] The full name of the Cheka was the All-Russian Extraordinary Commission for Combating Counter-Revolution and Sabotage. Haslam, *Near and Distant Neighbors*, p. 29.

[8] The Comintern (Communist International) was a Soviet organization dedicated to advancing Communism globally through the coordination of national communist parties. Owen Matthews, *An Impeccable Spy: Richard Sorge, Stalin's Master Agent* (London: Bloomsbury, 2019).

[9] David M. Glantz, *Soviet Military Intelligence in War* (New York: Frank Cass, 1990).

[10] Raymond L. Garthoff, *Soviet Leaders and Intelligence: Assessing the American Adversary During the Cold War* (Washington D.C.: Georgetown University Press, 2015), pp. 13-15, 46.

In addition, the GRU was responsible for the creation of special forces units known as *spetsnaz* (*voiska spetsialnogo naznacheniya*). Growing out of the Soviet experience during the Russian Civil War, both the NKVD (a KGB precursor) and the GRU trained units in sabotage and guerrilla-style operations, also known as *razvedchiki* (literally, "scouts").[11] This experience proved invaluable during World War II, when the Soviets used partisan formations extensively. In 1950, these forces became the *spetsnaz*, created to fulfill long-range battlefield reconnaissance and sabotage operations, specifically targeting NATO command and control and nuclear weapons.

Throughout the Cold War, the GRU *spetsnaz* gained extensive experience supporting, training, and supervising local allied forces in numerous conflicts.[12] *Spetsnaz* units played key roles in the Soviet invasions of Hungary in 1956 and Czechoslovakia in 1968. They also gained significant experience and notoriety during the Soviet invasion of Afghanistan (1979-1989). *Spetsnaz* units conducted rapid-response, interdiction, and ambush operations and were involved in the 1979 assassination of Afghanistan's leader, Hafizullah Amin.[13]

After the dissolution of the Soviet Union in 1991, the GRU, like the Ministry of Defense and other intelligence services, struggled for financial and political support in Russia. As the KGB was carved up into various organizations, the GRU fought for relevance and to prevent its missions from being given to newly emerging security organizations.[14] Despite massive personnel losses and budget cuts, the GRU retained its foreign intelligence presence and its independence under the General Staff.[15] At the same time, GRU *spetsnaz* forces suffered heavily from budget cuts and the lack of a clearly defined need, since conflict with NATO became unlikely. Many officers saw better prospects in the Airborne Forces (VDV), which positioned itself as a more capable and elite rapid-response unit. Some former *spetsnaz* allegedly worked for organized crime.[16] In wars against Russia's breakaway region of Chechnya in the 1990s and 2000s, the GRU and *spetsnaz* units participated in direct combat and managed local allied Chechen forces.[17]

Organizational Structure

Russian military intelligence headquarters is located in the Khoroshevsky District in Moscow.[18] Currently, the GRU is headed by Admiral Igor Kostyukov.[19] Under the command of the General

[11] Mark Galeotti, *Spetsnaz: Russia's Special Forces* (Oxford: Osprey Publishing, 2015), pp. 8-11.

[12] Mark Galeotti, "Spetsnaz: Operational Intelligence, Political Warfare, and Battlefield Role," *Marshall Center Security Insights*, no. 46 (February 2020).

[13] Galeotti, *Spetsnaz: Russia's Special Forces,* pp. 14-28.

[14] Amy Knight, *Spies Without Cloaks: The KGB's Successors* (Princeton: Princeton University Press, 1996), pp. 119-120; Andrei Soldatov and Irina Borogan, *The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB* (New York: Public Affairs, 2010), pp. 14, 21.

[15] Amy Knight, "This Russian Spy Agency Is in the Middle of Everything," *Daily Beast,* August 10, 2018.

[16] Graham Turbiville, "Organized Crime and the Russian Armed Forces," *Transnational Organized Crime* vol. 1, no. 4 (1995), pp. 57-104; Mark Galeotti, "The Criminalisation of Russian State Security," *Global Crime*, vol. 7, no. 3-4 (2006), p. 472; Mark Galeotti, *The Vory: Russia's Super Mafia* (New Haven: Yale University Press, 2018), pp. 207-208.

[17] Galeotti, *Spetsnaz: Russia's Special Forces,* pp. 31-35; Mark Kramer, "The Perils of Counterinsurgency: Russia's War in Chechnya," *International Security*, vol. 29, no. 3 (2004/05), pp. 14, 18; Olga Oliker, *Russia's Chechen Wars 1994-2000: Lessons from Urban Combat* (Santa Monica: RAND, 2001).

[18] President of Russia, "President Vladimir Putin visited the new headquarters of the Russian Armed Forces General Staff Chief Intelligence Directorate (GRU)," press release, November 8, 2006, at http://en.kremlin.ru/events/president/news/36598.

[19] TASS, "First Naval Officer Nominated to Head Russia's GRU," November 22, 2018; Tatiana Stanovaya, "New

Staff and Defense Minister Sergei Shoigu, the GRU maintains significant operational autonomy and can brief Russian President Vladimir Putin directly.[20]

GRU Organizational Structure

The GRU is divided into 15 directorates—4 regional and 11 mission-specific. Within the directorates are multiple sub-directorates or individual units. Individual GRU units are identified by their military postbox numbers. For example, the GRU's cyber capabilities are located within the Sixth Directorate and include Unit 26165 and Unit 74455.

The GRU's true structure is a closely guarded secret. The structure described below is based on publicly available reports and documents.

Regional Directorates (4)	Mission-Specific Directorates (11)
(1) First Directorate: European Union	(5) Fifth Directorate: Operational Intelligence
(2) Second Directorate: North and South America, United Kingdom, Australia, New Zealand	(6) Sixth Directorate: Electronic/Signals Intelligence
(3) Third Directorate: Asia	(7) Seventh Directorate: NATO
(4) Fourth Directorate: Africa	(8) Eighth Directorate: Spetsnaz
	(9) Ninth Directorate: Military Technology
	(10) Tenth Directorate: Military Economy
	(11) Eleventh Directorate: Strategic Doctrine
	(12) Twelfth Directorate: Information Operations
	(13) Space Intelligence Directorate
	(14) Operational and Technical Directorate
	(15) External Relations Department

Sources: Congressional Research Service (CRS) interview with Mark Galeotti; Viktor Suvorov, *Inside the Aquarium: The Making of a Top Soviet Spy* (New York: MacMillan, 1985); Stanislav Lekarev, "Two Types of Russian Intelligence Are Unified," *Nezavisimaya Gazeta*, August 31, 2001; Daniil Turovsky, "What Is the GRU? Who Gets Recruited to Be a Spy? Why Are They Exposed So Often?," *Meduza*, November 6, 2018; Mark Urban, *The Skripal Files: The Life and Near Death of a Russian Spy* (New York: Henry Holt and Company, 2018); RFE/RL, "On the Trail of the 12 Indicted Russian Intelligence Officers," July 19, 2020.

Today, Russian military intelligence is responsible for the collection of foreign intelligence using a full range of methods and sources (human, cyber, satellite, and signals intelligence), intelligence analysis, and battlefield reconnaissance and sabotage missions through its *spetsnaz* units. This means the GRU oversees both strategic- and tactical-level intelligence collection.[21] The GRU has increased its cyber capabilities in recent years (conducting election interference, offensive cyberattacks, and disinformation operations), in addition to its traditional electronic, signals, and radio intelligence capabilities.[22]

Boss, Old Rules," *Riddle*, November 28, 2018.

[20] Galeotti, "Putin's Hydra," p. 2.

[21] Andrew Roth, "How the GRU Spy Agency Targets the West, from Cyberspace to Salisbury," *Guardian*, August 6, 2018; Guy Faulconbridge, "What Is Russia's GRU Military Intelligence Agency?" Reuters, October 5, 2018.

[22] The GRU always had a large signals intelligence collection mission, but its capabilities were increased when it acquired the radio-electronic intelligence capabilities of the now-defunct Federal Agency of Government Communications and Information (FAPSI) in 2003. Gordon Bennett, "FPS and FAPSI—RIP," *Conflict Studies Research Centre*, Occasional Paper no. 96, p. 4.

Due to its dual role, the GRU has extensive capabilities and experience organizing proxy forces and local allies in numerous conflict zones, as well as in conducting assassinations and other targeted attacks. Despite overseeing both intelligence and *spetsnaz* operations, not all GRU officers have *spetsnaz* backgrounds or vice versa.[23] Analysts contend, however, that overseeing both types of operations has led to a risk-acceptant and risk-taking culture, thereby contributing to operations with a higher likelihood of exposure.[24]

Relationship to Other Russian Intelligence Agencies

Russia's intelligence agencies are divided organizationally and across factional and personal lines.[25] Agencies compete with each other for greater responsibilities, budgets, and political influence, often at the expense of other agencies.[26] This competitive environment often contributes to uncoordinated and duplicated intelligence efforts.[27]

The GRU operates alongside the Foreign Intelligence Service (SVR), Federal Security Service (FSB), and Federal Protective Service (FSO).[28] The GRU and the SVR are Russia's primary intelligence agencies responsible for the collection of foreign intelligence.[29] Domestically, the FSB is responsible for counterintelligence. The FSB, however, has sought to gain a greater foreign intelligence role and has significant international operations, especially in Russia's neighboring post-Soviet states.[30] This reportedly has caused significant friction within Russia's intelligence community, especially with the GRU and SVR, which consider foreign intelligence collection their primary responsibility.[31] The FSO operates as an overseer of the various security services, helping to monitor infighting and the accuracy of intelligence reporting. Although the GRU can directly brief the president, it does not have the same level of direct access as the SVR (the primary agency responsible for foreign intelligence), the FSB (the primary agency responsible for domestic security), or the FSO, which controls the Presidential Security Service.[32] Analysts and reporting therefore suggest the GRU's influence is often relative to the ability of its chief to develop personal relationships with Russia's political leadership.[33]

[23] Mark Galeotti, "Special Troops of GRU Will Be Growing Headache for the West," *Raamoprusland*, September 28, 2018.

