Exclusive: Secret Trump order gives CIA more powers to launch cyberattacks

By Zach Dorfman, Kim Zetter, Jenna McLaughlin and Sean D. Naylor

Published: 2020-07-15 · Archived: 2026-04-06 15:42:12 UTC

The Central Intelligence Agency has conducted a series of covert cyber operations against Iran and other targets since winning a secret victory in 2018 when President Trump signed what amounts to a sweeping authorization for such activities, according to former U.S. officials with direct knowledge of the matter.

The secret authorization, known as a presidential finding, gives the spy agency more freedom in both the kinds of operations it conducts and who it targets, undoing many restrictions that had been in place under prior administrations. The finding allows the CIA to more easily authorize its own covert cyber operations, rather than requiring the agency to get approval from the White House.

Unlike previous presidential findings that have focused on a specific foreign policy objective or outcome — such as preventing Iran from becoming a nuclear power — this directive, driven by the National Security Council and crafted by the CIA, focuses more broadly on a capability: covert action in cyberspace.

The “very aggressive” finding “gave the agency very specific authorities to really take the fight offensively to a handful of adversarial countries,” said a former U.S. government official. These countries include Russia, China, Iran and North Korea — which are mentioned directly in the document — but the finding potentially applies to others as well, according to another former official. “The White House wanted a vehicle to strike back,” said the second former official. “And this was the way to do it.”

President Trump and the CIA. (Photo illustration: Kelli R. Grant/Yahoo News; photos: AP(3), Getty Images)

The CIA's new powers are not about hacking to collect intelligence. Instead, they open the way for the agency to launch offensive cyber operations with the aim of producing disruption — like cutting off electricity or compromising an intelligence operation by dumping documents online — as well as destruction, similar to the U.S.-Israeli 2009 Stuxnet attack, which destroyed centrifuges that Iran used to enrich uranium gas for its nuclear program.

The finding has made it easier for the CIA to damage adversaries' critical infrastructure, such as petrochemical plants, and to engage in the kind of hack-and-dump operations that Russian hackers and WikiLeaks popularized, in which tranches of stolen documents or data are leaked to journalists or posted on the internet. It has also freed the agency to conduct disruptive operations against organizations that were largely off limits previously, such as banks and other financial institutions.

Another key change with the finding is it lessened the evidentiary requirements that limited the CIA's ability to conduct covert cyber operations against entities like media organizations, charities, religious institutions or businesses believed to be working on behalf of adversaries' foreign intelligence services, as well as individuals affiliated with these organizations, according to former officials.

"Before, you would need years of signals and dozens of pages of intelligence to show that this thing is a de facto arm of the government," a former official told Yahoo News. Now, "as long as you can show that it vaguely looks like the charity is working on behalf of that government, then you're good."

The CIA has wasted no time in exercising the new freedoms won under Trump. Since the finding was signed two years ago, the agency has carried out at least a dozen operations that were on its wish list, according to this former official. "This has been a combination of destructive things — stuff is on fire and exploding — and also public dissemination of data: leaking or things that look like leaking."

"Our government is basically turning into f*ing WikiLeaks."**

– Former U.S. official

Some CIA officials greeted the new finding as a needed reform that allows the agency to act more nimbly. "People were doing backflips in the hallways [when it was signed]," said another former U.S. official.

But critics, including some former U.S. officials, see a potentially dangerous attenuation of intelligence oversight, which could have unintended consequences and even put people's lives at risk, according to former officials.

The involvement of U.S. intelligence agencies in hack-and-dump activities also raises uncomfortable comparisons for some former officials. "Our government is basically turning into f****ing WikiLeaks, [using] secure communications on the dark web with dissidents, hacking and dumping," said one such former official.

The CIA declined to comment or respond to an extensive list of questions from Yahoo News. The National Security Council did not respond to multiple written requests for comment.

While the CIA has been pushing for years to expand its cyber authorities, Russia's interference in the 2016 election led Obama officials to grasp for new ways to retaliate against the Kremlin. High-level discussions included proposals for the CIA to dump embarrassing hacked information about Russian officials online, as well as to destroy Russian servers, according to former officials.

But just days away from launching operations in the late summer of 2016, intelligence operatives were told to stand down, according to former officials. The decision to do so was made at the highest levels of the Obama administration, according to a former senior national security official.

