The New York Times

Trump Loosens Secretive Restraints on Ordering Cyberattacks

By David E. Sanger

Sept. 20, 2018

President Trump has authorized new, classified orders for the Pentagon's cyberwarriors to conduct offensive attacks against adversaries more freely and frequently, the White House said on Thursday, wiping away Obama-era restrictions that his advisers viewed as too slow and cumbersome.

"Our hands are not as tied as they were in the Obama administration," John R. Bolton, the national security adviser, told reporters in announcing a new cyberstrategy.

Mr. Bolton rewrote a draft of the strategy after joining the administration in April. Many of his remarks on Thursday focused on a secret order — which Mr. Trump signed in August but which has never been publicly described — that appears to give far more latitude for the newly elevated United States Cyber Command to act with minimal consultation from a number of other government agencies.

The order essentially delegates more power to Gen. Paul M. Nakasone, who took over this year as the director of the National Security Agency and the commander of United States Cyber Command. During his Senate confirmation hearing in March, General Nakasone complained that America's online adversaries attacked with little concern about retaliation.

"I would say right now they do not think that much will happen to them," said General Nakasone, who previously oversaw the Army's cybercommand. "They don't fear us."

But this month, General Nakasone said he was more comfortable with the new guidance issued by the White House, even though the administration has not made any of it public.

Senior officials have said it eliminates a lengthy process of consensus-building across the government — the Departments of Commerce, Treasury and Homeland Security among them — before the United States conducts an offensive action.

It is not clear whether Mr. Trump must still approve every major offensive online operation, as Presidents George W. Bush and Barack Obama did.

Mr. Bolton did not shed much light. "Our presidential directive effectively reversed those restraints, effectively enabling offensive cyberoperations through the relevant departments," he said.

He said that since Mr. Trump took office, the administration has “authorized cyberoperations” against rivals, though he gave no details.

Much of the strategy that was made public on Thursday strongly echoes similar documents issued by Mr. Obama and Mr. Bush. They focus on improving digital defenses for the United States government, bettering training, working with private industry to share information about vulnerabilities and working with allies.

While the words in the strategy differ from the past, the impetus is the same. It did, however, identify specific countries as adversaries.

The order essentially delegates more power to Gen. Paul M. Nakasone, who took over this year as the director of the National Security Agency and the commander of United States Cyber Command. Erin Schaff for The New York Times

“Russia, Iran and North Korea conducted reckless cyberattacks that harmed American and international businesses and our allies and partners without paying costs likely to deter future cyberaggression,” the strategy read. “China engaged in cyberenabled economic espionage and trillions of dollars of intellectual property theft.”

But the classified directive appears to be significantly different, as Mr. Bolton said on Thursday.

His indictment of the previous administration omitted the fact that Mr. Obama continued or initiated three of the most aggressive cyberoperations in American history: one to disable Iran’s nuclear fuel production, another to attack North Korea’s missile programs and a third against online recruitment and communications by the Islamic State.

The first, code-named Olympic Games, was judged successful at destroying about 1,000 nuclear centrifuges for a year. The Korea operation had only mixed results at best, and Mr. Obama's own defense secretary later wrote that the operation against the Islamic State proved largely ineffective.

But Mr. Obama hesitated to strike back at Russia in 2016 after revelations of its breach into the Democratic National Committee, and acted only after the presidential election.

And, as Mr. Bolton noted, the United States declined to name other attackers, including the Chinese, for stealing roughly 22 million files on Americans with security clearances from the Office of Personnel Management. He noted that those files, "my own included, maybe yours, found a new residence in Beijing."

Mr. Bolton became the first American official to formally acknowledge what was widely known: that the Chinese government was behind that intrusion.

Additionally, the Trump administration accused North Korea of mounting the WannaCry attack that brought down the British health care system, and Russia of initiating the NotPetya attack that was aimed at Ukraine and cost hundreds of millions of dollars in damage, including to shipping companies like Maersk.

But Mr. Bolton, whose concepts of deterrence were formed in the Cold War, is likely to discover what his predecessors learned: Almost every strategy that worked in deterring nuclear attacks does not fit the digital era, and even figuring out where an attack originated can be a challenge.

The government has grown more skilled at attributing the source of a cyberattack, but the process remains lengthy. By the time a conclusion is reached, it is often too late to mount a successful counterstrike.

Mr. Trump has particularly muddied the waters in assigning blame for attacks, repeatedly expressing doubts that Russia was behind the hacking of the Democratic National Committee and members of Hillary Clinton's 2016 presidential campaign. The Justice Department has indicted officers of Russia's military intelligence unit, once known as the G.R.U., and the Internet Research Agency, in those attacks.

Part of the strategy calls for the United States to develop what it describes as an international cyberdeterrence initiative, which sounds similar to efforts to develop a theory of nuclear deterrence. The document provides few details, but says the Trump administration will build "a coalition and develop tailored strategies to ensure adversaries understand the consequences of their malicious cyberbehavior."

Some of those efforts have already begun: The American accusations against North Korea and Russia last year were immediately echoed by Britain and other Western powers.

Representative Jim Langevin, Democrat of Rhode Island who has been active in developing new cyberstrategies, said that the White House approach was focused "in starkly offensive terms."

"I agree that our adversaries need to know that we can — and will — challenge them in cyberspace," Mr. Langevin said. "But as the country with the most innovative economy in the world, we must also acknowledge the abiding interest of the United States in encouraging stability in this domain."

Get politics and Washington news updates via Facebook, Twitter and the Morning Briefing newsletter.

A version of this article appears in print on Sept. 21, 2018, on Page A4 of the New York edition with the headline: President Loosens Secretive Restraints on Ordering Cyberattacks