

## National Security

# Trump approved cyber-strikes against Iran's missile systems

By [Ellen Nakashima](#)

June 22 at 5:37 PM

President Trump approved an offensive cyberstrike that disabled Iranian computer systems used to control rocket and missile launches, even as he backed away from a conventional military attack in response to its downing Thursday of an unmanned U.S. surveillance drone, according to people familiar with the matter.

The cyberstrikes, launched Thursday night by personnel with U.S. Cyber Command, were in the works for weeks if not months, according to two of these people, who said the Pentagon proposed launching them after Iran's alleged attacks on two oil tankers in the Gulf of Oman earlier this month.

The strike against the Islamic Revolutionary Guard Corps was coordinated with U.S. Central Command, the military organization with purview of activity throughout the Middle East, these people said. They spoke on the condition of anonymity because the operation remains extremely sensitive.

Though crippling to Iran's military command and control systems, the operation did not involve a loss of life or civilian casualties — a contrast to conventional strikes, which the president said he called back Thursday because they would not be “proportionate.”

The administration on Saturday warned industry officials to be alert for cyberattacks originating from Iran.

The White House declined to comment, as did officials at U.S. Cyber Command. Pentagon spokeswoman Elissa Smith said: “As a matter of policy and for operational security, we do not discuss cyberspace operations, intelligence or planning.”

The cyberstrikes were first reported by Yahoo News.

“This operation imposes costs on the growing Iranian cyberthreat, but also serves to defend the United States Navy and shipping operations in the Strait of Hormuz,” said Thomas Bossert, a former senior White House cybersecurity official in the Trump administration.

“Our U.S. military has long known that we could sink every IRGC vessel in the strait within 24 hours if necessary. And this is the modern version of what the U.S. Navy has to do to defend itself at sea and keep international shipping lanes free from Iranian disruption.”

Thursday's strikes against the Revolutionary Guard represented the first offensive show of force since Cyber Command was elevated to a full combatant command in May. It leveraged new authorities, granted by the president, that have streamlined the approval process for such measures. It is also a reflection of a new Cyber Command strategy — called “defending forward” — that its leader, Gen. Paul Nakasone, has defined as operating “against our enemies on their virtual territory.”

Cybercom launched an operation against [Russia last fall to deny](#) Internet "trolls" affiliated with the Internet Research Agency the ability to carry out political influence operations on U.S. social media platforms. But the operation against Iran was more disabling.

"This is not something they can put back together so easily," said one person, who spoke on the condition of anonymity because they were not authorized to speak on the record.

The digital strike was an example, two people said, of what national security adviser John Bolton meant when he suggested recently that the United States is stepping up offensive cyber activity. "We're now opening the aperture, broadening the areas we're prepared to act in," Bolton said at a Wall Street Journal conference.

The United States in April designated the Revolutionary Guard as a foreign terrorist organization in response to its destabilizing behavior across the Middle East.

Iranian cyber forces have tried to hack U.S. naval ships and navigation capabilities in the Persian Gulf region for the past few years. The Strait of Hormuz is a strategically important sea lane through which about one-fifth of the world's oil passes daily.

On Saturday, the Department of Homeland Security issued a warning to U.S. industry that Iran has stepped up its cyber-targeting of critical industries — to include oil, gas and other energy sectors — and government agencies, and has the potential to disrupt or destroy systems.

"There's no question that there's been an increase in Iranian cyber activity," said Christopher Krebs, director of DHS's Cybersecurity and Infrastructure Security Agency. "Iranian actors and their proxies are not just your garden variety run-of-the-mill data thieves. These are the guys that come in and they burn the house down."

Krebs, in an interview, said, "We need everyone to take the current situation very seriously. Look at any potential incidents that you have and treat them as a worst-case scenario. This is not you waiting until you have a data breach . . . This is about losing control of your environment, about losing control of your computer."

He said the "shift in geopolitical dynamics" factored into the agency's warning.

The National Security Agency also urged industry to be vigilant. "In these times of heightened tensions, it is appropriate for everyone to be alert to signs of Iranian aggression in cyberspace and ensure appropriate defenses are in place," NSA spokesman Greg Julian said in a statement Saturday.


Iran has unleashed destructive cyberattacks in the past. In 2012, it launched the Shammoon virus that nearly destroyed more than 30,000 business network computers at Saudi Aramco, a state-owned oil company, and erased backup copies of data. Saudi Arabia and Iran are fierce adversaries.

Private-sector analysts have documented a gradual increase in cyber activity by Iran and its proxies targeting U.S. industry since 2014. It has often come in the form of spearphishing attempts seeking access to computer systems in the energy sector.

“In the last year, the activity has sped up,” said Robert M. Lee, co-founder of cybersecurity firm Dragos, who conducted cyber operations for the NSA and Cybercom from 2011 to 2015. “In the last six months, we saw another hike. And last week, we saw additional activity.”

“The reality is we’ve been seeing more and more aggressive activity for quite some time,” he said. “It’s just getting worse.”

### Ellen Nakashima

Ellen Nakashima is a national security reporter for The Washington Post. She covers cybersecurity, surveillance, counterterrorism and intelligence issues. She has also served as a Southeast Asia correspondent and covered the White House and Virginia state politics. She joined The Post in 1995. [Follow](#) 



The Washington Post

## It's the Summer Sale.

**Limited time offer:** ~~\$10~~ \$4 every month - that's every story for just \$1 a week.

[Get this offer](#)

[Send me this offer](#)

Already a subscriber? [Sign in](#)