During the early days of the Trump administration, intelligence officials were hopeful that the president would give the go-ahead to those operations. But senior Trump officials weren't interested in retaliating against Russia for the election interference, according to a former official. "It was radio silence," the former official said. "It all dissipated, went to nothing."

While plans for immediate cyber retaliation against Russia faded, discussions about expanding the CIA's cyber authorities continued to accelerate under Trump. For years, the CIA had bristled under what some intelligence officials considered onerous barriers to covert action in cyberspace that prevented it from even proposing many operations, according to former officials.

"Pompeo's message was: 'We don't want to hold you up, we want to move, move, move.'"

– Former U.S. official

When it came to covert action, "you always had the two camps [inside the CIA]," said Robert Eatinger, who served at the CIA for 24 years, including a stint as the agency's top lawyer. There were "those who felt that their hands were too tied, and those who felt the restrictions were wise and appropriate," recalled Eatinger, who said he has no knowledge of the CIA cyber finding signed by Trump and wouldn't discuss specific incidents that occurred during his time with the agency.

Advocates for greater cyber authorities gained the upper hand in these debates under the Trump administration, which encouraged the CIA to stretch its prior authorities to pursue more aggressive offensive cyber operations — particularly against Iran. "Trump wanted to push decision making to the lowest possible denominator," said a former intelligence official.

Mike Pompeo made that point clear after Trump made him CIA director in January 2017. Pompeo's message, the former official said, was: "We don't want to hold you up, we want to move, move, move."

A current senior intelligence official, who declined to discuss specific U.S. government operations or policies, called Trump-era interest in offensive operations “phenomenal.” The CIA, the National Security Agency and the Pentagon “have been able to play like we should be playing in the last couple years,” the current official said.

John Bolton’s appointment as national security adviser in April 2018 gave another boost to those seeking to ease restrictions on cyber operations. “We needed to scrap the Obama-era rules and replace them with a more agile, expeditious decision-making structure,” Bolton writes in his recently published memoir, “The Room Where It Happened.” Part of this involved strengthening the U.S. government’s “clandestine capabilities” in cyberspace against “nonstate actors” and others, he writes.

In September 2018, Bolton announced that Trump had signed a presidential directive easing Obama-era rules governing military cyber operations. Although the administration disclosed the existence of that directive — known as National Security Presidential Memorandum 13 — the underlying rules of engagement for military cyber operations remain secret. The administration also kept secret the CIA finding, which gave the agency its new authorities.

“Trump came in and way overcorrected.”
– Former U.S. official

The CIA’s new cyber powers prompted concerns among some officials. “Trump came in and way overcorrected,” said a former official. Covert cyber operations that in the past would have been rigorously vetted through the NSC, with sometimes years-long gaps between formulation and execution, now go “from idea to approval in weeks,” said the former official.

Former officials declined to speak in detail about cyber operations the CIA has carried out as a result of the finding, but they said the agency has already conducted covert hack-and-dump actions aimed at both Iran and Russia.

For example, the CIA has dumped information online about an ostensibly independent Russian company that was “doing work for Russian intelligence services,” said a former official. While the former official declined to be more specific, BBC Russia reported in July 2019 that hackers had breached the network of SyTech, a company that does work for the FSB, Russia’s domestic spy agency, and stolen about 7.5 terabytes of data; the data from that hack was passed to media organizations.

In another stunning hack-and-dump operation, an unknown group in March 2019 posted on the internet chat platform Telegram the names, addresses, phone numbers and photos of Iranian intelligence officers allegedly involved in hacking operations, as well as hacking tools used by Iranian intelligence operatives. That November, the details of 15 million debit cards for customers of three Iranian banks linked to Iran’s Islamic Revolutionary Guard Corps were also dumped on Telegram.

Although sources wouldn’t say if the CIA was behind those Iran breaches, the finding’s expansion of CIA authorities to target financial institutions, such as an operation to leak bank card data, represents a significant

escalation in U.S. cyber operations. Under prior administrations, senior Treasury Department officials argued successfully against leaking or wiping out banking data, according to former officials, because it could destabilize the global financial system. These were operations the “CIA always knew were an option, but were always a bridge too far," said a former official. “They had been bandied about at senior levels for a long time, but cooler heads had always prevailed."

“It was obvious that destabilization was the plan on Iran.”

