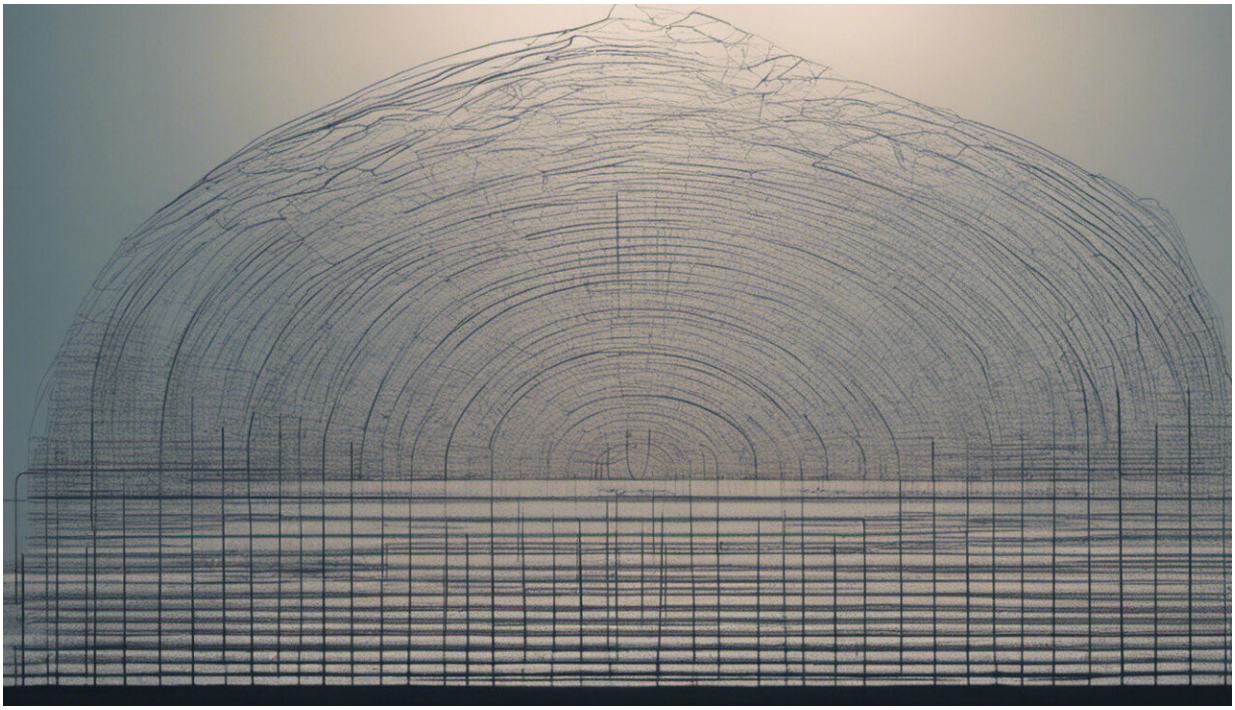
Tracing the sources of today's Russian cyberthreat

August 16 2017, by Dorothy Denning



Credit: AI-generated image (disclaimer)

Beyond carrying all of our phone, text and internet communications, cyberspace is an active battleground, with cybercriminals, government agents and even military personnel probing weaknesses in corporate, national and even personal online defenses. Some of the most talented and dangerous cybercrooks and cyberwarriors come from Russia, which

is a longtime meddler in other countries' affairs.

Over decades, Russian operators have stolen terabytes of data, taken control of millions of computers and raked in billions of dollars. They've shut down electricity in Ukraine and meddled in elections in the U.S. and elsewhere. They've engaged in disinformation and disclosed pilfered information such as the emails stolen from Hillary Clinton's campaign chairman, John Podesta, following successful spearphishing attacks.

Who are these operators, why are they so skilled and what are they up to?

Back to the 1980s

The Russian cyberthreat dates back to at least 1986 when Cliff Stoll, then a system administrator at Lawrence Berkeley National Laboratory, linked a 75-cent accounting error to intrusions into the lab's computers. The hacker was after military secrets, downloading documents with important keywords such as "nuclear." A lengthy investigation, described in Stoll's book "The Cuckoo's Egg," led to a German hacker who was selling the stolen data to what was then the Soviet Union.

By the late 1990s, Russian cyberespionage had grown to include the multi-year "Moonlight Maze" intrusions into U.S. military and other government computers, foretelling the massive espionage from Russia today.

The 1990s also saw the arrest of Vladimir Levin, a computer operator in St. Petersburg. Levin tried to steal more than US$10 million by hacking Citibank accounts, foreshadowing Russia's prominence in cybercrime. And Russian hackers defaced U.S. websites during the Kosovo conflict, portending Russia's extensive use of disruptive and damaging cyberattacks.

Conducting advanced attacks

In more recent years, Russia has been behind some of the most sophisticated cyberattacks on record. The 2015 cyberattack on three of Ukraine's regional power distribution companies knocked out power to almost a quarter-million people. Cybersecurity analysts from the Electricity Information Sharing and Analysis Center and the SANS Institute reported that the multi-staged attacks were conducted by a "highly structured and resourced actor." Ukraine blamed the attacks on Russia.

