Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated February 2, 2022

Russian Cyber Units

Russia has deployed sophisticated cyber capabilities to conduct disinformation, propaganda, espionage, and destructive cyberattacks globally. To conduct these operations, Russia maintains numerous units that are overseen by various security and intelligence agencies. Russia's security agencies compete with each other and often conduct similar operations on the same targets, making specific attribution and motivation assessments difficult. The U.S. government has indicted and imposed sanctions on Russian security personnel and agents for various cyberattacks. Congress may be interested in Russian agencies, units, and their attributes to better understand why and how Russia conducts cyber operations.

Early Russian Cyber Operations

According to media and government reports, Russia's initial cyber operations primarily consisted of Distributed Denial of Service (DDoS) attacks and often relied on the co-optation or recruitment of criminal and civilian hackers. In 2007, Estonia was the target of a large-scale cyberattack, which most observers blamed on Russia. Estonian targets ranged from online banking and media outlets to government websites and email services.

Russia again employed DDoS attacks during its 2008 war with Georgia. Although Russia denied responsibility, Georgia was the victim of a large-scale cyberattack that corresponded with Russian military actions. Analysts identified 54 potential targets (e.g., government, financial, and media outlets), including the National Bank of Georgia, which suspended all electronic operations for 12 days.

Russian Security and Intelligence Agencies

Over the past 20 years, Russia has increased its personnel, capabilities, and capacity to undertake a wide range of cyber operations. No single Russian security or intelligence agency has sole responsibility for cyber operations. Observers note that this framework contributes to competition among the agencies for resources, personnel, and influence, and some analysts cite it as a possible reason for Russian cyber units conducting similar operations, without any apparent awareness of each other.

Military Intelligence

The Main Directorate of the General Staff, commonly referred to as the GRU, is Russia's military intelligence agency. The GRU has been implicated in some of Russia's most notorious and damaging cyber operations. Media reporting and U.S. government indictments identify two primary GRU cyber units. The U.S. Department of Justice (DOJ) has charged personnel from both units for actions ranging from election interference in the 2016 U.S. presidential election to multiple damaging cyberattacks. The units' public profile underlines a high operational tempo. The GRU reportedly also controls several research institutes that help develop hacking tools and malware. Observers have noted an apparent willingness by GRU cyber units to conduct brazen and aggressive operations, sometimes with questionable levels of operational security and secrecy. Cyber analysts have referred to these units collectively as APT (Advanced Persistent Threat) 28, Fancy Bear, Voodoo Bear, Sandworm, and Tsar Team.

Unit 26165: Unit 26165 is one of two Russian cyber groups identified by the U.S. government as responsible for hacking the Democratic Congressional Campaign Committee, Democratic National Committee, and presidential campaign of Hillary Clinton. Media and Western governments also have linked Unit 26165 to cyber operations against numerous political, government, and private sector targets in the United States and Europe.

Unit 74455: Unit 74455 has been linked to some of Russia's most brazen and damaging cyberattacks. The U.S. government identified Unit 74455 as responsible for the coordinated release of stolen emails and documents during the 2016 U.S. presidential election. As opposed to primarily focusing on penetrating systems and collecting information, Unit 74455 appears to have significant offensive cyber capabilities. In October 2020, DOJ indicted members of GRU Unit 74455 for numerous cyberattacks, including the 2017 NotPetya malware attack. In June 2017, malware was deployed against numerous targets in Ukraine. The malware soon spread globally, causing significant damage to countries and businesses beyond Ukraine.

Unit 54777: This unit, also known as the 72nd Special Service Center, reportedly is responsible for the GRU's psychological operations. This includes online disinformation and information operations.

Foreign Intelligence Service

The Foreign Intelligence Service (SVR) is Russia's primary civilian foreign intelligence service. It is responsible for the collection of foreign intelligence using human, signals, electronic, and cyber methods. Most observers acknowledge the SVR operates with a strong emphasis on maintaining secrecy and avoiding detection. Most cyber operations reportedly linked to the SVR have focused on collecting intelligence. The SVR also is known to have high levels of technical expertise, often seeking to gain and retain access inside compromised networks. Cyber analysts have referred to SVR hackers as APT 29, Cozy Bear, and the Dukes.