[24] Galeotti, "Putin's Hydra," p. 2.

[25] Brian D. Taylor, *State Building in Putin's Russia: Policing and Coercion After Communism* (Cambridge: Cambridge University Press, 2011); Tatiana Stanovaya, "Why the Kremlin Can't Keep Its Chekists in Check," *Riddle*, July 25, 2019.

[26] Peter Reddaway, *Russia's Domestic Security Wars: Putin's Use of Divide and Rule Against His Hardline Allies* (London: Palgrave Pivot, 2018); Joss I. Meakins, "Squabbling *Siloviki*: Factionalism Within Russia's Security Services," *International Journal of Intelligence and Counterintelligence*, vol. 31, no. 2 (2018), pp. 235-270.

[27] Mark Galeotti, "The Intelligence and Security Services and Strategic Decision-Making," *Marshall Center Security Insights*, no. 30 (May 2019).

[28] For more on Russia's internal security and law enforcement agencies, see CRS In Focus IF11647, *Russian Law Enforcement and Internal Security Agencies*, by Andrew S. Bowen; Mark Galeotti, "Russian Intelligence and Security Agencies Vie for Central Role," *Jane's Intelligence Review*, August 29, 2018.

[29] The Foreign Intelligence Service (SVR) inherited the Committee for State Security's (KGB's) foreign intelligence operations of its First Main Directorate.

[30] Mark Galeotti, "The Spies Who Love Putin," *Atlantic*, January 17, 2017.

[31] Andrei Soldatov, "Russian Foreign Intelligence Might Be in for a More Prominent Political Role," *Raamoprusland*, May 24, 2019.

[32] Mark Galeotti, "Spooks in the Kremlin," *Foreign Policy*, April 27, 2019.

[33] Galeotti, "Spooks in the Kremlin."

2008 Georgian War to Present Day

In 2008, Russia fought a war with Georgia to prevent Georgia from asserting control over its breakaway region of South Ossetia.[34] While ultimately victorious, the Russian military performed poorly, struggling with command-and-control issues, lack of coordination across service branches, and a low level of accurate intelligence on Georgian military forces and capabilities.[35] Low-quality intelligence led to the bombing of empty airfields and military installations, friendly fire incidents, and a misunderstanding of the capabilities and morale of Georgian forces. Analysts assessed that, although intelligence provided by the GRU was inadequate, the *spetsnaz* brigades performed adequately.[36] Overall, Russia's disappointment with its military performance led to a program to modernize and reform the armed forces.[37]

Much of the blame for Russia's military performance was placed on the GRU for providing faulty intelligence.[38] In response, competing security and intelligence agencies, along with other branches of the military, sought to take advantage of the GRU's weakened political position. Due to its large size and expansive mission areas, the GRU suffered from the lack of a clearly defined role in the wake of the Georgian war.[39] In 2009, the GRU head, who had served since 1997, was replaced by his deputy.[40] Media reports alleged there was discussion of downgrading the GRU's status from a Main Directorate to a Directorate.[41] By 2011, the GRU was downsized by over 1,000 officers, with many retiring or transferring to other positions; the size of the GRU's foreign intelligence operations also was reduced.[42] Perhaps most significant were plans for the GRU to lose control of the *spetsnaz* brigades to Russia's military district commanders in 2010.[43]

The GRU's fortunes began to change with the appointment of Igor Sergun as GRU head in 2011.[44] Sergun presided over a revitalization of the GRU's prestige. In contrast to previous GRU heads, analysts reportedly viewed Sergun (who had a background as a defense attaché and an intelligence officer) as a politically astute leader able to lobby for the agency's interests.[45] The GRU and Sergun prioritized the agency's abilities to conduct "active measures," or aggressive

[34] Mikhail Barabanov, Anton Lavrov, and Vyacheslav Tseluiko, *Tanks of August*, ed. Ruslan Pukhov (Moscow: Center for Analysis of Strategies and Technologies, 2010).

[35]Ariel Cohen and Robert E. Hamilton, *The Russian Military and the Georgia War: Lessons and Implications* (Carlisle, PA: Strategic Studies Institute, 2011); Michael Kofman, "Russian Performance in the Russo-Georgian War Revisited," *War On The Rocks*, September 4, 2018.

[36] Cohen and Hamilton, *Russian Military and the Georgia War*; Kofman, "Russian Performance in the Russo-Georgian War Revisited."

[37] For more see CRS In Focus IF11603, *Russian Armed Forces: Military Modernization and Reforms*, by Andrew S. Bowen

[38] Tor Bukkvoll, "Russia's Military Performance in Georgia," *Military Review* vol. 89, no. 6 (2009), pp. 57-62.

[39] Mark Galeotti, "Putin's Secret Weapon," *Foreign Policy*, July 7, 2014.

[40] Mark Galeotti, "Korabelnikov Leaves Russian Military Intelligence," *In Moscow's Shadows*, April 26, 2009.

[41] This would represent a serious demotion that would limit the GRU's influence, autonomy, and political importance. It would have limited the GRU's direct access to the president and increased the General Staff's direct control.

[42] Brian Whitmore, "Resetting the Siloviki," *RFE/RL Power Vertical*, October 21, 2011; Denis Telmanov, "GRU Chief to be Fired Upon Leaving Hospital," *Izvestia*, September 27, 2011.

[43] Roger McDermott, "Bat or Mouse? The Strange Case of Reforming Spetsnaz," *Eurasia Daily Monitor*, November 2, 2010.

[44] Denis Telmanov, "GRU Headed by Igor Sergun," *Izvestia*, December 26, 2011.

[45] Roger McDermott, "Russian Military Intelligence: Shaken but Not Stirred," *Eurasia Daily Monitor*, February 7, 2012; Mark Galeotti, "We Don't Know What to Call Russian Military Intelligence and That May Be a Problem," *War On The Rocks*, January 19, 2016; Galeotti, "Putin's Hydra," p. 13.

operations such as assassinations, controlling proxy forces, political subversion, and eventually cyber operations.[46]The Russian military also abandoned plans in 2013 to move *spetsnaz* to the control of the ground forces due to a combination of bureaucratic hurdles and resistance.[47]

The GRU demonstrated its importance during Russia's 2014 occupation of Ukraine's Crimea region and invasion of eastern Ukraine.[48] Russia's Crimea operation relied heavily upon GRU intelligence and *spetsnaz* forces to seize strategic points across the peninsula.[49] The GRU's success continued in the Donetsk and Luhansk regions of eastern Ukraine by creating, supervising, and monitoring the numerous proxy and local rebel forces fighting against the Ukrainian government.[50]

The GRU's experience in managing proxy forces continued to prove useful as Russia intervened in Syria.[51] *Spetsnaz* proved instrumental in training, advising, and coordinating air strikes with Syrian government and pro-government militia forces.[52] The traditional *spetsnaz* mission of battlefield reconnaissance was particularly important for Russia's air campaign, which helped the Syrian government retake crucial areas and urban centers.[53]

As the GRU was reasserting its role and missions, it began to invest in cyber capabilities.[54] Development of these types of capabilities would allow the GRU to operate in an environment marked by confusion and low attribution.[55] Contested environments, such as in Ukraine and the

[46] Galeotti, "Putin's Hydra," p. 7.

[47] This also roughly coincided with the reversal of many of the initial military reforms and the removal of Anatoly Serdyukov, Minister of Defense, and General Nikolai Makarov, Chief of the General Staff, who initiated the wide-ranging reform program. Mark Galeotti, "The Rising Influence of Russian Special Forces," *Jane's Intelligence Review*, November 24, 2014; Alexander Golts, "Reform: The End of the First Phase – Will There Be a Second?" *Journal of Slavic Military Studies*, vol. 27, no. 1 (2014), pp. 131-146.

[48] Charles K. Bartles and Roger N. McDermott, "Russia's Military Operation in Crimea: Road Testing Rapid Reaction Capabilities," *Problems of Post-Communism*, vol. 61, no. 6 (2014), pp. 46-63; Galeotti, "Putin's Secret Weapon"; Michael Kofman et al., *Lessons From Russia's Operations in Crimea and Eastern Ukraine*, RAND, 2014.

[49] Anton Lavrov, "Russian Again: The Military Operation for Crimea," in *Brothers Armed: Military Aspects of the Crisis in Ukraine*, ed. Colby Howard and Ruslan Pukhov, vol. 2 (Minneapolis, MN: East View Press, 2015**)**, pp. 157-186.

