April 18, 2024

Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says

Partnerships, joint operations, and private sector vigilance can help us fight back

Director Wray, right, speaks with Vanderbilt University Chancellor Daniel Diermeier during the Vanderbilt Summit on Modern Conflict and Emerging Threats in Nashville on April 18, 2024.

FBI Director Christopher Wray on April 18 warned national security and intelligence experts, as well as students, that risks the government of China poses to U.S. national and economic security are “upon us now”—and that U.S. critical infrastructure is a prime target.

“The PRC [People’s Republic of China] has made it clear that it considers every sector that makes our society run as fair game in its bid to dominate on the world stage, and that its plan is to land low blows against civilian infrastructure to try to induce panic and break America’s will to resist,” he said in remarks at the Vanderbilt Summit on Modern Conflict and Emerging Threats in Nashville.

But he suggested that partnerships with both the private sector and academia can be powerful tools in the quest to neutralize this threat.

Understanding the Threat

The overall threat from the Chinese Communist Party (CCP) is a hybrid one that involves crime, counterintelligence, and cybersecurity—and which the FBI is countering with resources from all three missional spheres, Wray said.

The threat is partially “driven by the CCP’s aspirations to wealth and power,” Wray said, adding that China wants to “seize economic development in the areas most critical to tomorrow’s economy,” even if doing so requires theft. The Chinese government has tried to pilfer “intellectual property, technology, and research” from nearly every industry in the U.S. economy, he noted.

But the CCP also wants to prevent the United States from being able to get in the way of a potential future “crisis between China and Taiwan by 2027,” he said. Americans are starting to feel the effects of this sprint, he said, pointing to “cyber intrusions and criminal activity” as early deterrence efforts by the CCP.

Budgets currently being crafted will determine what resources the U.S. government will have available to fight back three years from now. “In the private sector and academia, too, the investments, partnerships, security, and capabilities you’re building today will dictate how those sectors are prepared—or not—three short years from now,” he added.

Protecting Critical Infrastructure

The FBI worries what this sprint means for our country's critical infrastructure, since “these vital sectors—everything from water treatment facilities and energy grids to transportation and information technology—form the backbone of our society.”

“The fact is, the PRC’s targeting of our critical infrastructure is both broad and unrelenting,” he said. And, he added, the immense size—and expanding nature—of the CCP’s hacking program isn’t just aimed at stealing American intellectual property. “It’s using that mass, those numbers, to give itself the ability to physically wreak havoc on our critical infrastructure at a time of its choosing,” he said.

This risk isn’t new, he said. CCP-sponsored cyber actors "pre-positioned” themselves to potentially mount cyber offenses against American energy companies in 2011—targeting 23 different pipeline operators.

But, Wray explained, their behavior gave us hints about their motivations.

“When one victim company set up a honeypot—essentially, a trap designed to look like a legitimate part of a computer network with decoy documents—it took the hackers all of 15 minutes to steal data related to the control and monitoring systems, while ignoring financial and business-related information, which suggests their goals were even more sinister than stealing a leg up economically,” he said.

Similarly, he said, during the FBI’s recent Volt Typhoon investigation, the Bureau found that the Chinese government had gained illicit access to networks within America’s “critical telecommunications, energy, water, and other infrastructure sectors.” But, he noted, the CCP has also targeted critical infrastructure organizations through more “scattershot, indiscriminate cyber campaigns” that also impact other victims—such as their Microsoft Exchange hack in 2021, which "targeted networks across a wide range of sectors.”

"The PRC [People’s Republic of China] has made it clear that it considers every sector that

makes our society run as fair game in its bid to dominate on the world stage, and that its plan is to land low blows against civilian infrastructure to try to induce panic and break America's will to resist."

FBI Director Christopher Wray

How We're Fighting Back

The FBI's ability to both collect and act on intelligence is crucial to our fight against the China threat. On the cyber front, this includes sharing lessons learned with the private sector and outreach to potential victims, using our technical prowess to halt cyber intrusions and safeguard victims, and taking additional "law enforcement actions" to disrupt and deter cyber incidents.

The FBI fights back against China through Bureau-led "joint, sequenced operations" alongside our partners. "As part of those operations, we're often sharing targeting and other information with partners like U.S. Cyber Command, foreign law enforcement agencies, the CIA, and others, and then acting as one," he said.

Wray used the FBI's responses to the aforementioned cyber compromises to illustrate what these collaborative operations can look like in practice.

In the case of the Microsoft Exchange hack, he said, the FBI "leaned on our private sector partnerships, identified the vulnerable machines, and learned the hackers had implanted webshells—malicious code that created a back door and gave them continued remote access to the victims' networks."

From there, he said, we co-authored and distributed a joint cybersecurity advisory with our partners at the Cybersecurity and Infrastructure Security Agency to arm "network defenders" with "the technical information they needed to disrupt the threat and eliminate those backdoors."

And when some victims had trouble removing the dangerous code on their own, the FBI worked with Microsoft to execute “a first-of-its-kind surgical, court-authorized operation, copying and removing the harmful code from hundreds of vulnerable computers ,” he explained. This, in turn, removed the hackers’ access to victims’ networks.

And in the case of Volt Typhoon, the FBI leveraged partnerships to share threat intelligence and to combat the actors responsible for the hack. After the Bureau learned that the malware was targeting U.S. critical infrastructure, we co-authored similar advisories that characterized the threat, called out the perpetuators, and provided victims with guidance for protecting themselves.

Then, we collaborated with private sector partners “to identify the threat vector and conduct a court-authorized operation—in coordination with others—to not only remove Volt Typhoon’s malware from the routers it had infected throughout the U.S., but also to sever their connection to that network of routers and prevent their reinfection.”

How Partners Can Join the Fight

Wray said that private sector organizations and academia, alike, can partner with the FBI to protect the nation’s “most essential networks” and to conduct “joint, sequenced operations.”
Since private companies own most of our nation’s critical infrastructure, they can help the FBI by defending against Chinese attacks and sharing "vital information about what adversaries are doing—or preparing to do—against us,” he said.

Vigilance, he said, is vital to this effort. “That includes resiliency planning—things like developing an incident response plan, actually testing and exercising that plan, and fortifying networks and devices to make the attack surface as inhospitable as possible,” he added. These plans should indicate when a company will contact the Bureau for assistance in the event of a cyber intrusion, he noted.

Likewise, he encouraged private sector organizations to keep an eye on their “hardware and supply chains” to avoid potential compromise, such as the Solar Winds hack that used “innocuous-looking software updates” as a vector.

“Vetting your vendors, their security practices, and knowing who’s building the hardware and software you’re granting access to your network is crucial, so push for transparency into what vendors and suppliers are doing with your data and how they will maintain it,” he said.
Wray said partnerships are critical to countering the risk posed by China, and that it’s vital for cyberattack victims to promptly notify the FBI. That way, we can gather threat intelligence that can help us both assist victims and mitigate risk to other organizations and sectors.

“We’ve seen the best outcomes in situations where a company made a habit of reaching out to their local FBI field office even before there was any indication of a problem, because that put everyone on the same page and contributed to the company’s readiness,” he said.

The FBI has also been long-dedicated to cultivating bonds within academia, he said, noting that partnerships between the FBI and academic institutions can give the Bureau a better understanding of the issues these institutions face when interacting with the Chinese government. They can also benefit academia by giving institutions “a better understanding of national security threats and make informed decisions about how to deal with them,” he added.

Resources:

- Director Wray's Remarks at the Vanderbilt Summit on Modern Conflict and Emerging Threats
- Inside the FBI Podcast: Technology & Espionage