

# The Wire *China*

COVER STORY

## Access Denied

Can Jen Easterly solve the China hacking problem?

BY BRENT CRANE – MAY 26, 2024

POLITICS

PROFILE

SECURITY

TECHNOLOGY



Illustration by Luis Grañena

In January, Jen Easterly, the eccentric director of America's youngest federal watchdog, the Cybersecurity and Infrastructure Security Agency (CISA), shook the proverbial lapels of lawmakers on Capitol Hill. Testifying before the congressional Select Committee on China, Easterly made plain that the U.S. was facing an unprecedented [danger](https://www.youtube.com/watch?v=kWFihTC2pOs&ab_channel=CISA) thanks to Beijing's increasing cyberspace prowess.

"In recent years, we have seen a deeply concerning evolution in Chinese targeting of U.S. critical infrastructure," she said. "This is a world where a major crisis halfway across the planet could well endanger the lives of Americans here at home through the disruption of our pipelines, the severing of our telecommunications, the pollution of our water facilities and the crippling of our transportation modes."

0:00 / 0:51

Despite the technical complexities of cyberspace, Easterly speaks with the matter-of-fact, clear diction of a kindergarten teacher — albeit one hoping to frighten her students and jar them out of complacency. Hacking events, after all, occur more or less routinely across the economy and government, and CISA has been tasked with both stemming leaks and preventing them since its founding in 2018. It operates as a kind of digital clearinghouse, identifying cyber threats and communicating them to an oft-hacked government and public, among other efforts. [Richard Forno](https://coeit.umbc.edu/deans-office-team/person/ma34575/) (<https://coeit.umbc.edu/deans-office-team/person/ma34575/>), a veteran cybersecurity expert who has advised federal agencies, compares it to “a cyber version of FEMA.”

**Jen Easterly speaks before the Select Committee on China, January 31, 2024. Credit: [Select Committee](https://youtu.be/kWFihTC2pOs?si=X4QHBjICw5uJART) (<https://youtu.be/kWFihTC2pOs?si=X4QHBjICw5uJART>)**

Yet in Easterly’s telling, the disaster is never-ending.

“The threat environment is getting more complex and more dynamic,” she told *The Wire China*. “Our peer competitors, our nation state adversaries, continue to put more resources into cyber. No one should underestimate the transformational nature of what we’re doing.”



**Jen Easterly solves a Rubik’s Cube during a keynote speech delivered during Black Hat USA, August 5, 2021. Credit: [CISA](https://www.youtube.com/watch?v=q7bu-L-m4K4) (<https://www.youtube.com/watch?v=q7bu-L-m4K4>)**

It’s difficult to imagine a better teacher on this subject than Easterly; the former military and intelligence official has both a comfort with the technical and a knack for spectacle. During her many public talks promoting CISA, she often solves a Rubik’s Cube on stage, a kind of flex for the audience that she is not daunted by complex problems. For a federal official, she also dresses ostentatiously, often appearing in calf-high cowboy boots, a leather jacket or scruffy jeans adorned with dragons. During a recent video conference with *The Wire* from her office, she wore a nose ring with a white tee emblazoned with the Ukrainian flag. A blue guitar was visible behind her.

Such a blithe aesthetic fits with the cybersecurity crowd — keyboard warriors with a countercultural ethos — which Easterly surely knows.

“She wants to get the cybersecurity community all moving in the same direction and aligned with security goals,” says [James Andrew Lewis](https://www.csis.org/people/james-andrew-lewis) (<https://www.csis.org/people/james-andrew-lewis>), a senior vice president at the Center for Strategic and International Studies. “She’s playing to her audience.”

**Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways**

Release Date: February 29, 2024      Alert Code: AA24-060B

**ACTIONS TO TAKE TODAY TO MITIGATE CYBER THREATS AGAINST IVANTI APPLIANCES:**

1. Limit outbound internet connections from SSL VPN appliances to restrict access to required services.
2. Keep all operating systems and firmware up to date.
3. Limit SSL VPN connections to unprivileged accounts.

