NSA: Volt Typhoon was ‘not successful’ at persisting in critical infrastructure

By Jonathan Greig

Published: 2025-07-15 · Archived: 2026-04-05 21:59:59 UTC

Senior cybersecurity officials at the National Security Agency and FBI said the agencies have been successful in addressing some of the Chinese cyber campaigns targeting critical infrastructure in the U.S.

During the International Conference on Cyber Security at Fordham University in New York City on Tuesday, experts spoke at length about Beijing’s so-called Typhoon campaigns — which have involved Chinese government and private sector groups launching attacks on U.S. government agencies and companies.

Kristina Walter, director of the NSA’s Cybersecurity Collaboration Center, focused on Volt Typhoon, an effort by Chinese actors to preposition themselves on U.S. critical infrastructure for disruptive or destructive cyberattacks in the event of a kinetic conflict centered around Taiwan.

“The good news is, they really failed. They wanted to persist in domestic networks very quietly for a very long time so that if and when they needed to disrupt those networks, they could. They were not successful in that campaign,” she said.

“We, with private sector, with FBI, found them, understood how they were using the operating systems, how they're using legitimate credentials to maintain persistence, and frankly, we equipped the entire private sector and U.S. government to hunt for them and detect them.”

Walter did not offer further details about those efforts. She said that after the NSA and other agencies released a public advisory in 2024, owners of critical infrastructure reached out to them to confirm that they found evidence of Volt Typhoon and ask for help.

Brett Leatherman, who was recently appointed assistant director for cyber at the FBI, echoed those remarks and noted that Volt Typhoon was specifically focused on critical infrastructure centered around the U.S. Navy — particularly in island communities like Guam.

Leatherman said U.S. efforts to shine a light on the campaign forced Chinese actors to pull back, adapt their tactics and burn previous methods they used to breach critical infrastructure systems.

The publicity fostered by U.S. agencies forced Chinese groups to come up with new ways to breach organizations while also providing ways for private industry to better defend themselves, he said.

“Even if you're not dismantling that network — we're never going to dismantle the CCP hacking apparatus — but if you can bring real relief to victims, you're also protecting national security by doing that, and that's why public attribution is so important when it comes to PRC hacking activity,” he said.

‘True cyberwarfare’

Publicity is not the only card the U.S. government has played in response to Chinese hacking campaigns. Leatherman walked the audience through an incident that he called “one of the first times that the FBI engaged in true cyberwarfare in real time against CCP actors.”

Leatherman described a past FBI effort to take down a botnet used by China’s Flax Typhoon — a campaign that was being backed by a now-indicted Chinese cybersecurity company named Integrity Technology Group.

Leatherman said the FBI was initially successful in pulling down the command and control infrastructure for those bots and redirecting them to FBI-controlled infrastructure.

But Integrity Technology Group fought back, launching a distributed denial of service (DDoS) against the FBI’s infrastructure and were able to gain control of their bots again.

Leatherman said it did not appear that the hackers knew they were attacking the U.S. government. Over the course of a weekend, the FBI and Integrity Technology Group went back and forth — attacking each other and trying to wrest control over the bot network.

“Finally, we published our splash page, which had the FBI and our partners on it, to let them know it was us, and it was at that point that the Flax Typhoon actors realized that they had actually DDoSed U.S. government infrastructure, and then they actually burned down their own infrastructure at that point,” he said.

“We didn't have to do it. We were going to continue to remove those capacity and capability systems from them, but they burned it down as soon as they saw that. So that demonstrates where the U.S. stands, as far as cyber capabilities, in our willingness to punch back at the bad actors.”

Leatherman said that traditional law enforcement activities are also part of the response, including last week’s arrest in Italy of a Chinese hacker allegedly involved in the Silk Typhoon campaign.

Leatherman and Walter compared the Chinese government’s association with cyber companies like iSoon and Integrity Technology Group as an example of what the U.S. needed to do in terms of partnering with the private sector to defend U.S. networks.

“When we look at the China cyber ecosystem, it is not the Chinese government targeting the United States,” Walter said. “It's this giant ecosystem of industry who has been unleashed to frankly do whatever they want to get access that's of interest to the government. It's academia. It's looking for zero-day vulnerabilities with contests and then feeding them into the government. So it's a whole ecosystem.”

U.S. agencies and companies have to work harder to expose the tools and infrastructure used by Chinese organizations to force them into expending more resources to start over.

Volt Typhoon’s failure forced China’s government to “drop back to the drawing board,” according to Walter.

“They had to yell at their companies who potentially were overly sloppy when targeting networks. They had to reassess how they were going to go after the United States,” she explained.

“All of that puts sand in the gears and puts friction in their spaces, and that's really our goal, at least from an intelligence perspective. Exposure makes them have to go back to the drawing board.”

The U.S. officials did not mention Salt Typhoon, the Chinese operation accused of hacking U.S. telecommunications companies. On Tuesday, national security transparency nonprofit Property of the People released a Department of Homeland Security memo from June that said Salt Typhoon breached an unidentified state's National Guard network.

No previous article

No new articles

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.