The attackers used a variety of techniques and adapted to the targets they faced. They used spearphishing email messages to gain initial access to systems. They installed "BlackEnergy" malware to establish remote control over the infected devices. They harvested credentials to move through the networks. They developed custom malicious firmware to render system control devices inoperable. They hijacked the Supervisory Control and Data Acquisition system to open circuit breakers in substations. They used "KillDisk" malware to erase the master boot record of affected systems. The attackers even went so far as to strike the control stations' battery backups and tie up the energy company's call center with thousands of calls.

The Russians returned in 2016 with more advanced tools to take down a major artery of Ukraine's power grid. Russia is believed to have also invaded energy companies in the U.S., including those operating nuclear power plants.

Top-notch cybereducation

Russia has many skilled cyberoperators, and for good reason: Their educational system emphasizes information technology and computer

science, more so than in the U.S.

Every year, Russian schools take a disproportionate number of the top spots in the International Collegiate Programming Contest. In the 2016 contest, St. Petersburg State University took the top spot for the fifth time in a row, and four other Russian schools also made the top 12. In 2017, St. Petersburg ITMO University won, with two other Russian schools also placing in the top 12. The top U.S. school ranked 13th.

As Russia prepared to form a cyberbranch within its military, Minister of Defense Sergei Shoigu took note of Russian students' performance in the contest. "We have to work with these guys somehow, because we need them badly," he said in a public meeting with university administrators.

Who are these Russian cyberwarriors?

Russia employs cyberwarriors within its military and intelligence services. Indeed, the cyberespionage groups dubbed APT28 (aka Fancy Bear) and APT29 (aka Cozy Bear and The Dukes) are believed to correspond to Russia's military intelligence agency GRU and its state security organization FSB, respectively. Both groups have been implicated in hundreds of cyberoperations over the past decade, including U.S. election hacking.

Russia recruits cyberwarriors from its colleges, but also from the cybersecurity and cybercrime sectors. It is said to turn a blind eye to its criminal hackers as long as they avoid Russian targets and use their skills to aid the government. According to Dmitri Alperovitch, co-founder of the security firm CrowdStrike, when Moscow identifies a talented cybercriminal, any pending criminal case against the person is dropped and the hacker disappears into the Russian intelligence services. Evgeniy Mikhailovich Bogachev, wanted by the FBI with a reward of $3 million

for cybercrimes, is also on the Obama administration's list of people sanctioned in response to interference in the U.S. election. Bogachev is said to work "under the supervision of a special unit of the FSB."

Allies outside official channels

Besides its in-house capabilities, the Russian government has access to hackers and the Russian media. Analyst Sarah Geary at cybersecurity firm FireEye reported that the hackers "disseminate propaganda on behalf of Moscow, develop cybertools for Russian intelligence agencies like the FSB and GRU, and hack into networks and databases in support of Russian security objectives."

Many seemingly independent "patriotic hackers" operate on Russia's behalf. Most notably, they attacked critical systems in Estonia in 2007 over the relocation of a Soviet-era memorial, Georgia in 2008 during the Russo-Georgian War and Ukraine in 2014 in connection with the conflict between the two countries.

At the very least, the Russian government condones, even encourages, these hackers. After some of the Estonian attacks were traced back to Russia, Moscow turned down Estonia's request for help – even as a commissar in Russia's pro-Kremlin youth movement Nashi admitted launching some of the attacks. And when Slavic Union hackers successfully attacked Israeli websites in 2006, Deputy Duma Director Nikolai Kuryanovich gave the group a certificate of appreciation. He noted that "a small force of hackers is stronger than the multi-thousand force of the current armed forces."

While some patriotic hackers may indeed operate independently of Moscow, others seem to have strong ties. Cyber Berkut, one of the groups that conducted cyberattacks against Ukraine, including its central election site, is said to be a front for Russian state-sponsored

cyberactivity. And Russia's espionage group APT28 is said to have operated under the guise of the ISIS-associated CyberCaliphate while attacking the French station TV5 Monde and taking over the Twitter account of U.S. Central Command.

One of many cyberthreats

Although Russia poses a major cyberthreat, it is not the only country that threatens the U.S. in cyberspace. China, Iran and North Korea are also countries with strong cyberattack capabilities, and more countries will join the pool as they develop their people's skills.

The good news is that actions to protect an organization's cybersecurity (such as monitoring access to sensitive files) that work against Russia also work against other threat actors. The bad news is that many organizations do not take those steps. Further, hackers find new vulnerabilities in devices and exploit the weakest link of all – humans. Whether cyberdefenses will evolve to avert a major calamity, from Russia or anywhere else, remains to be seen.

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

Provided by The Conversation

Citation: Tracing the sources of today's Russian cyberthreat (2017, August 16) retrieved 27 April 2024 from https://techxplore.com/news/2017-08-sources-today-russian-cyberthreat.html