The New York Times

U.S. Escalates Online Attacks on Russia's Power Grid

By David E. Sanger and Nicole Perlroth

June 15, 2019

WASHINGTON — The United States is stepping up digital incursions into Russia's electric power grid in a warning to President Vladimir V. Putin and a demonstration of how the Trump administration is using new authorities to deploy cybertools more aggressively, current and former government officials said.

In interviews over the past three months, the officials described the previously unreported deployment of American computer code inside Russia's grid and other targets as a classified companion to more publicly discussed action directed at Moscow's disinformation and hacking units around the 2018 midterm elections.

Advocates of the more aggressive strategy said it was long overdue, after years of public warnings from the Department of Homeland Security and the F.B.I. that Russia has inserted malware that could sabotage American power plants, oil and gas pipelines, or water supplies in any future conflict with the United States.

But it also carries significant risk of escalating the daily digital Cold War between Washington and Moscow.

Listen to 'The Daily': Hacking the Russian Power Grid

Attacks by the United States risk escalating a digital Cold War and renew questions about whether certain targets should be off limits in cyber conflict.

The administration declined to describe specific actions it was taking under the new authorities, which were granted separately by the White House and Congress last year to United States Cyber Command, the arm of the Pentagon that runs the military's offensive and defensive operations in the online world.

But in a public appearance on Tuesday, President Trump's national security adviser, John R. Bolton, said the United States was now taking a broader view of potential digital targets as part of an effort "to say to Russia, or anybody else that's engaged in cyberoperations against us, 'You will pay a price.'"

Power grids have been a low-intensity battleground for years.

Since at least 2012, current and former officials say, the United States has put reconnaissance probes into the control systems of the Russian electric grid.

But now the American strategy has shifted more toward offense, officials say, with the placement of potentially crippling malware inside the Russian system at a depth and with an aggressiveness that had never been tried before. It is intended partly as a warning, and partly to be poised to conduct cyberstrikes if a major conflict broke out between Washington and Moscow.

The commander of United States Cyber Command, Gen. Paul M. Nakasone, has been outspoken about the need to "defend forward" deep in an adversary's networks to demonstrate that the United States will respond to the barrage of online attacks aimed at it.

President Trump's national security adviser, John R. Bolton, said the United States was taking a broader view of potential digital targets as part of an effort to warn anybody "engaged in cyberoperations against us." Doug Mills/The New York Times

"They don't fear us," he told the Senate a year ago during his confirmation hearings.

But finding ways to calibrate those responses so that they deter attacks without inciting a dangerous escalation has been the source of constant debate.

Mr. Trump issued new authorities to Cyber Command last summer, in a still-classified document known as National Security Presidential Memoranda 13, giving General Nakasone far more leeway to conduct offensive online operations without receiving presidential approval.

But the action inside the Russian electric grid appears to have been conducted under little-noticed new legal authorities, slipped into the military authorization bill passed by Congress last summer. The measure approved the routine conduct of "clandestine military activity" in cyberspace, to "deter, safeguard or defend against attacks or malicious cyberactivities against the United States."

Under the law, those actions can now be authorized by the defense secretary without special presidential approval.

"It has gotten far, far more aggressive over the past year," one senior intelligence official said, speaking on the condition of anonymity but declining to discuss any specific classified programs. "We are doing things at a scale that we never contemplated a few years ago."

The critical question — impossible to know without access to the classified details of the operation — is how deep into the Russian grid the United States has bored. Only then will it be clear whether it would be possible to plunge Russia into darkness or cripple its military — a question that may not be answerable until the code is activated.

Both General Nakasone and Mr. Bolton, through spokesmen, declined to answer questions about the incursions into Russia's grid. Officials at the National Security Council also declined to comment but said they had no national security concerns about the details of The New York Times's reporting about the targeting of the Russian grid, perhaps an indication that some of the intrusions were intended to be noticed by the Russians.

Speaking on Tuesday at a conference sponsored by The Wall Street Journal, Mr. Bolton said: "We thought the response in cyberspace against electoral meddling was the highest priority last year, and so that's what we focused on. But we're now opening the aperture, broadening the areas we're prepared to act in."

He added, referring to nations targeted by American digital operations, "We will impose costs on you until you get the point."

Gen. Paul Nakasone, the commander of United States Cyber Command, was given more leeway to conduct offensive online operations without obtaining presidential approval. Erin Schaff for The New York Times

Two administration officials said they believed Mr. Trump had not been briefed in any detail about the steps to place "implants" — software code that can be used for surveillance or attack — inside the Russian grid.

Pentagon and intelligence officials described broad hesitation to go into detail with Mr. Trump about operations against Russia for concern over his reaction — and the possibility that he might countermand it or discuss it with foreign officials, as he did in 2017 when he mentioned a sensitive operation in Syria to the Russian foreign minister.

Because the new law defines the actions in cyberspace as akin to traditional military activity on the ground, in the air or at sea, no such briefing would be necessary, they added.

The intent of the operations was described in different ways by several current and former national security officials. Some called it "signaling" Russia, a sort of digital shot across the bow. Others said the moves were intended to position the United States to respond if Mr. Putin became more aggressive.

So far, there is no evidence that the United States has actually turned off the power in any of the efforts to establish what American officials call a "persistent presence" inside Russian networks, just as the Russians have not turned off power in the United States. But the placement of malicious code inside both systems revives the question of whether a nation's power grid — or other critical infrastructure that keeps homes, factories, and hospitals running — constitutes a legitimate target for online attack.

Already, such attacks figure in the military plans of many nations. In a previous post, General Nakasone had been deeply involved in designing an operation code-named Nitro Zeus that amounted to a war plan to unplug Iran if the United States entered into hostilities with the country.

