COUNCIL on FOREIGN RELATIONS

CFR PRESENTS

Net Politics

*CFR experts investigate the impact of information and communication technologies on security, privacy, and international affairs.*

# After Attributing a Cyberattack to Russia, the Most Likely Response Is Non Cyber

by **Adam Segal**
October 10, 2016

Russian President Vladimir Putin (C) chairs a meeting at the Novo-Ogaryovo state residence outside Moscow, Russia on September 21, 2016. (Sputnik/Kremlin/Alexei Druzhinin via Reuters).

Almost four months after the cybersecurity firm CrowdStrike claimed that two Russian hacker groups were behind the theft of data from computers at the **Democratic National Committee** and other political organizations, the U.S. government has publicly attributed the attacks to Russia. In a **joint statement** from the Director of National Intelligence and Department of Homeland Security, the intelligence community declared that it was "confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations." According to the statement, the hack was not the work of an individual calling himself **Guccifer 2.0** or a **400 pound hacker sitting on a bed**, but was: intended to interfere with the U.S. elections; consistent with other Russian efforts to influence public opinion in Europe and Eurasia; and was likely to have been authorized at the highest levels of the Russian government.

This is the latest in a growing list of cyberattacks that the United States has attributed to state-supported hackers. Washington accused the **PLA of hacking U.S. Steel** and others; **North Korea of attacking Sony**; and seven hackers tied to the **Iranian Revolutionary Guard Corps** of attacks on U.S. financial institutions and a dam in Rye, New York. Russia has, not surprisingly, denied any responsibility, saying the claims "lack proof" and are an attempt to create "**unprecedented anti-Russian hysteria**."

The next steps for the Obama administration are unclear. As **Henry Farrell** notes, the U.S. government will now have to decide if it will provide compelling evidence of Russian culpability. Releasing additional proof will be necessary if the United States wants to build some international legitimacy for whatever retaliatory actions it takes. In fact, the United States signed onto a 2015 UN report that said that accusations of internationally "wrongful acts brought against states"–the kind the United States is accusing Russia —"**should be substantiated**." But substantiation has significant risks. It will be difficult to assign responsibility without revealing intelligence capabilities, and attribution may allow Russia to patch vulnerabilities and result in the loss of U.S. defensive and offensive capabilities.

A number of analysts have stressed the challenges facing the United States in responding to these attacks, and especially in preventing the **confrontation from spinning out of control**. While covert cyber operations would be one example of **a proportional response**—and the United States certainly has the capability to attack Russian networks—it cannot ensure **escalation dominance** and the ability to end the conflict. Attacks that attempt to undermine Putin's legitimacy by exposing emails or financial records and revealing compromising information might provoke even more widespread threats to U.S. critical infrastructure. Moreover, as former NSA general counsel Rajesh De and former CIA deputy director Michael Morrell note, offensive cyberattacks are counterproductive to the norms of behavior that the United States is trying to establish.

This does not mean there should be no reaction. Instead, Washington will want to consider a range of options such as extending sanctions to those around Putin using **a new executive order**, more aid to Estonia and other states on Russia's periphery, and more funds for the development of next generation anonymizing tools for dissidents and non-governmental organizations that monitor the Kremlin. The United States could also take steps to dismantle the IT infrastructure and hop points that Russian intelligence used to compromise U.S. political institutions to disrupt future cyber operations. This could take the form of clandestine activity or publicly visible steps, such as working with the international network of computer emergency response teams much like the **United States did to counteract the 2011-2013 Iranian denial of service attacks against U.S. banks**.

Great powers are still trying to navigate the bounds of acceptable and proportionate responses when faced with confrontational state-sponsored cyber activity. Although analogies to nuclear policy or previous U.S. experience with **Russian *kompromat*** from the past may be helpful to navigate the present, cyberspace has **unique characteristics** that make these imperfect parallels. Washington's response to Moscow's actions will set the bar for future responses and set the example for other countries who could be victim of the same kind of activity. The White House will want to choose its next move carefully.

CFR seeks to foster civil and informed discussion of foreign policy issues. Opinions expressed on CFR blogs are solely those of the author or commenter, not of CFR, which takes no institutional positions. All comments must abide by CFR's **guidelines** and will be moderated prior to posting.

## Pingbacks