The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

U.S. Cyberattacks May Be Doing Putin a Favor

The Kremlin is going to spin the alleged cyberattack for its own purposes.

By Leonid Bershidsky

February 28, 2019



Jonathan Ernst / Ready

The U.S.'s claims that it successfully denied internet access last year to a Russian troll factory are highly dubious. But if America is changing its tactics by going on the offensive against Russian cyber threats, it would be a significant development for the future course of the two countries' internet skirmishes, and Russia can be expected to take countermeasures that would hurt its own citizens first and foremost.

The Washington Post reported this week that the U.S. Cyber Command temporarily took offline the servers of the Internet Research Agency during the 2018 midterm elections. The St. Petersburg-based organization had been in the news before: Its workers were indicted by

Special Counsel Robert Mueller last year for allegedly running a disinformation campaign during the 2016 U.S. presidential campaign. The indictment and media reports link the troll farm to Yevgeny Prigozhin, a catering and security entrepreneur with strong Kremlin ties and large Russian government contracts, though he denies any connection.

The Pentagon hasn't released any technical details of the attack, but the New York Times reported that the Cyber Command sent IRA staffers direct messages letting them know their identities were no secret to U.S. intelligence. On Thursday, the Federal News Agency, another Russian outfit linked to Prigozhin (both deny any connection to each other), published what it called an "investigation" of the U.S. cyberattack.

Related article: Kremlin Says Cyber Attacks on Russia Often Launched From U.S. Territory

It claimed that some of its own staffers had received "threatening text messages in broken Russian from African mobile numbers and e-mails in broken Russian calling on journalists to 'think about their activities.'" Then, according to the investigation, a FNA staffer's iPhone was hacked, and the agency's internal office server came under attack on Nov. 5, and two of its four hard drives were taken down. Also, hard disks were erased on servers rented by USAReally, an English-language website whose logo looks almost exactly like the FNA'S, in Sweden and Estonia. "The U.S. Cyber Command's attack failed completely," FNA wrote. "The FNA office wasn't 'paralyzed' and USAReally continued to work normally."

In any case, it doesn't make a lot of practical sense to take down a troll farm on the day before an election: A successful disinformation campaign would have been underway for many months. It's also hard to imagine that the IRA, the FNA or any of their sister organizations could have mounted a useful campaign ahead of the midterms: They aren't big or sophisticated enough to watch and comment intelligently and disruptively on a large number of races all over the U.S.; that would be much harder than creating memes and emotional tweets about two presidential candidates.

If the U.S. Cyber Command did attack the troll factory, it was to demonstrate its capabilities and serve notice that America was changing tactics. The U.S. is trying to tell Russian hackers and trolls that it won't passively watch their activities anymore and that they should expect to be counterattacked.

There are clear signs the message has been received — and that the Kremlin is going to spin it for its own purposes.

The day after the Washington Post report, state-owned Russian media ran articles alleging that the U.S. is capable of taking Russia off the internet. That isn't credible. The technical difficulty would be mind-boggling: Russia is linked to the rest of the world by a myriad of channels owned by private companies, many of which aren't Western. Besides, it's hard to imagine how the U.S. would benefit from taking all of Russia offline. Sure, the trolls would be hindered, but the West would lose its best conduit for sharing information with Russians.

But the Kremlin wants Russians to get the idea that their web access can be turned off from the U.S. Even before the Washington Post report last week, President Vladimir Putin talked of a threat, though he said the U.S. would shoot itself in the foot if it took Russia down. "It's their

invention, so they sit there and see and read what you're saying and stockpiling defense information," Putin said, referring to the internet. "I believe they'll think it over 100 times before doing it. But theoretically it's possible. So we, of course, must create such segments that don't depend on anyone."

On Thursday, Putin's spokesman Dmitry Peskov added some spin. "Because of such potential threats, lawmaking activity is under way that includes the so-called sovereign internet bill," he said.

Related article: Two Senior Russian Cybersecurity Experts Convicted of Treason. And the Legacy of Media Executive Igor Malashenko

The bill in question received the Russian Parliament's preliminary approval on Feb. 12. Technical experts have condemned it as poorly written, but essentially, it decrees the creation of a system of filters at Russia's virtual borders that would allow the government to cut off specific traffic flows or all traffic. If implemented, the new rules would establish a Russian version of China's "Great Firewall" in the name of keeping Russian internet resources online if the U.S. decides to take them down.

Russian legislators have 30 days to present amendments to the bill, but with Putin's support the measure is likely to be passed with few amendments. A preliminary estimate puts the initial cost at 25 billion rubles ($380 million).

So it appears that the Russian answer to the U.S. threat of offensive action in cyberspace is to set up a system that can, if needed, isolate Russia from any foreign attack. But from the point of view of a Russian internet user, the U.S. Cyber Command and the Kremlin might as well be working together to sell Russia on a system that would have other uses, too — for example, shutting down access to communication platforms that refuse to share information with Russian intelligence. Without a "Great Firewall," the Russian authorities have been unable completely to shutter one such platform, Telegram, despite months of effort.

Users' best hope is that the cyberwar isn't being fought by both sides' best experts (those are otherwise occupied, working for Google or building fintech start-ups). Then, U.S. attacks will be as unimpressive as the one on the troll farm, and Russian defenses will have enough holes in them to allow Russians still to get access to the information they want. For now, at least, that hope isn't lost.

This opinion piece was first published by Bloomberg View.

The views expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.

Original url:
https://www.themoscowtimes.com/2019/02/28/us-cyberattacks-may-be-doing-putin-a-favor-a64667