Analysts and observers have recognized the SVR as highly capable and professional. In contrast to GRU cyber units, the SVR appears focused on collecting intelligence and remaining undetected once it gains access to targeted networks. The U.S. government identified the SVR as one of two Russian cyber units responsible for hacking into political campaigns during the 2016 U.S. presidential election. Despite the focus on operating clandestinely, in 2018, a Dutch newspaper reported that Dutch intelligence compromised the SVR's infrastructure and provided crucial information to the U.S. government. Private cybersecurity firms noted that the SVR subsequently decreased its activity. More recently, however, SVR activity reportedly has increased, and the unit has been linked to numerous cyberespionage operations. For example, in April 2021, the U.S. government identified APT 29 as responsible for the SolarWinds attack that exploited supply chain vulnerabilities to infiltrate U.S. government and private sector networks. In a cybersecurity advisory alert, U.S. government noted APT 29 will "continue to seek intelligence from U.S. and foreign entities through cyber exploitation, using a range of initial exploitation techniques that vary in sophistication, coupled with stealthy intrusion tradecraft within compromised networks."

Federal Security Service

The Federal Security Service (FSB) is Russia's primary domestic security agency responsible for internal security and counterintelligence. Its missions include protecting Russia from foreign cyber operations and monitoring domestic criminal hackers, a mission jointly undertaken with Department K of the Ministry of Internal Affairs. In recent years, the FSB has expanded its mission to include foreign intelligence collection and offensive cyber operations. Cyber analysts have referred to FSB hackers as Berserk Bear, Energetic Bear, Gamaredon, TeamSpy, Dragonfly, Havex, Crouching Yeti, and Koala.

The FSB reportedly has two primary centers overseeing its information security and cyber operations. The first is the 16th Center, which houses most of the FSB's signals intelligence capabilities. The FSB also includes the 18th Center for Information Security, which oversees domestic operations and security but conducts foreign operations as well. The U.S. government indicted 18th Center FSB officers in 2017 for breaching Yahoo and millions of email accounts. In 2021, Ukrainian intelligence released information and recordings of 18th Center FSB officers based in Crimea as part of the "Gamaredon" hacking group.

Media reporting indicates FSB units are capable of manufacturing their own advanced malware tools and have been documented manipulating exposed malware to mimic other hacking teams and conceal their activities. Reporting indicates the FSB oversees training and research institutes, which directly support the FSB's cyber mission.

One FSB team reportedly focuses on penetrating infrastructure and energy sector targets. Most operations linked to this team appear to be reconnaissance or clandestine surveillance. The targeting of the energy sector has raised concern within the U.S. government. The Department of Homeland Security and the Federal Bureau of Investigation have documented the unit's reconnaissance and noted the possibility of inserting malware to cause future damage in an attack. The U.S. government also has linked the unit to attempts to penetrate state and local government networks in 2020.

Media reporting has documented close connections between the FSB and criminal and civilian hackers, which the FSB reportedly uses to augment and staff its cyber units. DOJ has indicted multiple Russian hackers for a variety of criminal and state-sponsored cyber activities. Many of these indictments describe the close relationship between criminal hackers and the FSB.

Federal Protective Service

The Federal Protective Service (FSO) is responsible for the physical and electronic security of the government and government personnel. As such, it has extensive signals and electronic capabilities to ensure the security of Russian government communications. The FSO appears primarily concerned with the defense of Russian government networks, and there is no indication it has launched offensive operations.

Internet Research Agency

The Internet Research Agency is a private organization, funded by Kremlin-connected oligarch Yevgeniy Prighozin, which has supported Russian government disinformation and propaganda operations. Often referred to as a *troll farm* or *troll factory*, this group has focused on disinformation by impersonating domestic activists and people, primarily through various social media channels. In 2018, the U.S. government indicted the Internet Research Agency and its personnel for efforts to sow discord and influence the U.S. political system, including during the 2016 presidential election.

Russian Cyber Weaknesses

Russia faces significant challenges in cyber operations, despite its capabilities and high operational tempo. Many of these challenges are not unique to Russia but still present hurdles to further growth of Russia's cyber operations.

Like other government agencies, Russian security services face challenges recruiting qualified personnel. Private-sector opportunities and rival agencies compete for talent. As noted, this often causes Russian security services to outsource operations to civilian and criminal hackers.

Russia's security services also are known for high levels of corruption. Russian security and intelligence agents have been unmasked and identified through information often reportedly sold by corrupt security officers. In 2020, media outlets identified the FSB agents reportedly responsible for the assassination attempt of Russian opposition figure Alexei Navalny from purchased data.

For more information see CRS Report R45415, *U.S. Sanctions on Russia*, coordinated by Cory Welt; CRS Report R46616, *Russian Military Intelligence: Background and Issues for Congress*, by Andrew S. Bowen.

Andrew S. Bowen, Analyst in Russian and European Affairs

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.