[50] Sam Jones, "Photos and Roses for GRU's 'Spetsnaz' Casualties," *Financial Times*, August 8, 2014; Roger McDermott, "Russian Spetsnaz Personnel Detained in Ukraine," *Eurasia Daily Monitor*, May 20, 2015; Tor Bukkvoll, "Russian Special Operations Forces in Crimea and Donbas," *Parameters*, vol. 46., no. 2 (2016), pp. 18-20; Tim Ripley and Mark Galeotti, "Donbass Conflict Offers Pointers for Future Russian Military Action," *Jane's Intelligence Review*, June 18, 2019.

[51] Sarah Fainberg, "Russian Spetsnaz, Contractors, and Volunteers in the Syrian Conflict," *Russie.nei Visions*, IFRI, December 2017; Brian Katz and Nicholas Harrington, "The Military Campaign," in *Moscow's War in Syria*, ed. Seth G. Jones (CSIS, 2020), pp. 18-40.

[52] Mark Galeotti, "The Three Faces of Russian Spetsnaz in Syria," *War on the Rocks*, March 21, 2016; Thomas Gibbons-Neff, "How Russian Special Forces Are Shaping the Fight in Syria," *Washington Post*, March 29, 2016.

[53] Anton Lavrov, "Russian Aerial Operations in the Syrian War," in *Russia's War in Syria: Assessing Russian Military Capabilities and Lessons Learned*, ed. Robert E. Hamilton, Chris Miller, Aaron Stein (Philadelphia, PA: Foreign Policy Research Institute, 2020), p. 95.

[54] Anton Troianovski and Ellen Nakashima, "How Russia's Military Intelligence Agency Became the Covert Muscle in Putin's Duels with the West," *Washington Post*, December 28, 2018.

[55] Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019), pp. 237-242; Bilyana Lilly and Joe Cheravitch, "The Past, Present, and Future of Russia's Cyber Strategy and Forces," *NATO Cooperative Cyber Defence Centre of Excellence*, 12th International Conference on Cyber Conflict (2020), pp. 140-142.

cyber arena, have provided the GRU another way to justify and demonstrate its importance to the political leadership.[56]

In recent years, several GRU operations were uncovered (see "Attempted Hacking of the Organization for the Prohibition of Chemical Weapons," below), exposing Russian complicity and complicating diplomatic relations.[57] Some analysts question whether these exposures are a result of GRU incompetence and amateurishness.[58] Other analysts suggest competing Russian security agencies may have undermined the GRU's position for their own benefit.[59] The GRU also suffered numerous leadership changes; then-GRU head Sergun died in late 2015 and was replaced by Igor Korobov, who himself died in 2018.[60]

There is no outward indication the GRU has fallen into disfavor, despite these setbacks.[61] At its 100th anniversary celebration in 2018, shortly after the attempted assassination of former GRU intelligence officer Sergei Skripal in the UK, Putin thanked the agency and stated, "As supreme commander, I of course know with no exaggeration about your unique abilities including in conducting special operations."[62] Although it is unclear exactly how Russia's political leadership views the GRU, the agency's operations and publicly available information indicate the GRU remains a valued asset, especially for aggressive and risky operations.

Intelligence Collection

The GRU and the SVR share responsibility for the collection of foreign intelligence.[63] This includes the use of intelligence officers operating both under legal (diplomatic) cover out of Russia's embassies and under illegal or nonofficial (without diplomatic) cover.[64] GRU intelligence officers are trained at the Military Diplomatic Academy of the General Staff.[65] In each embassy, the GRU and the SVR operate individually, with separate command structures.[66]

The GRU nominally focuses on the collection of militarily relevant information, such as the size and capabilities of foreign militaries and decisionmaking, as well as technology acquisition. This focus does not preclude the collection of political intelligence, which is the primary focus of the SVR.[67] However, as analyst Mark Galeotti has opined, "Russian collection operations are not just

[56] Roth, "How the GRU Spy Agency Targets the West, from Cyberspace to Salisbury."

[57] Sarah Rainsford, "Have Russian Spies Lost Their Touch?," BBC, October 6, 2018.

[58] Karina Orlova, "Russia's Intelligence Failures," *American Interest*, October 10, 2018; Luke Harding, "A Chain of Stupidity: The Skripal Case and the Decline of Russia's Spy Agencies," *Guardian*, June 23, 2020.

[59] Tatiana Stanovaya, "GRU Exposure: A Sign of Internal Power Struggles?," *Riddle*, October 16, 2018.

[60] Ivan Nechepurenko, "Igor D. Sergun, Chief of Russian Military Intelligence, Dies at 58," *New York Times*, January 5, 2016; TASS, "Head of Russian Military Intelligence GRU Igor Korobov Dies—Source," November 21, 2018.

[61] Mark Galeotti, "Russia's Military Intelligence Agency Isn't Stupid," *Foreign Policy*, September 6, 2018.

[62] Tom Balmforth, "Putin Praises Skills of GRU Spy Agency Accused of UK Poison Attack," Reuters, November 2, 2018; RFE/RL, "Putin Praises GRU Spy Agency Blamed for Spy Attacks in West," November 3, 2018.

[63] Faulconbridge, "What Is Russia's GRU Military Intelligence Agency?"

[64] Daniil Turovsky, "What Is the GRU? Who Gets Recruited to Be a Spy? Why Are They Exposed So Often?," *Meduza*, November 6, 2018.

[65] Turovsky, "What Is the GRU?"; Richard Framingham, "Career Training Program, GRU Style," Central Intelligence Agency, September 18, 1995, at https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol10no4/html/v10i4a04p_0001.htm.

[66] Mark Urban, *The Skripal Files: The Life and Near Death of a Russian Spy* (New York: Henry Holt and Company, 2018).

[67] Amie Ferris-Rotman and Ellen Nakashima, "Estonia Knows a Lot About Battling Russian Spies, and the West Is

highly active but also extremely professional. Tasking, though, appears less impressive. While the Foreign Intelligence Service and GRU have a strong sense of the military and technical secrets they are meant to uncover, their political objectives are sometimes naive."[68] Analysts contend this tendency may reflect a poor understanding of democratic political systems.

Arrests of GRU agents and assets in recent years illustrate the level of GRU activity. The 2019 annual report of Estonia's Foreign Intelligence Service stated that five GRU assets were uncovered from 2014 to 2018.[69] In 2020, uncovered GRU assets included French and Austrian military officers, as well as a former U.S. Special Forces officer.[70] In late December 2020, Bulgaria expelled a Russian military attaché over espionage, the sixth expulsion of Russian diplomats since October 2019.[71] In March 2021, Bulgarian prosecutors arrested six people for running a Russian spy ring and passing classified information to Russian military intelligence.[72] In April 2021, Italian authorities caught two Russian military intelligence officers accepting classified information from an Italian navy officer.[73]

Spetsnaz

The GRU oversees Russia's *spetsnaz* brigades.[74] *Spetsnaz* are an elite light infantry force designed to conduct battlefield reconnaissance, sabotage, and small unit direct action missions. They are organized into seven regular Independent Special Designation Brigades, a naval *spetsnaz* unit for each of Russia's fleets, a brigade used for testing new weapons and equipment, and an independent regiment in occupied Crimea. Despite efforts to professionalize the force, units are still composed of some conscripts.

Paying Attention," *Washington Post*, November 1, 2018.

[68] Galeotti, "Putin's Hydra," p. 7.

[69] Michael Weiss, "The Hero Who Betrayed His Country," *Atlantic*, June 26, 2019; Estonian Foreign Intelligence Service, *International Security and Estonia*, Annual Report (2019), pp. 45-46.

[70] RFE/RL, "Retired Austrian Army Colonel Found Guilty of Spying for Russia," June 10, 2020; U. S. Department of Justice, "Former Army Special Forces Officer Charged in Russian Espionage Conspiracy," press release, August 21, 2020; Victor Mallet, "French Military Officer Held on Suspicion of Spying," *Financial Times*, August 30, 2020.

[71] Reuters, "Bulgaria Expels Russian Diplomat Over Espionage," December 18, 2020; Vessela Sergueva, "Bulgaria Breaks Up Suspected Russia-Linked Spy Ring," AFP, March 19, 2021.

[72] Georgi Kantchev, "How an Alleged Russian Spy Ring Used Cold War Tactics," *Wall Street Journal*, March 25, 2021.

[73] Alvise Armellini, "Italy Expels Russians After Spies 'Caught Red-Handed,'" AFP, April 2, 2021.

[74] They are nominally on loan to the Military District Commanders across Russia.

Spetsnaz

Spetsnaz operate as Russia's primary military reconnaissance force. They are similar in structure, mission, and training to U.S. Army Rangers. The below structure is recreated from publicly available sources.

