The New York Times

U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections

By Julian E. Barnes

Oct. 23, 2018

WASHINGTON — The United States Cyber Command is targeting individual Russian operatives to try to deter them from spreading disinformation to interfere in elections, telling them that American operatives have identified them and are tracking their work, according to officials briefed on the operation.

The campaign, which includes missions undertaken in recent days, is the first known overseas cyberoperation to protect American elections, including the November midterms.

The operations come as the Justice Department outlined on Friday a campaign of "information warfare" by Russians aimed at influencing the midterm elections, highlighting the broad threat the American government sees from Moscow's influence campaign.

Defense officials would not say how many individuals they were targeting, and they would not describe the methods that Cyber Command has used to send the direct messages to the operatives behind the influence campaigns. It is not clear if the information was delivered in an email, a chat or some other electronic intervention.

Senior defense officials said they were not directly threatening the operatives. Still, former officials said anyone singled out would know, based on the United States government's actions against other Russian operatives, that they could be indicted or targeted with sanctions. Even the unstated threat of sanctions could help deter some Russians from participating in covert disinformation campaigns, said Andrea Kendall-Taylor, a former intelligence official now with the Center for a New American Security.

"This would be a way to generate leverage that can change behavior," she said.

The Cyber Command operations appear relatively measured, especially in comparison with the increasingly elaborate and sophisticated efforts by Russia to use disinformation to sow dissent in the United States.

But the American campaign undertaken in response to Russia's information offensive is limited in large part to keep Moscow from escalating in response by taking down the power grid or conducting some other reprisal that could trigger a bigger clash between great powers. Compared with traditional armed conflict, the rules of cyberwarfare are not well defined.

Cyber Command was founded in 2009 to defend military networks but has also developed offensive capabilities. The command shares a headquarters and leadership with the National Security Agency, which collects electronic and signals intelligence. A joint Cyber Command-N.S.A. team has been working on the effort to identify and deter foreign influence campaigns.

American officials also said the campaign is one aspect of a broader effort, which includes purges by social media companies of fake accounts that spread propaganda, to fight Russian intrusion in democratic elections. Cyber Command has also sent teams to Europe to shore up the defenses of American allies and partners so they can combat Russian intrusions on their own government networks, according to defense officials.

American intelligence officials have concluded that Russia is unlikely to try to hack into voting machines or directly manipulate voting results this year. On Friday, the director of national intelligence said that state and local governments have reported attempted intrusions into their networks, but that foreign governments have not penetrated voting systems.

But Russian efforts to sway public opinion by spreading false information have continued, and officials said those efforts are becoming more refined, targeting specific groups of Americans. Almost all of the Russian disinformation efforts, according to current and former officials, are aimed at sowing dissent, polarizing the political parties and setting the stage for the 2020 presidential election.

The defense officials would not identify their targets. But other officials said some of the targets were involved in previous Russian efforts to spread disinformation in the United States and Europe, including the 2016 presidential election. The new American campaign, according to these officials, is aimed at both oligarch-funded hacking groups and Russian intelligence operatives who are part of Moscow's disinformation campaign. It is not clear whether Cyber Command's effort is also aimed at halting Russian operatives charged with hacking political entities.

Others said the American government must be ready to go further — cutting off the Russians' ability to spread propaganda.

"It is very important to identify the source and essentially be able to neutralize that source," said Laura Rosenberger, the director of the Alliance for Securing Democracy and a former Obama administration official. "These are networks that operate. The more we can identify the key nodes in those networks and remove them by taking them offline is really how we will get at this problem in a systemic way and not play Whac-a-Mole."

Gen. Paul M. Nakasone, the head of Cyber Command and the National Security Agency, hinted at the new cyberoperations this month as he noted that American adversaries are "looking to really take us on below that level of armed conflict" by sowing distrust in society and "attempt to disrupt our elections."

"This is what great power competition looks like today, and it's what we will look at as we look to the future," he said during a panel discussion in Washington.

Cyber Command has a relatively short history of overseas operations against adversaries, but it did conduct missions aimed at curtailing the ability of the Islamic State to spread propaganda and recruit online. Those operations, which included efforts to freeze computers, yielded mixed results.

