(U) Russian Cyber

U.S. ARMY

(U) This infographic provides information on Russian Cyberspace operations: Cyber operations are part of Russia's attempts to control the information environment. Moscow views the information dimension as strategically decisive and critically important to control its domestic populace and influence adversary states. Information warfare is a key means of achieving its ambitions of becoming a dominant player on the world stage. Since at least 2010, the Russian military has prioritized the development of forces and means for what it terms "information confrontation," which is a holistic concept for ensuring information superiority, during peacetime and wartime. This concept includes control of the information content as well as the technical means for disseminating that content.

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. Two primary GRU cyber units have been identified. They reportedly control several research institutes that help develop hacking tools and malware. Cyber analysts have referred to these units collectively as APT (Advanced Persistent Threat) 28, Fancy Bear, Voodoo Bear, Sandworm, and Tsar Team.

- **Unit 26165:** 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. It 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.
- **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

Source:

https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/Russia_Military_Power_Report_2017.pdf

https://crsreports.congress.gov/product/pdf/IF/IF11718

Foreign Intelligence Service (SVR)

The 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 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.

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.

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.