

Russian Threats to the United States

Threat to U.S. Homeland (Brian Cavanaugh)

Among the threats facing the American homeland, Vladimir Putin's Russia stands out as a foreign adversary with an extensive track record of targeting critical civilian and commercial infrastructure to achieve its means. The resurgence of Russian assertiveness on the global stage, coupled with its sophisticated cyber capabilities, poses multifaceted risks that extend beyond conventional military confrontations. With America at the forefront of an increasingly interconnected and technologically advancing world, we cannot afford to ignore the evolving nature of national security threats.

One of the most immediate and insidious threats posed by Russia is in the realm of cybersecurity and information warfare. Much like the cyber threat posed by the Chinese Communist Party, offensive cyber operations from Russia are often in collusion with the Russian state to advance Vladimir Putin's interests. Russian cyber operations have repeatedly demonstrated their capacity to infiltrate critical infrastructure, disrupt essential services, and undermine public confidence in democratic institutions. In Ukraine, Russian cyberattacks have targeted power grids, leading to massive blackouts and causing significant disruption to daily life. The 2015 attack on Ukraine's power grid, which left approximately 230,000 people without electricity, is a stark example of Russia's ability to cripple critical infrastructure. Similarly, the NotPetya malware attack in 2017, which originated in Ukraine but spread globally, inflicted billions of dollars in damages by targeting financial systems, government institutions, and businesses. In the United States, a federal grand jury indicted six Russian officers of the Russian Main Intelligence Directorate (GRU) for their role in the NotPetya attack. The indictment found that American facilities "including hospitals and other medical facilities in the Heritage Valley Health System (Heritage Valley) in the Western District

of Pennsylvania; a FedEx Corporation subsidiary, TNT Express B.V.; and a large U.S. pharmaceutical manufacturer” suffered upwards of \$1 billion in damages from the malware attack.²

Through sophisticated phishing attacks, malware, and social media manipulation, Russian operatives have exploited vulnerabilities and soft targets to influence public opinion and destabilize the political landscape. In 2022, cyberattacks linked to Russian groups targeted Ukrainian telecommunications and media companies, disrupting communications and spreading Russian propaganda during a critical period of military conflict. These activities underscore Russia’s strategy of leveraging cyber capabilities to achieve political and military objectives without direct confrontation.

The implications of such cyber activities and their willingness to use them are profound. An attack on the U.S. power grid, financial systems, or healthcare infrastructure could cause widespread chaos and economic disruption. For instance, the 2020 SolarWinds hack against the Austin, Texas-based software company was attributed to a hacker group supported by the Russian government. The hack infected and compromised systems from numerous U.S. local, state, and federal agencies, including the Departments of Commerce, Homeland Security, State, and Treasury, and private American companies, highlighting the potential for widespread damage.

America’s cyber vulnerabilities are further amplified by the global, just-in-time nature of our supply chains and infrastructure networks: the services from our infrastructure can be disrupted by targeted attacks on our allies and partners. The pervasive nature of these threats requires constant vigilance and robust cybersecurity measures to protect critical infrastructure and maintain public confidence in the stability and security of the nation.

Beyond the cyber realm, Russia’s military ambitions and strategic posturing present direct threats to American interests and security. The annexation of Crimea in 2014 and the ongoing conflict in Eastern Ukraine underscore Russia’s willingness to use military force to achieve its geopolitical goals. This aggression extends to the Arctic region, where Russia has been steadily increasing its military presence and asserting territorial claims, potentially threatening global

2. SIX RUSSIAN GRU OFFICERS CHARGED... OFFICE OF PUBLIC AFFAIRS, U.S. DEPARTMENT OF JUSTICE. [JUSTICE.GOV/OPA/PR/SIX-RUSSIAN-GRU-OFFICERS-CHARGED-CONNECTION-WORLDWIDE-DEPLOYMENT-DESTRUCTIVE-MALWARE-AND](https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and)

shipping routes and access to natural resources.

Russia's development of advanced weapons systems, including hypersonic missiles and nuclear-powered torpedoes, signals a renewed emphasis on military modernization aimed at challenging American military superiority. These advancements not only enhance Russia's strategic capabilities but also pose an unacceptable and unpredictable threat to the American homeland.

Another challenge within the American homeland is Russia's long history of subverting political processes in other countries. By supporting extremist groups, funding propaganda campaigns, and exploiting social divisions, Russia aims to weaken its adversaries and create an environment of perpetual instability. The Kremlin's global propaganda campaign, aimed explicitly at weakening the U.S., has proved particularly effective. For example, over the past two years, Russian state media has become the most watched foreign service network in Latin America, a key region for U.S. national security.³ Sowing societal discord and turning public opinion against the U.S. can destabilize the region, exacerbate vulnerabilities at the southern border, and undermine critical economic relationships with some of the U.S.'s key trading partners.

States must continue to play a key role in strengthening the security and resilience of the homeland. The federal government must support states as they manage and lead this effort at the local level. By implementing cybersecurity protocols, investing in targeted infrastructure upgrades, and securing supply chains, states can effectively combat threats posed by adversaries such as China and Russia and protect America's national security and economic resilience. Russia has repeatedly demonstrated its vast capabilities and willingness to harm Americans at home. Through coordination and proactive measures, states and the federal government can safeguard America's national interests and uphold the principles of democracy, freedom, and economic strength in an era of great power competition.

3. DFRLAB. A GLIMPSE INTO RT'S LATIN AMERICAN AUDIENCE. [MEDIUM.COM/DFRLAB/A-GLIMPSE-INTO-RTS-LATIN-AMERICAN-AUDIENCE-487D52BED507](https://medium.com/dfrlab/a-glimpse-into-rt-s-latin-american-audience-487d52bed507)