The Washington Post

National Security

U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms

By Ellen Nakashima
February 27

The U.S. military blocked Internet access to an infamous Russian entity seeking to sow discord among Americans during the 2018 midterms, several U.S. officials said, a warning that the Kremlin's operations against the United States are not cost-free.

The strike on the Internet Research Agency in St. Petersburg, a company underwritten by an oligarch close to President Vladimir Putin, was part of the first offensive cyber-campaign against Russia designed to thwart attempts to interfere with a U.S. election, the officials said.

"They basically took the IRA offline," according to one individual familiar with the matter who, like others, spoke on the condition of anonymity to discuss classified information. "They shut them down."

The operation marked the first muscle-flexing by U.S. Cyber Command, with intelligence from the National Security Agency, under new authorities it was granted by President Trump and Congress last year to bolster offensive capabilities. The president approved of the general operation to prevent Russian interference in the midterms, officials said.

Whether the impact of the St. Petersburg action will be long-lasting remains to be seen. Russia's tactics are evolving, and some analysts were skeptical that the strike would deter the Russian troll factory or Putin, who, according to U.S. intelligence officials, ordered an "influence" campaign in 2016 to undermine faith in U.S. democracy. U.S. officials have also assessed that the Internet Research Agency works on behalf of the Kremlin.

"Such an operation would be more of a pinprick that is more annoying than deterring in the long run," said Thomas Rid, a strategic-studies professor at Johns Hopkins University who was not briefed on the details.

Some U.S. officials argued that "grand strategic deterrence" is not always the goal. "Part of our objective is to throw a little curveball, inject a little friction, sow confusion," said one defense

official. “There’s value in that. We showed what’s in the realm of the possible. It’s not the old way of doing business anymore.”

The action has been hailed as a success by Pentagon officials, and some senators credited Cyber Command with averting Russian interference in the midterms.

“The fact that the 2018 election process moved forward without successful Russian intervention was not a coincidence,” said Sen. Mike Rounds (R-S.D.), who did not discuss the specific details of the operation targeting the St. Petersburg group. Without Cybercom’s efforts, he said, there “would have been some very serious cyber-incursions.”

Cybercom and the NSA declined to comment.

Kremlin spokesman Dmitry Peskov asserted Wednesday that “in general” there are a “huge number of cyberattacks against various Russian organizations, legal entities and private individuals from the territory” of the United States. “This is the reality now in which we live,” he told reporters. He added that such threats underscore the need for a “sovereign Internet” in Russia.

The disruption to the Internet Research Agency’s networks took place as Americans went to the polls and a day or so afterward as the votes were tallied, to prevent the Russians from mounting a disinformation campaign that cast doubt on the results, according to officials.

The blockage was so frustrating to the trolls that they complained to their system administrators about the disruption, the officials said.

The Internet Research Agency as early as 2014 and continuing through the 2016 presidential election sought to undermine the U.S. political system, according to the Justice Department. Posing as Americans and operating social media pages and groups, Russian trolls sought to exacerbate tensions over issues such as race, sexual identity and guns.

The agency, according to federal prosecutors, is financed by Yevgeniy Prigozhin, a tycoon from St. Petersburg and an ally of Putin. Prigozhin, the Internet Research Agency and a company Prigozhin runs called Concord Management and Consulting were among 16 Russian individuals and companies a grand jury indicted a year ago as part of special counsel Robert S. Mueller III’s investigation into Russian interference in the 2016 election.

In response to questions from The Washington Post, Prigozhin said in a statement on the Russian version of Facebook, “I cannot comment on the work of the Internet Research Agency in any way

because I have no relation to it." Concord Management declined to comment, citing the ongoing litigation in the United States.

Another element of the Cyber Command campaign, first reported by the New York Times, involved "direct messaging" that targeted the trolls as well as hackers who work for the Russian military intelligence agency, the GRU. Using emails, pop-ups, texts or direct messages, U.S. operatives beginning in October let the Russians know that their real names and online handles were known and that they should not interfere in other nations' affairs, defense officials said.

Some Internet Research Agency officials were so perturbed by the messaging that they launched an internal investigation to root out what they thought were insiders leaking personnel information, according to two individuals.

The operation was part of a broader government effort to safeguard the 2018 elections, involving the Homeland Security, State and Justice departments, as well as the FBI. It was led by Gen. Paul Nakasone, who in July formed the Russia Small Group, made up of 75 to 80 people from Cybercom and the NSA, which are part of the Defense Department.

When Nakasone took the helm at the NSA and Cybercom in May, the White House and then-Defense Secretary Jim Mattis told him his priority needed to be the defense of the midterm elections, officials said. No one wanted a repeat of the 2016 campaign, when the GRU hacked Democratic Party computers and released troves of emails, and when the Internet Research Agency mounted its social media campaign to exploit social divisions.

In August, Director of National Intelligence Daniel Coats said Russia was continuing "a pervasive messaging campaign" to try to weaken and divide the United States, though officials concluded it was not as aggressive as the 2016 operation by Russia.

Two new U.S. authorities facilitated the move against the Internet Research Agency. A presidential order in August gave Cybercom greater latitude to undertake offensive operations below the level of armed conflict — actions that would not result in death, significant damage or destruction. And a provision in the National Defense Authorization Act passed last year also cleared the way for clandestine cyber-operations that fall below that same threshold, categorizing them as "traditional military activity."

"The calculus for us here was that you're just pushing back in the same way that the adversary has for years," a second defense official said. "It's not escalatory. In fact, we're finally in the game."

Other officials were more circumspect.

“Causing consternation or throwing sand in the gears may raise the cost of engaging in nefarious activities, but it is not going to cause a nation state to just drop their election interference or their malign influence in general,” a third official said. “It’s not going to convince the decision-maker at the top.”

The operation also was the first real test of Cybercom’s new strategy of “persistent engagement,” issued in April, involving continually confronting the adversary and sharing information with partners. Cybercom in fall 2018 sent troops to Montenegro, Macedonia and Ukraine to help shore up their network defenses, and the Americans were able to obtain unfamiliar malware samples that private security researchers traced to the GRU, according to officials.

The Cybercom campaign also was part of what Nakasone described in an interview with Joint Force Quarterly as “acting outside our borders, being outside our networks, to ensure that we understand what our adversaries are doing.”

Joseph Marks in Washington and Amie Ferris-Rotman in Moscow contributed to this report.

Ellen Nakashima
Ellen Nakashima is a national security reporter for The Washington Post. She covers cybersecurity, surveillance, counterterrorism and intelligence issues. She has also served as a Southeast Asia correspondent and covered the White House and Virginia state politics. She joined The Post in 1995.