How Mr. Putin's government is reacting to the more aggressive American posture described by Mr. Bolton is still unclear.

"It's 21st-century gunboat diplomacy," said Robert M. Chesney, a law professor at the University of Texas, who has written extensively about the shifting legal basis for digital operations. "We're showing the adversary we can inflict serious costs without actually doing much. We used to park ships within sight of the shore. Now, perhaps, we get access to key systems like the electric grid."

Russian intrusion on American infrastructure has been the background noise of superpower competition for more than a decade.

How President Vladimir V. Putin's government would react to the more aggressive American posture is unclear. Dmitri Lovetsky/Associated Press

A successful Russian breach of the Pentagon's classified communications networks in 2008 prompted the creation of what has become Cyber Command. Under President Barack Obama, the attacks accelerated.

But Mr. Obama was reluctant to respond to such aggression by Russia with counterattacks, partly for fear that the United States' infrastructure was more vulnerable than Moscow's and partly because intelligence officials worried that by responding in kind, the Pentagon would expose some of its best weaponry.

At the end of Mr. Obama's first term, government officials began uncovering a Russian hacking group, alternately known to private security researchers as Energetic Bear or Dragonfly. But the assumption was that the Russians were conducting surveillance, and would stop well short of actual disruption.

That assumption evaporated in 2014, two former officials said, when the same Russian hacking outfit compromised the software updates that reached into hundreds of systems that have access to the power switches.

"It was the first stage in long-term preparation for an attack," said John Hultquist, the director of intelligence analysis at FireEye, a security company that has tracked the group.

In December 2015, a Russian intelligence unit shut off power to hundreds of thousands of people in western Ukraine. The attack lasted only a few hours, but it was enough to sound alarms at the White House.

A team of American experts was dispatched to examine the damage, and concluded that one of the same Russian intelligence units that wreaked havoc in Ukraine had made significant inroads into the United States energy grid, according to officials and a homeland security advisory that was not published until December 2016.

"That was the crossing of the Rubicon," said David J. Weinstein, who previously served at Cyber Command and is now chief security officer at Claroty, a security company that specializes in protecting critical infrastructure.

In late 2015, just as the breaches of the Democratic National Committee began, yet another Russian hacking unit began targeting critical American infrastructure, including the electricity grid and nuclear power plants. By 2016, the hackers were scrutinizing the systems that control the power switches at the plants.

In 2012, the defense secretary at the time, Leon E. Panetta, was warned of Russia's online intrusions, but President Barack Obama was reluctant to respond to such aggression by Moscow with counterattacks. Luke Sharrett for The New York Times

Until the last few months of the Obama administration, Cyber Command was largely limited to conducting surveillance operations inside Russia's networks. At a conference this year held by the Hewlett Foundation, Eric Rosenbach, a former chief of staff to the defense secretary and who is now at Harvard, cautioned that when it came to offensive operations "we don't do them that often." He added, "I can count on one hand, literally, the number of offensive operations that we did at the Department of Defense."

But after the election breaches and the power grid incursions, the Obama administration decided it had been too passive.

Mr. Obama secretly ordered some kind of message-sending action inside the Russian grid, the specifics of which have never become public. It is unclear whether much was accomplished.

"Offensive cyber is not this, like, magic cybernuke where you say, 'O.K., send in the aircraft and we drop the cybernuke over Russia tomorrow,'" Mr. Rosenbach said at the conference, declining to discuss specific operations.

After Mr. Trump's inauguration, Russian hackers kept escalating attacks.

Mr. Trump's initial cyberteam decided to be far more public in calling out Russian activity. In early 2018, it named Russia as the country responsible for "the most destructive cyberattack in human history," which paralyzed much of Ukraine and affected American companies including Merck and FedEx.

When General Nakasone took over both Cyber Command and the N.S.A. a year ago, his staff was assessing Russian hackings on targets that included the Wolf Creek Nuclear Operating Corporation, which runs a nuclear power plant near Burlington, Kan., as well as previously unreported attempts to infiltrate Nebraska Public Power District's Cooper Nuclear Station, near Brownville. The hackers got into communications networks, but never took over control systems.

In August, General Nakasone used the new authority granted to Cyber Command by the secret presidential directive to overwhelm the computer systems at Russia's Internet Research Agency — the group at the heart of the hacking during the 2016 election in the United States. It was one of four operations his so-called Russia Small Group organized around the midterm elections. Officials have talked publicly about those, though they have provided few details.

But the recent actions by the United States against the Russian power grids, whether as signals or potential offensive weapons, appear to have been conducted under the new congressional authorities.

As it games out the 2020 elections, Cyber Command has looked at the possibility that Russia might try selective power blackouts in key states, some officials said. For that, they said, they need a deterrent.

In the past few months, Cyber Command's resolve has been tested. For the past year, energy companies in the United States and oil and gas operators across North America discovered their networks had been examined by the same Russian hackers who successfully dismantled the safety systems in 2017 at Petro Rabigh, a Saudi petrochemical plant and oil refinery.

The question now is whether placing the equivalent of land mines in a foreign power network is the right way to deter Russia. While it parallels Cold War nuclear strategy, it also enshrines power grids as a legitimate target.

"We might have to risk taking some broken bones of our own from a counterresponse, just to show the world we're not lying down and taking it," said Robert P. Silvers, a partner at the law firm Paul Hastings and former Obama administration official. "Sometimes you have to take a bloody nose to not take a bullet in the head down the road."

David E. Sanger reported from Washington, and Nicole Perlroth from San Francisco.

A version of this article appears in print on June 15, 2019, Section A, Page 1 of the New York edition with the headline: U.S. Buries Digital Land Mines To Menace Russia's Power Grid