

Summary by Bloomberg AI

AI Generated



- The Trump administration's push for aggressive cybersecurity tactics is sparking questions about how far companies can go without facing retaliation, escalated conflicts, or legal risks.
- The administration's goal is to pivot from a defensive stance to one that shrinks the incentive for nation states, ransomware groups, and other cyber criminals to act, with the private sector playing a role in disruptive cyber actions.
- Companies will have to strike a careful balance in taking disruptive cyber actions, with concerns about legal certainty and the potential for unintended consequences, such as revictimization, collateral damage, and disrupted ongoing investigations.

The Trump administration's push for aggressive cybersecurity tactics that would tap the private sector to help disrupt suspected malicious cyber actors is sparking questions about how far companies can go without facing retaliation, escalated conflicts, or legal risks.

Deterring adversaries' attacks is one of the key pillars of the soon-to-come National Cyber Strategy, which spells out the White House's cybersecurity priorities, according to sources briefed on the administration's plans. National Cyber Director Sean Cairncross has already voiced the administration's goal to pivot from a defensive stance to one that shrinks the incentive for nation states, ransomware groups, and other cyber criminals to act.

The shift in strategy, backed by an unprecedented \$1 billion allocation for offensive cyber operations in Trump's 2025 tax and spending law, is raising questions about how far the private sector can take disruptive cyber actions without the safeguards afforded by government contracts. As the administration prepares to release its cyber plan, the private sector and government are grappling with the evolving role that private companies from established tech giants to Silicon Valley startups will play in this new cyber landscape.

"There will be encouragement, more space, if you will, to make sure that we're being disruptive," said Bruce Byrd, executive vice president and general counsel at Palo Alto Networks Inc.

But companies will have to strike a careful balance, he said. "You don't want to just be running around taking a sledgehammer to every intrusion you see," Byrd added. "Not all intrusions have a truly detrimental effect, but you can learn from them."

'Giving Bad Actors a Bad Day'

The government has already issued multimillion dollar contracts to defense contractors to assist with offensive cyber missions, Bloomberg News reported. Some of the most sophisticated private companies, meanwhile, have been pursuing what's sometimes referred to as active cyber defense in their own networks.

For example, cyber professionals point to activities including planting decoys in targeted files to collect information about attackers or trigger encryption protocols. Others have sharpened threat hunting capabilities. Leading US platforms like Microsoft and Google have used their threat intelligence to disrupt online criminal activity through civil legal actions, technical countermeasures, and public sector partnerships.

"What we're talking about isn't necessarily using cyber bullets to take a machine offline. What we want to do is enable the private industry to be a part of giving bad actors a bad day, thwarting their ability to conduct ransomware attacks, espionage activity, etc," said a cybersecurity industry leader briefed on the national cyber strategy who wasn't authorized to discuss the administration's plans.

But there's a limit to how far private industry can go alone.

"There are so many unintended consequences if we allow for this notion of unfettered hacking back, whereby private sector entities are the ones on the front lines, taking offensive action against adversaries," said Drew Bagley, vice president and counsel on privacy and cyber policy at CrowdStrike. The most important thing "for the private sector to do is to engage in active defense" and "make that as ubiquitous as possible," he said.

The appetite and capabilities for disruptive strategies have grown in recent years among some of the biggest cloud, tech, and cyber platforms. And the government's push for more offensive cyber actions will likely spur the private sector to ramp up its active defense efforts.

But it may also test existing legal frameworks.

The use of what's known as beacons or canaries, for example, that, once stolen, could signal the location of a bad actor or stolen data, sits in a "gray area," said John Carlin, chair of Paul Weiss's National Security practice group. "If you use that beacon to cause damage, then you're looking more like a traditional hack back and you have the concerns about the Computer Fraud and Abuse Act. But if it's just signaling its location, what is that, essentially, is the question."

Such concerns about legal certainty were on display during a January House subcommittee hearing on offensive cyber.

"What remains unresolved is how far they should be permitted to go under what legal authorities and with what safeguards," Frank Cilluffo, director of the McCrary Institute for Cyber and Critical Infrastructure Security at Auburn University, and one of the hearing witnesses, said in his testimony.

Hacking Back

The conversation around offensive cybersecurity is opening the door for another discussion: allowing victims of cyberattacks to go after bad actors directly, in what is known as hacking back.

To that end, Rep. David Schweikert (R-Ariz.) introduced a bill last August to authorize the president to issue letters of marque—which he said hasn’t happened since the War of 1812—to deputize cyber operators to defend critical infrastructure. No action has been taken on the legislation.

Allowing a broad array of private entities to go after cybercriminals directly could lead to revictimization, collateral damage, disrupted ongoing investigations, and even potential harms to innocent citizens, cyber leaders said in interviews.

“If we allow everybody to be out there in a disorganized way, engaging in hacking back, then there are going to be lots of unintended consequences,” Bagley said.

Government officials and industry stakeholders are also cautioning against a policy shift that would abandon resources supporting traditional defense strategies, especially in light of budget and staff cuts at the Cybersecurity and Infrastructure Security Agency, which protects American critical infrastructure and facilitates collaboration with the private sector.

Cybersecurity leaders say they’re watching for how the strategy will be implemented, including through executive orders, and how the administration will use existing tools to strengthen private and public sector collaboration.

“It’s relatively easy to say that we should go more on the offense, and then it’s a lot harder to actually turn that into execution,” said Michael Daniel, CEO and president of Cyber Threat Alliance, and a former cybersecurity executive under the Obama administration. He added, “I’ll be particularly interested to see how this administration frames that pillar.”

– With assistance from Evan Ochsner.

To contact the reporter on this story: **Cassandra Coyer** in Washington at ccoyer@bloombergindustry.com

To contact the editors responsible for this story: Jeff Harrington at jharrington@bloombergindustry.com; Michelle M. Stein at mstein1@bloombergindustry.com

© 2026 Bloomberg Industry Group, Inc. All Rights Reserved