***Spetsnaz* Units**

- 2nd Brigade *(Promezhitsa, Pskov)*
- 3rd Guards Brigade *(Tolyatti)*
- 10th Brigade *(Molkino)*
- 14th Brigade *(Usurisk)*
- 16th Brigade *(Chuchkogo/Tambov, Moscow)*
- 22nd Guards Brigade *(Aksai/Stepnoi)*
- 24th Brigade *(Irkutsk)*
- 100th Brigade *(Mozdok)*
- 25th Independent Spetsnaz Regiment *(Stavropol)*

Naval *Spetsnaz*

- 42nd Independent Naval Reconnaissance Spetsnaz Point *(Vladivostok, Pacific Fleet)*
- 420th Independent Naval Reconnaissance Spetsnaz Point *(Severomorsk, Northern Fleet)*
- 431st Independent Naval Reconnaissance Spetsnaz Point (*Sevastopol, Black Sea Fleet*)
- 561st Independent Naval Reconnaissance Spetsnaz Point (*Parusnoe, Kaliningrad, Baltic Fleet)*

Sources: Mark Galeotti, "Spetsnaz: Operational Intelligence, Political Warfare, and Battlefield Role," *Marshall Center*, Security Insights no. 46 (February 2020); *Russian Military Capability in a Ten Year Perspective-2019*, eds. Fredrik Westerlund and Susanne Oxenstierna (Stockholm: Swedish Defence Research Agency FOI, 2019).

Supervising Proxy Forces

The GRU and *spetsnaz* have gained significant experience creating and managing local allied proxy forces. Often these proxy forces are composed of organized criminals, warlords, or former rebels. Most often, *spetsnaz* operators act as overseers and trainers, helping to create new units directly subordinated to the GRU. This gives the GRU greater direct control over local proxies, which helps limit the influence of competing security agencies and increases leverage over local politicians.[75]

During Russia's Second Chechen War (1999-2009), the GRU—along with other agencies, such as the FSB—managed several local pro-Russian Chechen units, which proved effective against Chechen rebels.[76] The most famous units were Special Battalions Zapad and Vostok, which also participated in Russia's 2008 war against Georgia.[77]

During Russia's invasion of Ukraine in 2014, the GRU relied heavily upon its experience managing proxies. During the course of the conflict, media reporting documented the presence of the Vostok Battalion, reportedly reconstituted after being demobilized in 2008, and identified GRU officer Oleg Ivannikov as allegedly responsible for transporting the anti-aircraft system that shot down Malaysian Airlines Flight 17 in 2014.[78] Ukraine also was used as a testing ground for

[75] Other Russian security and intelligence agencies also create their own local units to compete for influence and control.

[76] Emil Souleimanov, "An Ethnography of Counterinsurgency: Kadyrovtsy and Russia's Policy of Chechenization," *Post-Soviet Affairs*, vol. 31, no. 2 (2015), pp. 91-114.

[77] Tomas Smid and Miroslav Mares, "Kadyrovtsy: Russia's Counterinsurgency Strategy and the Wars of Paramilitary Clans," *Journal of Strategic Studies*, vol. 38, no. 5 (2015), pp. 650-677.

[78] Claire Bigg, "Vostok Battalion, a Powerful New Player in Eastern Ukraine," RFE/RL, May 30, 2014; Andrew Roth, "A Separatist Militia in Ukraine with Russian Fighters Holds a Key," *New York Times*, June 4, 2014; Bellingcat, "MH17 - Russian GRU Commander 'Orion' Identified as Oleg Ivannikov," May 25, 2018.

Russian private military companies, including the Wagner Group, which reportedly was closely tied to the GRU.[79]

Spetsnaz also played a key role in Russia's intervention in Syria.[80] *Spetznaz* forces conducted battlefield reconnaissance and acted as trainers and advisers for the Syrian army and various pro-government militia forces, such as the 5th Assault Corps.[81]

Assassinations and Targeted Attacks

The GRU's military capabilities have enabled it to carry out targeted attacks abroad. The GRU is implicated in numerous attempted and successful assassinations or targeted attacks (see "Targeted Overseas Attacks Linked to GRU Since 2014: Role of Unit 29155," below). Some of these attacks were uncovered due to careless or lackluster spycraft, leading to accusations of incompetence on the part of the GRU.[82] Some analysts, however, contend that the intent behind some targeted attacks is to send a message rather than to hide complicity.[83] If so, exposure is not a failure if the attack succeeds in conveying Russia's ability and willingness to carry out targeted attacks.[84]

One of the GRU's most notorious and high-profile assassinations occurred in 2004; former Chechen separatist president Zelimkhan Yandarbiyev and his 13-year-old son were killed in a car bomb attack while living in exile in Qatar.[85] Eventually, Qatar convicted two Russian agents of his murder, while a third was released due to his status as first secretary of the Russian Embassy, with diplomatic immunity.[86] The men reportedly were GRU agents. They were repatriated to Russia to serve out their sentence but disappeared upon their return.[87]

Targeted Overseas Attacks Linked to GRU Since 2014: Role of Unit 29155

According to information compiled from multiple media outlets, Unit 29155 is an elite GRU unit that conducts sensitive foreign operations, including assassinations and targeted attacks.[88] Unit 29155 is reportedly connected to Russia's elite Special Operations Forces Command headquarters unit, based in Senezh, outside of Moscow.[89] The reported head of Unit 29155 is Major General

[79] For more information, see CRS In Focus IF11650, *Russian Private Military Companies (PMCs)*, by Andrew S. Bowen.

[80] Anton Mardasov, "What Are Russian Special Operations Forces Doing in Idlib?," *Al Jazeera*, August 29, 2019.

[81] Gregory Waters, "The Lion and the Eagle: The Syrian Arab Army's Destruction and Rebirth," *Middle East Institute*, July 18, 20919; Anton Lavrov, "The Efficiency of the Syrian Armed Forces: An Analysis of Russian Assistance," *Carnegie Middle East Center*, March 26, 2020.

[82] Bellingcat, "305 Car Registrations May Point to Massive GRU Security Breach," October 4, 2018.

[83] David V. Gioe, Michael S. Goodman, and David S. Frey, "Unforgiven: Russian Intelligence Vengeance as Political Theater and Strategic Messaging," *Intelligence and National Security*, vol. 34, no. 4 (2019), pp. 561-575.

[84] Galeotti, "Russia's Military Intelligence Agency Isn't Stupid."

[85] Nick Paton Walsh, "Top Chechen Separatist Dies in Qatar Bomb Blast," *Guardian*, February 13, 2002.

[86] Steven Lee Myers, "Qatar Court Convicts 2 Russians in Top Chechen's Death," *New York Times*, July 1, 2004.

[87] Sarah Rainsford, "Convicted Russia Agents 'Missing,'" BBC, February 17, 2005; Soldatov and Borogan, *The New Nobility*, pp. 193-200.

[88] Michael Schwirtz, "Top Secret Russian Unit Seeks to Destabilize Europe, Security Officials Say," *New York Times*, October 8, 2019; Bellingcat, "Skripal Poisoner Attended GRU Commander Family Wedding," October 14, 2019.

[89] RFE/RL, "On the Trail of the 12 Indicted Russian Intelligence Officers," July 29, 2018. For more on the Special Operations Forces Command, see Roger McDermott, "Russia's Special Operations Forces Command and the Strategy of Limited Actions," *Eurasia Daily Monitor*, May 21, 2019.

Andrey Averyanov.[90] Anatoliy Chepiga—a suspected attacker in the 2018 poisoning of Sergei Skripal and his daughter in the UK—was photographed at the wedding of Averyanov's daughter in 2017.[91] Many operatives of Unit 29155 also appear to have backgrounds in GRU *spetsnaz* brigades—including unit commander Averyanov. Further information supporting the unit's operational nature is its reported headquarters at the 161st Special Purpose Specialist Training Center, a *spetsnaz* training facility.[92]

In recent years, prosecutors and journalists have linked Unit 29155 to numerous malign activities across Europe. Such activities include Russia's invasion and occupation of Ukraine's Crimea region in 2014; the poisonings of Bulgarian arms dealer Emilian Gebrev in 2015; a coup attempt in 2016 to overthrow and replace a pro-Western prime minister in Montenegro, potentially to prevent the country from joining NATO; and the poisoning of Russian intelligence defector Sergei Skripal in 2018.[93]

In addition, Unit 29155 operatives were traced to Switzerland around the time other GRU units hacked the World Anti-Doping Agency and planned hacks on the Organization for the Prohibition of Chemical Weapons (OPCW), which were investigating state-sponsored doping in sports and Russia's use of chemical weapons, respectively.[94] Spain also has opened an investigation of travel by known Unit 29155 operative Denis Sergeev to Barcelona in 2017 around the time Catalan separatists organized an illegal referendum on independence.[95]

In 2019, French newspaper *Le Monde* reported that European intelligence agencies had tracked GRU operatives from Unit 29155 who appeared to be using France's Haute-Savoie region in the Alps as a base to conduct operations.[96]

In June 2020, media organizations reported that U.S. intelligence officials had concluded GRU agents had offered payments to Taliban-linked militants to attack U.S. and other international

[90] Reportedly, Averyanov and the two suspected assassins of Sergei Skripal were awarded Russia's highest medal—Hero of Russia. Bellingcat, "The Dreadful Eight: GRU's Unit 29155 and the 2015 Poisoning of Emilian Gebrev," November 23, 2019; Bellingcat, "An Officer and a Diplomat: The Strange Case of the GRU Spy with a Red Notice," February 25, 2020.

[91] *BBC News*, "Russian Spy Poisoning: Woman 'Identifies' Suspect as Anatoliy Chepiga," September 29, 2018; Bellingcat, "Skripal Poisoner Attended GRU Commander Family Wedding," October 14, 2019.

[92] Schwirtz, "Top Secret Russian Unit Seeks to Destabilize Europe."

