CRS INSIGHT

Russia and the U.S. Presidential Election

January 17, 2017 (IN10635)

|

Related Authors

- Catherine A. Theohary
- Cory Welt

|

Catherine A. Theohary, Specialist in National Security Policy and Information Operations (ctheohary@crs.loc.gov, 7-0844)
Cory Welt, Analyst in European Affairs (cwelt@crs.loc.gov, 7-0530)

On January 6, 2016, the Office of the Director of National Intelligence (ODNI) released a declassified report on Russian activities and intentions related to the 2016 U.S. presidential election. The report states that the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) have "high confidence" that Russian President Vladimir Putin "ordered an influence campaign in 2016 aimed at the US presidential election" in order to "undermine public faith in the US democratic process, denigrate [Hillary] Clinton, and harm her electability and potential presidency." The report also contends the Russian government "aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him."

Allegations

Unofficial allegations of Russian interference in the presidential election were made public in or around June 2016. It is alleged that the Russian government illicitly collected and authorized the release of emails and documents of the Democratic National Committee (DNC) and emails of Clinton's campaign chairman John Podesta. These operations were alleged to be part of broader collection efforts against the Democratic Party. Targets included other Clinton campaign staffers (some of whom had emails released) and the Democratic Congressional Campaign Committee (which had emails and personal information released).

Operations focused on the Democratic Party, in turn, were alleged to be part of a broader campaign against U.S. and international targets. In the United States, targets were alleged to have included a number of Republican-connected individuals, including state-level officials and campaigns, as well as former NATO Supreme Allied Commander Phillip Breedlove and former Secretary of State Colin Powell. While collection efforts included Republican targets, FBI Director James Comey stated in a January 10, 2017, hearing that Russian hackers breached and exfiltrated data from "old domains" of the Republican National Committee (RNC) and that investigators found no evidence that the current RNC or the Trump campaign were "successfully hacked." No emails connected to either the committee or the campaign were released.

The majority of emails that were released, including most of those from the DNC and Podesta, were disclosed by Wikileaks, which was alleged to have received emails from Russian intelligence-connected sources. Other emails and materials were released by online persona Guccifer 2.0 and website DC Leaks, both allegedly linked to Russian intelligence.

The ODNI report generally corroborates these claims. It also corroborates further claims that "Russian intelligence accessed elements of multiple state or local electoral boards" and that the Russian government engaged in international propaganda efforts through state-run media and "quasi-government trolls" to praise Trump and denigrate Clinton. While some state-level voter registration systems may have been hacked, the report states there is no evidence of tampering with vote tallies or that information in emails released by Wikileaks had been tampered with prior to their release. It also states that while Russia pursued Republican-affiliated targets, it "did not conduct a comparable disclosure campaign."

Evidence Debate

Previously, the Department of Homeland Security and FBI released a Joint Analysis Report (JAR) on December 29 that also attributes these malicious activities—known collectively as Grizzly Steppe—to Russia. The JAR does not present evidence but instead reveals "indicators of compromise" and actions for network defenders to take using these indicators. As a general practice, the intelligence community does not present evidentiary proof of attribution that is obtained through clandestine collection if there is a possibility of revealing sources and methods and thereby compromising future sources. The lack of clear open source evidence has led some to question the validity of the attribution. In addition, some of the indicators of malicious cyber activity that were reported to be linked to Grizzly Steppe were later proven unrelated.

Potential Impact

While much of the reporting refers to the cyber element of Russian activities, the series of network intrusions, reconnaissance, and data releases appear to be tactical weapons used in support of a broader information warfare campaign around the U.S. presidential election.

Data exfiltration from the networks belonging to both political parties could offer the Russian government insight to the negotiating strategies, redlines, foreign policy goals, and platforms of the incoming administration, whatever the election outcome. Cyber tools were also used to create psychological effects in the American population. The likely collateral effects of these activities include compromising the fidelity of information, sowing discord and doubt in the American public about the validity of intelligence community reports, and prompting questions about the legitimacy of the democratic process itself.

Although it is clear these operations attempted to influence American voters, the January 6 report notes that the Intelligence Community "did not make an assessment of the impact that Russian activities had on the outcome of the 2016 election."

U.S. Response

On December 29, 2016, President Obama imposed sanctions for election-related malicious cyber activity by expanding an existing executive order issued in April 2015. The Obama administration identified nine individuals and entities, including Russia's two leading intelligence agencies, for election-related malicious cyber activity. Designees are subject to blocking of assets under U.S. jurisdiction, prohibitions on transactions with U.S. persons, and (for individuals) denial of entry into the United States. Some have questioned whether sanctions would have a deterrent effect and if more punitive measures should be taken against the Russian government. Based on comments from U.S. officials, there may be additional responses.

The nature of these activities has raised questions as to whether they constitute an act of war or espionage. There are no clear criteria for determining whether a cyberattack should be considered a use of force that could justify a military response. Whether or not Russian cyber activity is declared an act of war, at least two authorities provide for military operations in cyberspace.

Under Title 10, the Department of Defense may conduct offensive cyberspace operations upon direction of the President, subject to the War Powers Resolution (50 U.S.C. 1541). The President may also order a covert operation under Title 50 authorities. Offensive cyberspace operations and influence operations can be examples of covert activities conducted without a formal declaration of war.