What are all these Russian hackers up to?

September 30 2016, by Ryan C. Maness And Margarita Levin Jaitner

Credit: AI-generated image (disclaimer)

Russia has been implicated in many breaches of U.S. networks in recent months, most notably the Democratic National Committee and the Democratic Congressional Campaign Committee hacks, whose data were subsequently dumped to the whistleblowing site WikiLeaks. On Sept. 28, FBI Director James Comey told a congressional hearing that Russian hackers have been testing cyberdefenses of voter registration databases in more than a dozen states.

Last year, hackers working on behalf of the Russian government stole sensitive information from the IRS, the Pentagon, the State Department and the White House.

Hacking groups using names like Cozy Bear and Fancy Bear, and pseudonymous individuals like Guccifer 2.0, are not just targeting the U.S., but are also going after any entity that obstructs the interests of Russia's government.

These hackers are tied to, for example, the recent breach of the World Anti-Doping Agency, making public the health records of many Olympians. That attack was an apparent response to the doping scandal that saw many Russian athletes banned from Olympic competition in Rio de Janeiro – possibly to suggest that it wasn't just Russians who broke the rules. (They have also hacked the email accounts of the whistleblowers who revealed Russia's violations.)

What is Russia trying to do with its hacking efforts? Who are the people doing this? How do we know they're working for Russia, and how closely tied are they to the government? As scholars of Russian cyber-conflict and information warfare, we have learned that this is just Russia's most recent digital effort to benefit its national interests.

Taking on Hillary Clinton

One clear goal for the Russian hackers involved in these recent attacks is to make the presidential campaign harder for Democratic nominee Hillary Clinton and easier for her Republican opponent, Donald Trump. The hack of emails belonging to former Secretary of State Colin Powell was an obvious effort to deepen the private email saga that has damaged Clinton's campaign.

Given the DNC and DCCC hacks, it seems that Russian hackers are

targeting only Clinton and the Democrats. There is evidence that the Republican National Committee was hacked as well, but no documents obtained have yet been made public. Furthermore, the U.S. affiliates of Russian state-owned media outlets such as RT (formerly Russia Today) and Sputnik daily report negative stories about Clinton and upbeat stories about Trump.

There are very good reasons Russian President Vladimir Putin would favor Trump. Trump's views on NATO's relevance, Russia's annexation of Crimea and the Ukraine conflict more generally are music to Putin's ears. By contrast, a Clinton presidency would see a stronger and expanded NATO, increased pressure on Russia over the Ukraine dispute, and even a push to oust Russian allies from powerful positions in the Middle East.

It's impossible to be certain, but a personal conflict may be in play, too: Putin is a patient and calculated seeker of revenge. In Russia's 2011-2012 legislative and presidential elections, Putin's United Russia Party won big, and Putin was again elected president by large margins. Some election watchdogs cried foul, alleging stuffed ballots and overcounts for the United Russia candidates. Then Secretary of State Clinton demanded further investigations, which lent support to anti-Putin demonstrations across Russia.

Understanding Russian information warfare

Russia has a long history of using information as a political and military tool. Domestically, the practice of doctoring and censoring information dates back to the beginnings of the commercial newspaper industry during the late years of imperial Russia. It continued, in an ever more sophisticated form, throughout the Soviet era.

Using information as a support for domestic political systems led to its

use as a lever in foreign affairs and a weapon in military conflict. That did not disappear with the dissolution of the Soviet Union. Rather, decades-old methods have been used in new ways.

Some Russian cyberattacks made headlines for backfiring. The large-scale DDoS attack on Estonia in 2007, a response to the relocation of a Soviet war memorial, failed. In fact, it pushed Estonia to build some of the world's strongest cyberdefenses.

A year later, Russia brought information warfare to its conflict with Georgia. Targeting Georgian communications, both online and physically, its efforts were not only aimed at providing an advantage for troops on the ground. They also had the goal of preventing the spread of objections to Russia's forcible annexation of the Georgian territories of Abkhazia and South Ossetia. Word got out anyway.

Similar efforts have been under way in Russia since the beginnings of the Ukraine crisis. Sometimes they have been unimaginative and unsuccessful; other efforts have been more effective.

For example, many people still question the "Western" version of the Malaysia Airlines 17 plane crash, which pins the blame on Russia or the Kremlin-backed separatists in Ukraine. This skepticism is an effect of Russian propaganda. While the Russian versions have failed to convince most people, they still have spread doubts about who actually shot down the airliner in 2014.

Taking on the West

Russia conducts both overt and covert information operations in Europe and the U.S. The overt methods include using state-owned Russian media outlets to inject pro-Russian narratives into the political discourse. Less visible efforts include having individuals and groups spread Russia's

messages, a phenomenon that has become known as a "troll army." Also, well-placed individuals and interest groups spread Russian narratives in support of their own causes, with some even being paid for their support.

As with the Malaysia Airlines 17 narrative, credibility is not always Russia's main goal. Rather, it's just trying to spread distrust of official viewpoints, particularly those coming from the EU or NATO. With any Western fringe group Russia can attract, it is attempting to stall Western decisions, sow discontent and distrust, and draw apart societies and partnerships.

We are now seeing this tactic making inroads in the American political discourse. For example, the DNC emails released by WikiLeaks showed party leaders' prejudices against insurgent candidate Bernie Sanders, and their efforts to divert DNC funds to help Clinton win the nomination.

Although the revelations don't disclose anything illegal, the popular narrative from many U.S. media outlets was that the DNC unduly influenced the outcome of the primary. That divided the Democratic Party, potentially giving Trump an advantage.

Similarly, recent DCCC voting list releases shouldn't have any direct effect on the electoral outcomes in November, but spread doubt about the legitimacy of the election. There's also no way to say whether it worked – if Trump ends up winning, it'll be impossible to say any of these leaks was the cause.

Ties to the Russian government

There are some advantages to taking on adversaries in cyberspace, rather than the physical world. It is less costly in terms of risk and escalation: Conventional espionage would require physical infiltrations and, if caught, could spark an escalating crisis between Russia and the U.S.

Cyberspace is also relatively ungoverned by international law and a much easier place to achieve plausible deniability.

Despite evidence to the contrary, the Russian government has denied any involvement or collusion with Cozy Bear, Fancy Bear, Guccifer 2.0, the Dukes and Quedagh. Usually malicious nonstate group cyberattackers are motivated by money – but these groups and individuals seem to be focused on stealing information that could be used geopolitically against Russia's adversaries. That suggests a direct connection to the Russian government.

Key to stopping these incursions will be improving American cyber-hygiene practices, building more resilient networks throughout the public and private sectors and promoting international cyber-norms. Therefore, perhaps contrary to the sophisticated cyberattacks it has launched in the past, the U.S. must cooperate with international efforts to improve global cybersecurity.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation