The Washington Post

National Security

Trump signed presidential directive ordering actions to pressure North Korea

By Karen DeYoung, Ellen Nakashima and Emily Rauhala September 30

Early in his administration, President Trump signed a directive outlining a strategy of pressure against North Korea that involved actions across a broad spectrum of government agencies and led to the use of military cyber-capabilities, according to U.S. officials.

As part of the campaign, U.S. Cyber Command targeted hackers in North Korea's military spy agency, the Reconnaissance General Bureau, by barraging their computer servers with traffic that choked off Internet access.

Trump's directive, a senior administration official said, also included instructions to diplomats and officials to bring up North Korea in virtually every conversation with foreign interlocutors and urge them to sever all ties with Pyongyang. Those conversations have had significant success, particularly in recent weeks as North Korea has tested another nuclear weapon and ballistic missiles, officials said.

So pervasive is the diplomatic campaign that some governments have found themselves scrambling to find any ties with North Korea. When Vice President Pence called on one country to break relations during a recent overseas visit, officials there reminded him that they never had relations with Pyongyang. Pence then told them, to their own surprise, that they had $2 million in trade with North Korea. Foreign officials, who asked that their country not be identified, described the exchange.

The directive also instructed the Treasury Department to outline an escalating set of sanctions against North Korean entities and individuals, and foreigners who dealt with them. Those instructions are reflected in a steady stream of U.S. and international sanctions in recent months.

The directive was not made public at the time it was signed, following a policy review in March, because "we were providing every opportunity as a new administration to North Korea to sit down and talk, to take a different approach," said the official, who spoke on the condition of anonymity to discuss closed-door policy decisions.

"We made clear the door was open for talks before the president had even signed off on this strategy, but North Korea continued to launch missiles, continued to kidnap Americans to keep as hostages . . . all the things they did when we were early in the administration and sending signals that the door was open to talks."

That door remains open, Secretary of State Rex Tillerson said Saturday in Beijing. Speaking to reporters following talks with Chinese officials, Tillerson for the first time acknowledged that the United States was in direct communication with North Korea.

“We are probing, so stay tuned,” he said. “We ask, ‘Would you like to talk?’ We have lines of communications to Pyongyang. We’re not in a dark situation, a blackout. We have a couple, three, channels open. . . . We can talk to them; we do talk to them.”

In Washington, however, officials quickly played down any idea that negotiations were underway or that anything had yet come of the talks. State Department spokeswoman Heather Nauert issued a statement saying that “North Korean officials have shown no indication that they are interested in or are ready for talks regarding denuclearization.”

The senior administration official said it would be wrong to “read too much into” Tillerson’s remarks. “The U.S. has always maintained some kind of channel, kept some channel open even in the darkest days of previous administrations.”

Those channels include conversations between the State Department’s special representative for North Korea, Joseph Yun, and Pak Song Il, a senior member of Pyongyang’s delegation to the United Nations. They have met several times this year to discuss American prisoners being held by North Korea, among other matters. Other contacts have taken place through the “track two” process, which regularly brings together nongovernmental U.S. experts — and occasionally U.S. officials — and North Korean officials.

Tillerson’s remarks Saturday came after a day of meetings with top Chinese officials, including President Xi Jinping, which saw both sides strike a careful, conciliatory tone following a new North Korean nuclear test and missile launches, and weeks of insults and threats between Trump and North Korean dictator Kim Jong Un.

In brief formal statements before their meetings, Chinese leaders — who have repeatedly called for restraint — did not mention North Korea. Instead, they tried to keep the focus on Trump’s upcoming Asia visit, which Xi promised would be a “special, wonderful and successful” event.

The Cyber Command operation, which was due to end Saturday, was part of the overall campaign set in motion many months ago. The effects were temporary and not destructive, officials said. Nonetheless, some North Korean hackers griped that lack of access to the Internet was interfering with their work, according to another U.S. official, who also spoke on the condition of anonymity to discuss a secret operation.

Cyber Command and the White House had no comment. But the senior administration official said, “What I can tell you is that North Korea has itself been guilty of cyberattacks, and we are going to take appropriate measures to defend our networks and systems.”

Eric Rosenbach, who led the Pentagon’s cyber-efforts as assistant secretary of defense in the Obama administration, said the operation “could have the advantage of signaling to the North Koreans a more aggressive posture. However, there’s accompanying risk of an escalation and a North Korean cyber-counterattack.”

Rosenbach, now co-director of the Belfer Center at the Harvard Kennedy School, said that he was not aware of the actual operation but that if it is "truly a military operation," he sees no reason to hide it. "The Department of Defense should probably own it," he said.

Aaron Hughes, a former senior cyber-official in the Obama administration, said he, too, was not aware of the actual operation. But "if I was still in my [Pentagon] seat, I would actively be advocating we do these types of things. . . . We should be using all elements of national power to deter and message the North Koreans, to include our military, including cyber," Hughes said.

Others said they would be cautious about using even minor cyber-capabilities against North Korea and doing it openly because of the risk of retaliation.

"I wonder what the disruptive payoff is that we're getting that's worth even a marginal extra chance of nuclear war?" said Jason Healey, a former military cyber-operator and now a senior research scholar at Columbia University's School of International and Public Affairs.

Rauhala reported from Beijing.

Karen DeYoung is associate editor and senior national security correspondent for the Washington Post. Follow @karendeyoung1

Ellen Nakashima is a national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties. Follow @nakashimae

Emily Rauhala is a China Correspondent for the Post. She was previously a Beijing-based correspondent for TIME, and an editor at the magazine's Hong Kong office. Follow @emilyrauhala