[93] For more on the Skripal poisoning and U.S. sanctions imposed in response, see CRS In Focus IF10962, *Russia, the Skripal Poisoning, and U.S. Sanctions*, by Dianne E. Rennack and Cory Welt; David Bond, Henry Mance, and Henry Foy, "UK Blames Russian Military Intelligence Agents for Skripal Attack," *Financial Times*, September 5, 2018; Crown Prosecution Service, "CPS Statement – Salisbury," September 5, 2018; Bellingcat, "The GRU Globetrotters: Mission London," June 28, 2019; Michael Schwirtz, "How a Poisoning in Bulgaria Exposed Russian Assassins in Europe," *New York Times*, December 22, 2019; Shaun Walker, "Alleged Russian Spies Sentenced to Jail over Montenegro Coup Plot," *Guardian*, May 9, 2019; RFE/RL, "Bulgaria Charges Three Russians In Absentia Over Attempted Murders in 2015," January 23, 2020; RFE/RL, "Poisons, Patents, Phone Logs: Records Reveal Russian Scientists' Ties to Military Intelligence," October 23, 2020; Bellingcat, "Russia's Clandestine Chemical Weapons Programme and the GRU's Unit 29155," October 23, 2020.

[94] U.S. Department of Justice, "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," press release, October 4, 2018; Bellingcat, "GRU Globetrotters 2: The Spies Who Loved Switzerland," July 6, 2019.

[95] Oscar Lopez-Fonseca, Lucia Abellan, Maria R. Sahuquillo, "Western Intelligence Services Tracked Russian Spy in Catalonia," *El Pais*, November 22, 2019.

[96] See Ken Dilanian and Michele Neubert, "Russian Agents Planned Hit from Assassins' Lairs in French Alps, Say Intel Officials," *NBC News*, December 5, 2019; Alla Hurska, "Europe Ensnared in a Web of Russian Spies," *Eurasia Daily Monitor*, December 11, 2019 (citing *Le Monde*, "La Haute-Savoie camp de base d'espions russes specialises dans les assassinats cibles," December 4, 2019, in French).

forces in Afghanistan. Reportedly, U.S. intelligence sources believed GRU Unit 29155 was responsible for facilitating these payments.[97] U.S. intelligence agencies reportedly differed in their level of confidence concerning the accuracy of specific "bounty" payments and the direct role of the Kremlin in authorizing payments, but the agencies reportedly shared "high confidence" in the existence of "strong ties ... between Russian operatives and the Afghan network where the bounty claims arose."[98]

In April 2021, Czech authorities blamed Unit 29155 for a series of previously unexplained explosions at arms depots in 2014, which killed two people.[99] In response, Czech authorities expelled 18 Russian diplomats; Russia responded by expelling 20 Czech diplomats.[100] Ultimately, Czech authorities expelled over 70 diplomats to bring the traditionally large Russian diplomatic mission to Prague in line with the Czech mission in Moscow.[101] Media reporting alleged the arms belonged to Bulgarian arms dealer Emilian Gebrev, who reportedly survived poisoning attempts by Unit 29155 in 2015 and was planning to ship the ammunition to Ukraine at the time of the explosions.[102] Soon after the revelations, Bulgarian prosecutors announced investigations into a series of unexplained explosions at several ammunition depots inside Bulgaria.[103]

In addition to the GRU and Unit 29155, Russia's other intelligence services reportedly operate clandestine teams for sensitive operations abroad. The FSB controls Russia's elite antiterrorist teams, Alpha and Vympel, located within the FSB's Special Purpose Center.[104] Alpha is Russia's primary counterterrorist force. Vympel is responsible for external operations, including sabotage, alleged assassinations, and covert surveillance. Vympel reportedly is linked to the 2019 daytime assassination of former Chechen military commander Zelimkhan Khangoshvili in Berlin.[105] The SVR also reportedly has an elite operational unit known as Zaslon; little public information is available about the unit, although its presence was reportedly documented in Syria.[106]

[97] Charlie Savage, Eric Schmitt and Michael Schwirtz, "Russia Secretly Offered Afghan Militants Bounties to Kill U.S. Troops, Intelligence Says," *New York Times*, June 26, 2020; Charlie Savage et al., "Suspicions of Russian Bounties Were Bolstered by Data on Financial Transfers," *New York Times*, June 30, 2020.

[98] Charlie Savage, Eric Schmitt, and Michael Schwirtz, "Russian Spy Team Left Traces That Bolstered CIA's Bounty Judgement," *New York Times*, May 7, 2021.

[99] Mike Eckel, Ivan Bedrov, and Olha Komarova, "A Czech Explosion, Russian Agents, A Bulgarian Arms Dealer: The Recipe for a Major Spy Scandal in Central Europe," RFERL, April 18, 2021; Loveday Morris, Ladka Bauerova, and Robyn Dixon, "Accusations of Spying and Sabotage Plunge Russian-Czech Relations Into the Deep Freeze," *Washington Post*, April 19, 2021.

[100] James Shotter, "Czechs Expel 18 Russian Diplomats over 2014 Explosion," *FT*, April 18, 2021.

[101] Henry Foy, "Russia Expels Seven More European Diplomats," *FT*, April 28, 2021; RFERL, "Dozens of Russian Diplomats Leave Czech Republic amid Strained Relations," May 29, 2021.

[102] Michael Schwirtz, "The Arms Merchant in the Sights of Russia's Elite Assassination Squad," *New York Times*, April 24, 2021.

[103] Boryana Dzhambazova and Michael Schwirtz, "Russian Spy Unit Investigated for Links to Bulgarian Explosions," April 28, 2021.

[104] These units are known officially as Directorate-A and Directorate-V. For more, see Boris Volodarsky, "License to Kill," *Wall Street Journal*, December 20, 2006; Mark Galeotti, *Russian Security and Paramilitary Forces Since 1991* (Oxford: Osprey Publishing, 2013), pp. 35-42.

[105] The Federal Security Service (FSB) also is linked to numerous assassinations of ex-Chechen fighters and Islamists in Turkey. *BBC News*, "Have Russian Hitmen Been Killing with Impunity in Turkey?" December 13, 2016; Bellingcat, "'V' For 'Vympel': FSB's Secretive Department 'V' Behind Assassination of Georgian Asylum Seeker in Germany," February 17, 2020; Bellingcat, "FSB's Magnificent Seven: New Links Between Berlin and Istanbul Assassinations," June 29, 2020.

[106] Galeotti, "The Three Faces of Russian Spetsnaz in Syria."

Cyberespionage and Disinformation Activities

In his 2018 confirmation hearing to head U.S. Cyber Command and the National Security Agency, General Paul K. Nakasone said, "as the most technically advanced potential adversary in cyberspace, Russia is a full-scope cyber actor, employing sophisticated cyber operations tactics, techniques, and procedures against U.S. and foreign military, diplomatic, and commercial targets, as well as science and technology sectors."[107] Most observers believe the GRU is responsible for many of these types of operations.[108]

Since 2008, the GRU has developed significant cyber capabilities, complementing its long-standing experience in conducting psychological and information operations.[109] The development of GRU cyber capabilities coincided with two broader developments in Russian security and military thinking: the role of nonviolent tools in conflict and information warfare. Since the early 2000s, Russian military doctrine has adopted an evolving view of warfare, in which the line between peace and conflict is increasingly blurred and the utility of nonviolent tools is increasingly important. The Russian military understands cyber operations as an effective and relatively cheap tool (in part due to deniability and difficulty in attribution) to undermine, subvert, and manipulate an adversary.[110] Cyber tools have become an increasingly crucial component in Russia's efforts to accomplish a range of tasks in the larger informational struggle between adversaries.[111]

Attempted Hacking of the Organization for the Prohibition of Chemical Weapons

On March 4, 2018, former GRU officer Sergei Skripal and his daughter were exposed to a highly toxic and potentially lethal chemical weapon agent in Salisbury, United Kingdom (UK). Russia and the GRU were quickly blamed for the attack, despite repeated denials from Russian authorities. GRU agents eventually were identified in Salisbury and charged for the attack. UK authorities also identified the chemical weapon as a Novichok, a class of nerve agent developed in the Soviet Union.

To help confirm these findings, samples were sent to the Organization for the Prohibition of Chemical Weapons (OPCW) in The Hague, Netherlands. The OPCW also was investigating claims of an alleged gas attack in Syria by the Bashar al Asad regime against the town of Douma.

On April 10, 2018, four GRU agents traveling on diplomatic passports entered the Netherlands. Between April 11 and April 12, the agents conducted reconnaissance of the area around OPCW headquarters and booked rooms at a hotel directly next to the OPCW. Working with UK intelligence, Dutch security services arrested the four men on April 13. Discovered in a GRU agent's car was high-tech equipment, which could be used to hack into OPCW Wi-Fi networks, a so-called "close access hack." The equipment was confiscated and the agents were expelled from the country.

The Netherlands and the UK held a joint press conference on October 4, 2018, detailing the GRU operation and identifying the agents. At the same time, Australia, New Zealand, Canada, and NATO released statements supporting the identification of malicious cyber activity from Russia and condemned Russian actions. On the same

[107] Paul Nakasone, "Advance Policy Questions for Lieutenant General Paul Nakasone, USA Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service," U.S. Senate Armed Services Committee, March 1, 2018.

[108] For more, see CRS In Focus IF11718, *Russian Cyber Units*, by Andrew S. Bowen.