– Former U.S. official

The new cyber finding further emboldened the CIA’s operations against Iran, according to former officials. Even before Trump signed the directive, administration officials were already encouraging the CIA to aggressively interpret preexisting secret Iran-related authorities to help prosecute the administration’s “maximum pressure” campaign against Tehran. Using the Cold War strategy of rolling back the Soviet Union as inspiration, senior Trump national security officials believed that destabilizing Iran within its borders would force the regime to cease its adventurism abroad and, perhaps, collapse.

The maximum-pressure campaign includes punishing economic sanctions, but has also involved CIA cyberattacks on Iranian infrastructure, said former officials. “It was obvious that destabilization was the plan on Iran,” said one former official, and Trump administration officials were eager to have the CIA conduct destructive cyber operations against targets inside that country. Bolton “wanted another tool, he wanted another hammer. He was looking at Stuxnet and how to be mean to Iran, so that was probably attractive to him,” said another source.

The Trump administration was able to lean on extensive legal powers for covert action against the Islamic Republic that were already on the books, including a presidential finding dating back at least to the early 2000s devoted to counterproliferation — in other words, preventing a nuclear-armed Iran, according to former officials. Another long-standing Iran-focused presidential finding authorizes the CIA to counter Tehran’s influence in the Middle East, in particular by combating Iran’s Islamic Revolutionary Guard Corps and by supporting groups in the region opposed to the regime, according to former U.S. officials.

Neither these two Iran-related findings, nor the new cyber finding, mention regime change as a stated goal, according to former officials. Over time, however, the CIA and other national security officials have interpreted the first two Iran findings increasingly broadly, with covert activities evolving from their narrow focus on stopping Tehran’s nuclear program, they said. The Iran findings have been subject to “classic mission creep,” said one former official.

Fatigue from having to continually beat back Iran’s nuclear progress gradually led U.S. officials to take an even more aggressive approach that began to resemble a regime change strategy, according to former officials. The thinking became “If we can impact the regime, then no bomb,” said another former official. “We’re playing semantics — destabilization is functionally the same thing as regime change. It’s a deniability issue,” the former official said.

While the CIA's new powers expand the agency's ability to target Iran and other foreign adversaries, they also present potential pitfalls, according to former officials. The CIA and the Pentagon have long tussled over authorities in cyberspace, and these coordination issues will only become more critical now, according to former officials — especially when U.S. military operatives online unknowingly run up against their counterparts from the CIA.

"I would look at the intel community as the same as the military in that there should be civilian control of big decisions – who to go to war against, who to launch an attack against, who to fight a particular battle."

– Robert Eatinger, former top CIA attorney

"If you're doing something on someone's network and you have friendly forces also on the network, you don't want to have fratricide," said a former senior military intelligence official. Even inside the U.S. intelligence community, the CIA has a reputation for secrecy, according to former officials. The CIA's "deconfliction is poor, they're not keeping people in the loop on what their cyber operations are," said another former official.

Some former officials even worry about the oversight of cyber operations within the CIA. Agency cyber operatives "weren't always transparent" about their activities, said a former senior official. "It was a problem. There were times I was surprised."

This more permissive environment may also intensify concerns about the CIA's ability to secure its hacking arsenal. In 2017, WikiLeaks published a large cache of CIA hacking tools known as "Vault 7." The leak, which a partially declassified CIA assessment called "the largest data loss in CIA history," was made possible by "woefully lax" security practices at the CIA's top hacker unit, the assessment said.

Eatinger, the former top CIA attorney, who retired in 2015, said it's unclear to him whether the new cyber finding would be a return to the agency's more freewheeling days of the 1980s, or something that goes even further. Either way, it's a "big deal," he said.

Removing NSC oversight of covert operations is a significant departure from recent history, according to Eatinger. "I would look at the intel community as the same as the military in that there should be civilian control of big decisions — who to go to war against, who to launch an attack against, who to fight a particular battle," he said. "It makes sense that you would have that kind of civilian or non-intelligence civilian leadership for activities as sensitive as covert action."

Regardless, these expansive new cyber powers may become a lasting legacy of the Trump administration, solidifying the greater role the CIA has long coveted in a key arena, and providing the agency with authorities it

has desired for three presidential administrations.

“People thought, ‘Hey, George W. Bush will sign this,’ but he didn’t,” said a former official. CIA officials then believed, “‘Obama will sign it.’ Then he didn’t.”

“Then Trump came in, and CIA thought he wouldn’t sign,” recalled this official. “But he did.”

———

Read more from Yahoo News:

-
-
-
-
-
