Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

January 4, 2021

# 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 overseen by its 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. Congress may be interested in the various 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.

Shortly thereafter, Russia again employed DDoS attacks during its August 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. Additionally, some agencies appear to prioritize the development of in-house capabilities, whereas others look to contract outside actors for operations.

### 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 also reportedly 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. Collectively, these units are sometimes referred to 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. DOJ alleges Unit 74455 is responsible for numerous malicious cyberattacks. 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.

### 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 as opposed to causing damage through cyberattacks. The SVR also is known to have high levels of technical expertise, often seeking to gain and retain access inside compromised networks. SVR hackers sometimes are referred to 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 in the following years, the SVR decreased its activity. The SVR's activity reportedly has increased since, and the unit has been linked to numerous cyberespionage operations. Most recently, reports link the SVR to cyberespionage on COVID-19 vaccine research and the tools of cybersecurity firm FireEye. Reports also link the SVR to the SolarWinds attack that reportedly compromised many U.S. government agencies.

### 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 Interior. In recent years, the FSB has expanded its mission to include foreign intelligence collection and offensive cyber operations.

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. The FSB can coerce civilian and criminal hackers into working as contractors with the threat of imprisonment. 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. These indictments and media reporting describe a relationship where civilian and criminal hackers can conduct freelance commercial operations in return for assisting the FSB. FSB hackers are sometimes referred to as Berserk Bear, Energetic Bear, Gamaredon, TeamSpy, Dragonfly, Havex, Crouching Yeti, and Koala.

One FSB team reportedly focuses on penetrating infrastructure and energy-sector targets. In contrast to other hacking teams, 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 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 indicates another active and sophisticated FSB unit is capable of manufacturing its own advanced malware tools and has been documented manipulating exposed malware to mimic other hacking teams and conceal its activity.

### 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 close Putin confidant 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 or to purchase malware.

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. Most recently, media outlets identified the FSB agents reportedly responsible for the assassination attempt of Russian opposition figure Alexei Navalny from purchased data.

Observers also note corrupt Russian officers conduct cyberattacks for personal enrichment. Domestic hackers have targeted Russian government personnel with embarrassing leaks of emails and correspondence. *Shaltai Boltai* (*Humpty Dumpty* in Russian), or Anonymous International, acquired and sold private information of Russian officials from 2013 to 2016 and reportedly coordinated with FSB officers who were subsequently arrested for treason.

For more information see CRS Insight IN11559, *SolarWinds Attack—No Easy Fix*, by Chris Jaikaran; CRS Report R46616, *Russian Military Intelligence: Background and Issues for Congress*, by Andrew S. Bowen; and CRS In Focus IF11625, *Russian Armed Forces: Military Doctrine and Strategy*, by Andrew S. Bowen.

**Andrew S. Bowen**, Analyst in Russian and European Affairs

## Disclaimer