[109] Ellen Nakashima, "U.S. Sanctions Russian Lab That Built What Experts Say Is Potentially the World's Deadliest Hacking Tool," *Washington Post*, October 23, 2020.

[110] Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies*, vol. 17, no. 2 (2004), pp. 237-256; Lilly and Cheravitch, "Past, Present, and Future of Russia's Cyber Strategy and Forces," pp. 130-134.

[111] Stephen Blank, "Cyber War and Information War a la Russe," in *Understanding Cyber Conflict*, ed. George Perkovich and Ariel E. Levite (Washington, DC: Georgetown University Press, 2017), pp. 81-98; Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," *CNA*, March 2017; Andrew Radin, Alyssa Demus, and Krystyna Marcinek, "Understanding Russian Subversion: Patterns, Threats, and Responses," RAND, February 2020, pp. 12-16.

day, the U.S. Department of Justice released indictments against seven GRU officers for the attempted OPCW hack, as well as for hacking the World Anti-Doping Agency (and other anti-doping agencies) in 2016; the agencies were investigating Russia's use of performance-enhancing drugs during the 2014 Sochi Winter Olympics. In response to the Skripal attack and the attempted OPCW hack, more than 26 countries expelled more than 150 Russian diplomats. The UK expelled 23 diplomats; the United States expelled 60 officials and closed the Russian consulate in Seattle and two recreational facilities allegedly used for intelligence collection in Maryland and Long Island.

Sources: CRS In Focus IF10962, *Russia, the Skripal Poisoning, and U.S. Sanctions*, by Dianne E. Rennack and Cory Welt; Government of the Netherlands, "Netherlands Defence Intelligence and Security Service Disrupts Russian Cyber Operation Targeting OPCW," press release, October 4, 2018; Government of the Netherlands, "Joint Statement by Prime Minister May and Prime Minister Rutte on Cyber Activities of the Russian Military Intelligence Service, the GRU," press release, October 4, 2018; U.S. Department of Justice, "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," press release, October 4, 2018; *U.S. v. Aleksei Sergeyevich Morenets*, 2:18-cr-00263-MRH (United States District Court Western District of Pennsylvania 2018); UK National Cyber Security Centre, "Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed," press release, October 3, 2018; Mark Odell, "How Dutch Security Service Caught Alleged Russian Spies," *Financial Times*, October 4, 2018.

At the same time, Russian security and military doctrines view information and disinformation operations as a crucial foreign policy tool.[112] Russian authorities, and their Soviet predecessors, have long recognized the importance of psychological operations, but their views have evolved in recognition of the changing information landscape since the 1990s.[113] The ease of access to information presents both dangers and opportunities to Russia's leaders.[114]

On the one hand, Russia's leadership is concerned with the destabilizing effects of the free flow of information, such as instigating popular protests and stoking societal discontent. These effects are more dangerous due to the Russian belief that Western governments have manipulated information to overthrow unfriendly regimes.[115] During 2020 protests in Belarus against President Alexander Lukashenko, Russian SVR chief Sergei Naryshkin accused the West of conducting a "poorly disguised attempt to organize another 'color revolution' and an anti-constitutional coup."[116] Russia sees itself as the target of such information operations, and Russia's security and military doctrines describe the dangers posed by foreign manipulation of domestic audiences.[117]

[112] Roland Heickero, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, Swedish Defense Research Agency (FOI), March 2020; Joe Cheravitch, *The Role of Russia's Military in Information Confrontation*, CNA, July 2021.

[113] Herbert Romerstein, "Disinformation as a KGB Weapon in the Cold War," *Journal of Intelligence History*, vol. 1, no. 1 (2001), pp. 54–67; Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020).

[114] Recent media reporting has documented the elevation of a former deputy commander of GRU Unit 55111, involved in psychological and disinformation operations, as a scientific adviser to the Russian Security Council. Denis Dmitriev, Alexey Kovalev, and Lilia Yapparova, "Psy-ops in High Places: Putin's New Science Advisor to Russia's National Security Council Is a Military Intelligence Agent Accused of Spreading Disinformation About the Coronavirus," *Meduza*, May 17, 2021.

[115] Karrie J. Koesel and Valerie J. Bunce, "Diffusion Proofing: Russian and Chinese Responses to Waves of Popular Mobilizations Against Authoritarian Rulers," *Perspectives on Politics*, vol. 11. no. 3 (2013), pp. 753-768; Dmitry Gorenburg, "Countering Color Revolutions: Russia's New Security Strategy and Its Implications for U.S. Policy," *PONARS Eurasia*, no. 342 (September 2014); Tracey German, "Harnessing Protest Potential: Russian Strategic Culture and the Colored Revolutions," *Contemporary Security Policy*, vol. 41, no. 4 (2020), pp. 541-563.

[116] Tom Balmforth, "Russia Accuses U.S. of Promoting Revolution in Belarus, Toughens Stance," Reuters, September 16, 2020.

[117] Nicolas Bouchet, "Russia's 'Militarization' of Colour Revolutions," Center for Security Studies, *Policy Perspectives*, vol. 4, no. 2 (January 2016).

On the other hand, the use and manipulation of information provides opportunities for Russia. Many analysts note that due to a perception by Russian policymakers that the West targets Russia with information operations, Russian intelligence and security services in response seek to actively disrupt and undermine the domestic politics of adversaries, while at the same time disrupting and obfuscating any accusations of Russian culpability.[118] The Russian government seeks to manipulate domestic audiences and undermine faith in democratic systems of government. Often, instead of seeking a particular outcome, the goal for Russian information operations is to cause chaos and weaken the domestic legitimacy of an adversary's government.[119]

Additionally, Russia has offensively used cyber operations to further Russian foreign policy objectives and inflict punishment on adversaries. These efforts have included offensive attacks against foreign electrical networks, banking sectors, government institutions, and even sporting events.[120] These attacks may be in service to a range of Russian foreign policy objectives. In an October 2020 indictment against GRU Unit 74455, U.S. Assistant Attorney General for National Security John C. Demers stated, "No country has weaponized its cyber capabilities as maliciously or irresponsibly as Russia, wantonly causing unprecedented damage to pursue small tactical advantages and to satisfy fits of spite."[121]

Media reporting and federal indictments indicate that to develop its cyber capabilities, the FSB has relied on co-opting, coercing, and recruiting talented individuals from Russia's cyber-criminal community, often under threat of criminal prosecution.[122] In contrast, the GRU apparently has sought to cultivate talent internally and developed multiple recruiting pathways.[123] Due to its history in conducting signals intelligence and disinformation operations, the GRU was able to develop its capabilities into cyber operations.

[118] Peter Pomerantsev, "Russia and the Menace of Unreality," *Atlantic*, September 9, 2014; Martin Kragh and Sebastian Asberg, "Russia's Strategy for Influence Through Public Diplomacy and Active Measures: The Swedish Case," *Journal of Strategic Studies*, vol. 40, no. 6 (2017), pp. 773-816; Clint Watts, "Russia's Active Measures Architecture: Task and Purpose," *Alliance for Securing Democracy*, May 22, 2018; Renee Diresta and Shelby Grossman, "Potemkin Pages and Personas: Assessing GRU Online Operations, 2014-2019," Stanford Internet Observatory Cyber Policy Center, 2019.

[119] Reporting has linked Russian military intelligence to numerous disinformation operations, including the COVID-19 pandemic and German parliamentary elections. Observers connect many of these operations to a group referred to as "Ghostwriter," reportedly linked to Russian military intelligence. Mandiant, *Ghostwriter Update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity*, April 28, 2021; Loveday Morris, "Germany Complains to Moscow Over Pre-Election Phishing Attacks on Politicians," *Washington Post*, September 6, 2021.

[120] Benjamin Jensen, Brandon Valeriano, and Ryan Maness, "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist," *Journal of Strategic Studies*, vol. 42, no. 2 (2019), pp. 212-234; Greenberg, *Sandworm*, pp. 46-49.

[121] U.S. Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," press release, October 19, 2020.

[122] Soldatov and Borogan, *The New Nobility*, pp. 227-238; Cory Bennett, "Kremlin's Ties to Russian Cyber Gangs Sow US Concerns," *The Hill*, October 11, 2015; Daniil Turovsky, "It's Our Time to Serve the Motherland: How Russia's War in Georgia Sparked Moscow's Modern-Day Recruitment of Criminal Hackers," *Meduza*, August 7, 2018; Liliya Yapparova, "The FSB's Personal Hackers" *Meduza*, December 12, 2018; Joseph Marks, "Evil Corp Indictments Show Cybercrime Pays—For Those At The Top," *Washington Post*, December 6, 2019; Mike Eckel, "More Glimpses of How Russian Intelligence Utilized Hackers Revealed in U.S. Trial," RFE/RL, March 16, 2020.

[123] Troianovski and Nakashima, "How Russia's Military Intelligence Agency Became the Covert Muscle in Putin's Duels with the West."

GRU Cyber Operations and October 2020 U.S. Indictment

The GRU has conducted numerous aggressive, malicious, and wide-ranging cyber operations against multiple targets. In 2015, GRU officers reportedly hacked the Bundestag, Germany's national parliament. Germany issued an arrest warrant for GRU officer Dmitry Badin, who is an accused member of Unit 26165 and indicted by the United States for his role in 2016 election interference. In October 2020, the European Union and the United Kingdom sanctioned Badin and GRU head Igor Kostyukov over the hack.