Sheryl Sandberg, left, and Jack Dorsey, executives at Facebook and Twitter, testified before Congress recently about Russian social media campaigns to interfere in American elections. Twitter and Facebook purges of Russian accounts have reduced the effectiveness of the propaganda, outside experts say. Tom Brenner for The New York Times

Assessing the effectiveness of American cyberoperations at this point is difficult. The director of national intelligence, Dan Coats, is expected to complete a review after the November midterm elections.

But some American officials said they believed the initial operations had at least partly diminished the effectiveness of Moscow's election manipulation effort.

Similarly, British officials also said they had seen less activity by Russian propagandists than expected after their identification of the Russian intelligence agents behind the poisoning in the spring of a former Russian spy and the Dutch authorities' detailing this month of a failed Russian cyberattack on the Organization for the Prohibition of Chemical Weapons.

Outside experts believe that a major reason Russian social media trolls are less effective is aggressive work by technology companies. Twitter and Facebook purges of Russian-created or -controlled accounts have reduced the effectiveness of Moscow's propaganda, said Ben Nimmo, an expert on Russia's online misinformation efforts at the Atlantic Council's Digital Forensic Research Lab.

Some American officials have said they were frustrated by what they viewed as President Trump's timidity at taking on the Russians involved in election meddling. Mr. Trump has frequently wavered about whether he believes the Russians interfered in the 2016 elections to help his bid for the presidency.

But officials said broad agreement existed throughout the rest of the government that the Russian interference campaign was ongoing and required a more muscular response to deter further meddling.

With the new campaign, American officials said, they are trying to hamper Russia from meddling in the 2018 vote and deter future efforts. Cyber Command's new operations reflect a push by Defense Secretary Jim Mattis to expand the Pentagon's role countering Russian hackers threatening America and its allies. In the White House, John R. Bolton, the national security adviser, has also been pushing to speed up approval for election defense operations.

Mr. Bolton announced new cyberwarfare authorities last month, but the White House provided few details. Under the new guidelines, Mr. Trump has handed off approval for certain actions to the National Security Council, secretary of defense or head of Cyber Command, depending on the operation.

In the final months of the Obama administration, as details of Russia's interference in the 2016 election were uncovered, officials privately pushed Cyber Command and the National Security Agency to create options to respond.

Cyber Command and the N.S.A. were hesitant to offer options, a former official said, out of concern that if they tried to directly deter Moscow's activities, Russian operatives would learn too much about America's espionage techniques, among the government's most closely held secrets.

Since taking the helm of Cyber Command and the N.S.A. in May, General Nakasone has said he has the authority to act against adversaries threatening American elections. Inside both the command and the agency, he has pushed to develop new options to deter interference.

American officials say the Russian effort to destabilize the American elections is closely tied to Moscow's work in Europe.

The criminal complaint unsealed on Friday showed that Elena Alekseevna Khusyaynova, the St. Petersburg accountant involved in the disinformation campaign in the United States, was also active in Europe, including in Ukraine, considered the focus of Moscow's efforts to weaken its neighbors and the West.

Cyber Command has also sent teams to Ukraine, Macedonia and Montenegro to build up defenses against Russian hackers intent on penetrating government networks on its doorstep in Eastern Europe.

The United States is helping Montenegro remove Russian cyberoperatives from nonclassified government systems, a senior Montenegrin official said. Painstaking work, the effort could take months to find and close all the access points Russian hackers have created. Russians have not penetrated the government's classified systems, the official said.

European leaders have been asking the United States to take a bigger role in helping block Russian meddling and cyberactivity.

Lithuania is working with the United States on military cyberdefense training as well as research and development on cyberdefenses, President Dalia Grybauskaite said an interview. But Ms. Grybauskaite has also pushed for expanded cooperation, including a rotating presence of military experts at Lithuania's cyberdefense center.

"What we see is a steadily growing pressure on cyber, the information front, propaganda and, recently, fake news," Ms. Grybauskaite said. "Their efforts and instruments are becoming more sophisticated every day."

Helene Cooper and Eric Schmitt contributed reporting.

A version of this article appears in print on Oct. 24, 2018, on Page A20 of the New York edition with the headline: U.S. Begins Cyberoperation Against Russia in Effort to Protect Elections