Also in October 2020, the U.S. Department of Justice indicted six GRU officers for a range of cyberattacks. In the indictment, Unit 74455, identified as *Sandworm*, allegedly is responsible for multiple cyberattacks, including the following:

- 2015 attacks on Ukraine's electrical infrastructure, Ministry of Finance, and State Treasury Service
- a 2017 hack-and-leak effort targeting French President Emmanuel Macron's emails and interference in France's presidential election
- a 2017 malware attack, commonly known as NotPetya, which infected computers globally and caused an estimated $10 billion in damage
- a 2018 hacking attack against the PyeongChang Winter Olympics in South Korea, in which GRU hackers attempting to disguise themselves as North Korean hackers used malware to disrupt the opening ceremony
- a 2018 hacking campaign against UK, European, and Organization for the Prohibition of Chemical Weapons investigations into the nerve agent attack against Sergei Skripal and his daughter
- a 2018-2019 cyber campaign against Georgian media companies and the Georgian parliament.

Sources: Andy Greenberg, "The US Blames Russia's GRU for Sweeping Cyberattacks in Georgia," *Wired*, February 20, 2020; Kate Connolly, "Russian Hacking Attack on Bundestag Damaged Trust, Says Merkel," *Guardian*, May 13, 2020; Catherine Stupp, "Germany Seeks EU Sanctions for 2015 Cyberattack on Its Parliament," *Wall Street Journal*, June 11, 2020; U.S. v. Yuriy Sergeyevich Andrienko et al., 20316 (United States District Court of Western Pennsylvania 2020); U.S. Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," press release, October 19, 2020; Robin Emmott, "EU Imposes Sanctions on Russian Military Intelligence Chief," Reuters, October 22, 2020.

Unit 26165

Unit 26165 was established as the 85th Main Special Service Center during the Cold War, responsible for military intelligence's cryptography.[124] Often referred to as APT 28 or *Fancy Bear*, Unit 26165 is one of two units identified by the U.S. government responsible for hacking the Democratic Congressional Campaign Committee (DCCC), the Democratic National Committee (DNC), and the presidential campaign of Hillary Clinton (see "2016 Election Interference," below).[125]

[124] Lilly and Cheravitch, "Past, Present, and Future of Russia's Cyber Strategy and Forces," p. 145.

[125] Director of National Intelligence, "Background to 'Assessing Russian Activities and Intentions in Recent U.S. Elections': The Analytic Process and Cyber Incident Attribution," January 6, 2017; U.S. Department of Justice, "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election," press release, July 13, 2018; Department of Homeland Security and Federal Bureau of Investigation, *GRIZZLY STEPPE—Russian Malicious Cyber Activity*, Joint Analysis Report, December 29, 2016; Rick Noack, "The Dutch Were a Secret U.S. Ally in War Against Russian Hackers, Local Media Reveal," *Washington Post*, January 26, 2018; Estonian Foreign Intelligence Service, *International Security and Estonia*, Annual Report (2018), p. 55; Mike Eckel, "The Return of Cozy Bear: Russian Hackers in the Crosshairs of Western Intelligence Agencies—Again," RFE/RL, July 18, 2020.

Unit 74455

Unit 74455 appears to be a newer unit created to help support and expand the GRU's cyber capabilities.[126] Unit 74455 also is known as the Main Center for Special Technologies and is commonly referred to by media reports and the U.S. government as *Sandworm*. This cyber unit is linked to some of Russia's most brazen cyber operations, such as the 2017 NotPetya attack in Ukraine.[127] On October 19, 2020, the U.S. Department of Justice unsealed indictments against six members of Unit 74455 for attacks on various international targets (see "GRU Cyber Operations and October 2020 Indictment," above).

Unit 54777

This unit, also known as the 72nd Special Service Center, is reportedly responsible for the GRU's psychological operations.[128] This includes operating in support of other GRU cyber units and operating on the tactical level by conducting electronic warfare and psychological operations. Media reports have linked Unit 54777 to online disinformation campaigns, specifically regarding the COVID-19 pandemic.[129]

2016 Election Interference

According to U.S. Special Counsel Robert Mueller, the intelligence community (the IC, comprising the Central Intelligence Agency, National Security Agency, Federal Bureau of Investigation Intelligence Branch, and fourteen other statutory elements), and subsequent investigations by the House and Senate Intelligence Committees, Russia conducted an extensive effort to interfere in the 2016 U.S. presidential election.[130] Then-Director of National Intelligence Dan Coats stated, "Russia conducted an unprecedented influence campaign to interfere in the U.S. electoral and political process."[131] Congressional leadership subsequently affirmed the IC's assessment.[132]

According to Mueller and investigations by the Senate Select Committee on Intelligence (SSCI), as well as numerous media reports, Units 26165 and 74455 were directly responsible for Russia's

[126] Lilly and Cheravitch, "Past, Present, and Future of Russia's Cyber Strategy and Forces," pp. 145-146.

[127] Ellen Nakashima, "Russian Military was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes," *Washington Post*, January 12, 2018; Greenberg, *Sandworm*, pp. 179-220.

[128] Troianovski and Nakashima, "How Russia's Military Intelligence Agency Became the Covert Muscle in Putin's Duels with the West"; RFE/RL, "On the Trail of the 12 Indicted Russian Intelligence Officers."

[129] Julian E. Barnes and David E. Sanger, "Russian Intelligence Agencies Push Disinformation on Pandemic*," New York Times*, July 28, 2020.

[130] Director of National Intelligence, "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution," January 6, 2017; David E. Sanger, "Putin Ordered 'Influence Campaign' Aimed at U.S. Election, Report Says," *New York Times*, January 6, 2017; Ken Dilanian, "Intelligence Director Says Agencies Agree on Russian Meddling," *NBC News*, July 21, 2017; Special Counsel Robert S. Mueller, III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, U.S. Department of Justice, vol I of II, Washington, DC, March 2019; U.S. Congress, Senate Select Committee on Intelligence, "Volume 5: Counterintelligence Threat/Vulnerabilities" in *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, 116th Cong., 2020.

[131] Karen Yourish and Troy Griggs, "8 U.S. Intelligence Groups Blame Russia for Meddling, but Trump Keeps Clouding the Picture," *New York Times*, August 2, 2018.

[132] Michael Collins, Nicole Guadiano, and Eliza Collins, "Congressional GOP Leadership: No Doubt That Russia Meddled in 2016 Presidential Election," *USA Today*, July 17, 2018.

"hack-and-leak" operation.[133] Unit 26165 conducted an extensive effort to hack the emails and systems of the "DCCC and DNC, as well as email accounts of individuals affiliated with the [Hillary] Clinton Campaign."[134] These investigations document Unit 74455 as responsible for releasing tens of thousands of the stolen documents through various fictitious online personas and in coordination with WikiLeaks.[135]

According to the Special Counsel, SSCI, and the IC, beginning in March 2016, the GRU conducted an extensive spearphishing and malware campaign to hack the networks and email accounts of the DNC, DCCC, and Clinton campaign, including the email account of campaign chairperson John Podesta.[136] The GRU stole tens of thousands of documents and emails from these accounts until at least September 2016.[137] Using numerous social media aliases, including "DCLeaks" and "Guccifer 2.0," Unit 74455 coordinated the release of stolen documents to interfere in the 2016 election.[138] According to SSCI, the GRU used these aliases to communicate with WikiLeaks to transmit stolen documents, which WikiLeaks then released for "maximum political impact" starting on the eve of the 2016 Democratic National Convention.[139]

Recent Cyber Activities

The GRU appears to be continuing and adapting its cyber operations abroad, despite numerous indictments and the exposure of multiple operations. In September 2020, Federal Bureau of Investigation (FBI) Director Christopher Wray stated that Russia had "very active efforts" to interfere in the 2020 elections.[140] In March 2021, the Director of National Intelligence released the IC's assessment of foreign interference in the 2020 election. The assessment stated that Russia conducted influence and disinformation operations but that, "Unlike in 2016, we did not see persistent Russian cyber efforts to gain access to election infrastructure."[141] The U.S. government and media reporting implicates the GRU as central to these Russian efforts to hack into political campaigns and U.S. government agencies.[142] Further reporting and private sector

[133] U.S. Congress, Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, p. 176.

[134] This effort included the targeting of state and local election officials. Special Counsel Robert S. Mueller, III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, pp. 37, 50.

[135] *U.S. v. Viktor Borisovich Netyksho et al.*, 1:18-cr-00215-ABJ (United States District Court for the District of Columbia 2018); Thomas Rid, "How Russia Pulled Off the Biggest Election Hack in U.S. History," *Esquire*, October 20, 2016.

[136] *U.S. v. Viktor Borisovich Netyksho et al.*, 1:18-cr-00215-ABJ.

[137] *U.S. v. Viktor Borisovich Netyksho et al.*, 1:18-cr-00215-ABJ; U.S. Congress, Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, p. 171.

[138] *U.S. v. Viktor Borisovich Netyksho et al.*, 1:18-cr-00215-ABJ; U.S. Congress, Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, pp. 183-183, 188.

[139] U.S. Congress, Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, pp. 172-173, 199.

[140] Kyle Cheney, "Wray Says Russia Engaged in 'Very Active Efforts' to Interfere in Election, Damage Biden," *Politico*, September 17, 2020.

[141] Office of the Director of National Intelligence, *Foreign Threats to the 2020 U.S. Federal Elections*, March 10, 2021, at https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

[142] Meg Kelly and Elyse Samuels, "How Russia Weaponized Social Media, Got Caught and Escaped Consequences," *Washington Post*, November 18, 2019; Andy Greenberg, "Russia's Fancy Bear Hackers Are Hitting US Campaign Targets Again," *Wired*, September 10, 2020; Julian E. Barnes and David E. Sanger, "U.S. Accuses Russian Military Hackers of Attack on Email Servers," *New York Times*, May 28, 2020; National Security Agency, "Exim Mail Transfer Agent Actively Exploited by Russian GRU Cyber Actors," press release, May 28, 2020; Andy Greenberg, "Russia's Fancy Bear Hackers Likely Penetrated a US Federal Agency," *Wired*, October 1, 2020; Raphael Satter, Christopher

cybersecurity firms alleged the GRU hacked into the computer networks of the Ukrainian natural gas company Burisma, where President Joe Biden's son, Hunter Biden, previously was a board member.[143] Both France and Germany have publicly accused GRU cyber units of conducting extensive and intense cyber espionage campaigns against government targets and in the run-up to elections.[144] Additionally, a cybersecurity firm has tied the GRU to attempted breaches of U.S. critical infrastructure.[145] In July 2021, a joint advisory of the National Security Agency, Cybersecurity and Infrastructure Security Agency, FBI, and the UK's National Cyber Security Centre (NSA-CISA-NCSC-FBI) also identified Unit 26165 as conducting a "widespread, distributed, and anonymized brute force access attempts against hundreds of government and private sector targets worldwide."[146] The agencies described the operation beginning in mid-2019 and likely ongoing as of July 2021.[147]

U.S. Policy Responses and Issues for Congress[148]

The United States has been proactive in countering GRU operations and malign activities. The U.S. government has demonstrated a willingness to "name and shame" the GRU and its operations. Detailing substantial information regarding GRU personnel and operations potentially may dissuade or deter further actions due to the high risk of public exposure.[149]

After the 2016 presidential election, the U.S. Department of Justice pursued three indictments against a total of 21 GRU officers for malicious cyber activity, including interference in the 2016 U.S. presidential election, disinformation and information campaigns, and offensive cyber operations leading to billions of dollars in losses.[150] The indictments, issued in 2018, detail the officers themselves; identify their units; and closely describe the operations, activities, and methods used by the GRU.

The U.S. government also has imposed sanctions on the GRU and 21 GRU officers for the same and additional malign activities abroad.[151] Sanctions designations were made pursuant to

Bing, and Joel Schectman, "Russian Hackers Targeted California, Indiana Democratic Parties," Reuters, October 30, 2020.

[143] Nicole Perlroth and Matthew Rosenberg, "Russian Hacked Ukrainian Gas Company at Center of Impeachment," *New York Times*, January 13, 2020.

[144] Andy Greenberg, "France Ties Russia's Sandworm to a Multiyear Hacking Spree," *Wired*, February 15, 2021; Loveday Morris, "Germany Complains to Moscow over Pre-Election Phishing Attacks to Politicians," *Washington Post*, September 6, 2021.

[145] Andy Greenberg, "Hackers Tied to Russia's GRU Targeted U.S. Grid for Years, Researchers Warn," *Wired*, February 24, 2021.

[146] Cybersecurity and Infrastructure Security Agency, "NSA-CISA-NCSC-FBI Joint Cybersecurity Advisory on Russian GRU Brute Force Campaign," press release, July 1, 2021.

[147] Julian E. Barnes and David E. Sanger, "After Biden Meets Putin, U.S. Exposes Details of Russian Hacking Campaign," *New York Times*, July 1, 2021.

[148] This section partially draws on CRS Report R45415, *U.S. Sanctions on Russia*, coordinated by Cory Welt.

[149] The sharing of biometric information among allies also could potentially degrade operatives' freedom and ability to travel and conduct operations.

[150] Four GRU officers are indicted twice. U.S. Department of Justice, "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election," press release, July 13, 2018; U.S. Department of Justice, "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," press release, October 4, 2018; U.S. Department of Justice, "Six Russian GRU Officers Charged.".

[151] Thirteen GRU officers are both indicted and designated for sanctions. The GRU and four GRU officers are designated twice.

Executive Order (EO) 13694, as amended, and Section 224 of the Countering Russian Influence in Europe and Eurasia Act of 2017 (CRIEEA; P.L. 115-44, Countering America's Adversaries Through Sanctions Act [CAATSA], Title II).[152]

U.S. sanctions designations against the GRU and its officers include the following:

- In December 2016, the Obama Administration designated the GRU and four GRU officers (as well as the FSB) for activities related to election interference, pursuant to EO 13694, as amended.[153]
- In March 2018, the Trump Administration designated the GRU, the four GRU officers first designated in 2016, and two more GRU officers (as well as the FSB) for "destructive cyberattacks," including the 2017 NotPetya malware attack, pursuant to Section 224 of CRIEEA. [154]
- In December 2018, the Trump Administration designated nine GRU officers for activities related to election interference; four GRU officers for cyber-enabled operations against the World Anti-Doping Agency and the OPCW; and two GRU officers for the nerve agent attack on Sergei Skripal and his daughter, pursuant to Section 224 of CRIEEA.[155]

Congress, the Administration, and analysts continue to debate the effectiveness of indictments and sanctions.[156] Media reporting suggests that in addition to "name and shame" strategies of indictments and sanctions, the U.S. government has authorized more aggressive and offensive use of cyber capabilities to thwart and deter Russian operations. Media reports allege that, over the past few years, the United States has conducted operations to disrupt internet access from an alleged Russian "troll farm" and conducted incursions and surveillance of Russia's electric power grid.[157] Although not specifically directed at the GRU, these actions may be intended to signal capabilities and potential costs, should Russia continue to conduct brazen cyber operations.

The U.S. government also appears to be increasing its communication and coordination with private-sector actors to counter Russian and GRU cyber activity. In the October 2020 indictment (see "GRU Cyber Operations and October 2020 U.S. Indictment," above), U.S. Department of Justice officials thanked "Google, including its Threat Analysis Group (TAG); Cisco, including its Talos Intelligence Group; Facebook; and Twitter, for the assistance they provided in this investigation."[158] Additionally, media reporting suggests U.S. Cyber Command has closely

[152] Executive Order (EO) 13694 was amended by EO 13757. EO 13694 of April 1, 2015, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," 80 *Federal Register* 18077, April 2, 2015; EO 13757 of December 28, 2016, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," 82 *Federal Register* 1.

[153] White House, "Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment," December 29, 2016.

[154] U.S. Department of the Treasury, "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks, press release, March 15, 2018.

[155] Although the attack on Sergei Skripal was not cyber-related, the Office of Foreign Assets Control used Section 224 (on undermining cybersecurity) to designate these officers as agents of the previously designated GRU. U.S. Department of the Treasury, "Treasury Targets Russian Operatives over Election Interference, World Anti-Doping Agency Hacking, and Other Malign Activities," press release, December 19, 2018.

[156] Jack Goldsmith, "The Puzzle of the GRU Indictment," *Lawfare,* October 21, 2020.

[157] Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, February 27, 2019; David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *New York Times,* June 15, 2019.

[158] U.S. Department of Justice, "Six Russian GRU Officers Charged."

coordinated with private companies in operations against Russian disinformation and cyber operations.[159]

Outlook

Congress and other interested stakeholders continue to debate the effectiveness of sanctions, indictments, and other "name and shame" strategies to counter malign Russian military intelligence activities. Due to its position, roles, and capabilities, the GRU prides itself on conducting aggressive and high-risk operations. Therefore, some observers argue, specific actions directed solely against the GRU may not have the desired level of impact. As a result, some observers argue that the exposure of the GRU and its operations is not necessarily a deterrent, as long as Russia's political leadership finds it useful to have such an agency capable and willing to conduct such operations.

Nonetheless, the exposure of GRU operations has led to some media reports of infighting among Russian security agencies seeking to take advantage of GRU exposure, thereby undermining Russian capabilities. After the 2018 attempted assassination of Sergei Skripal in the UK, the United States and several allies enacted sanctions and expelled Russian diplomats and suspected intelligence officers. Some reports suggest these measures not only created tensions within the Russian government, which blamed the GRU for its situation, but also may have limited Russian intelligence operations by expelling potential intelligence officers. Some observers argue that a full range of responses targeting other actors and sectors beyond the GRU may produce, or at least encourage, more desired Russian behavior; at the same time, it is unclear to what extent such responses would have any bearing on the GRU's future actions. In addition to the wide range of options available, coordinating responses with allies could increase the costs to Russia and the effectiveness of policy options, while isolating Russia and the GRU in response to their aggressive actions.

Author Information

Andrew S. Bowen
Analyst in Russian and European Affairs

Acknowledgments

Cory Welt, Specialist in Russian and European Affairs, contributed valuable assistance to this report.

[159] David E. Sanger and Nicole Perlroth, "As Election Nears, Government and Tech Firms Push Back on Russia (and Trump)," *New York Times*, October 20, 2020.

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.