**A CISA advisory on vulnerabilities in Ivanti software products being exploited by threat actors, February 29, 2024. Credit: CISA (<https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b>)**

With a \$3 billion budget, CISA has hired over 1,750 employees since Easterly joined in 2021. And yet the pace of attacks appears to be gaining steam. Over the last six months alone, notes [Daniel Castro](https://itif.org/person/daniel-castro/) (<https://itif.org/person/daniel-castro/>), vice president at the Information Technology and Innovation Foundation, there have been numerous high-profile [attacks](https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents) (<https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>) involving American targets: on Microsoft's corporate systems, on an [Indiana water plant](https://www.cnn.com/2024/04/22/politics/russia-linked-hacking-group-targets-indiana-water-plant/index.html) (<https://www.cnn.com/2024/04/22/politics/russia-linked-hacking-group-targets-indiana-water-plant/index.html>), on a [Texas water tank](https://spectrumlocalnews.com/tx/south-texas-el-paso/news/2024/04/17/russian-linked-hackers-suspected-of-texas-cybersecurity-attack) (<https://spectrumlocalnews.com/tx/south-texas-el-paso/news/2024/04/17/russian-linked-hackers-suspected-of-texas-cybersecurity-attack>), on [United HealthGroup](https://www.reuters.com/technology/cybersecurity/hhs-opens-probe-into-hack-unitedhealth-unit-2024-03-13/) (<https://www.reuters.com/technology/cybersecurity/hhs-opens-probe-into-hack-unitedhealth-unit-2024-03-13/>). In February, CISA itself was the [victim](https://therecord.media/cisa-takes-two-systems-offline-following-ivanti-compromise) (<https://therecord.media/cisa-takes-two-systems-offline-following-ivanti-compromise>) of an intrusion into its networks.

Often, the attackers are nations; CISA refers to Russia, Iran, North Korea and China as the “usual suspects.” And while each adversary's ambitions and capabilities concern CISA, it is China and its rapidly progressing capability that takes up the most bandwidth. “China is the threat that I'm most concerned about and have prioritized for the agency,” says Easterly.

Under Xi Jinping, China's technological capabilities have ballooned alongside its security state. China boasts the most software developers of any country (7 million), and several of the world's biggest and most adept technology behemoths — such as [Huawei](#) —, [Tencent](#) — and [Baidu](#) — — are Chinese firms. In recent years, Chinese universities have also begun offering cybersecurity degrees which appear to mimic American programs.

**[Jen Easterly] brought with her [to CISA] a wide set of experience points. This reflects the way CISA likes to think of its central role as a multi-stakeholder agency, which she personified.**

— [Asaf Lubin](https://law.indiana.edu/about/people/details/lubin-asaf.html) (<https://law.indiana.edu/about/people/details/lubin-asaf.html>), a cyber law scholar at Indiana University

“The government was literally saying, ‘We need cyber talent,’ so the universities started offering these degrees,” says Mei Danowski, a cyber threat researcher and expert (<https://nattothoughts.substack.com/p/i-soon-another-company-in-the-apt41>), on China’s booming cybersecurity ecosystem.

In February, it was revealed the extent to which China’s state security organs tap private firms to conduct intelligence operations. A massive cache of emails from the Chengdu-based cybersecurity firm **i-Soon** — were leaked (<https://www.thewirechina.com/2024/03/03/hacking-the-hackers-i-soon-chengdu-404-data-leak/>) and showed in intimate, often mundane detail how profit-driven firms engage in the state’s hacker-for-hire operations. “We had seen clues here and there but this gave us the whole picture,” says Danowski.



NEWS AND ANALYSIS

## Hacking the Hackers

BY ELIOT CHEN

The Chinese hacking company at the center of a major data leak this month has strong connections within China’s cyber security industry and to the...

(<https://www.thewirechina.com/2024/03/03/hacking-the-hackers-i-soon-chengdu-404-data-leak/>)

The enormity of China’s offensive cyber activity is “way beyond anything we’ve ever seen,” says Nigel Inkster, former head of operations at MI6, the British intelligence service, and an expert on Chinese spying. “The imperative to collect intelligence on potential adversaries and critics is such that nothing is off limits and there appear to be no political constraints on collecting. China no longer seems to care about getting caught with its fingers in the till.”

In other American arenas — politics, business, trade — there is a contentious debate about the shape of the China threat. Critics claim that America has entered into a “[new red scare](https://archive.is/704dA) (https://archive.is/704dA).” Although cyber alarmism could be construed as part and parcel of that, many experts argue that the alarm here is fully warranted. Easterly is certainly doing her part to ring it, but with the nation being overwhelmed nonetheless, some ask if CISA is up to the task of fighting back.

“If you were comparing CISA to the FAA and this many planes were crashing on a monthly basis, you’d say something was terribly wrong,” says Castro. “It’s almost become normalized to see these types of attacks.”



**Former CISA director Chris Krebs Chris Krebs speaks speaks with reporters about efforts to secure the 2020 elections, November 3, 2020. Credit: DHS**

And yet, ironically, what has not been totally normalized is CISA's existence. In 2020, former president Donald Trump fired CISA's inaugural director, Chris Krebs, in a vindictive rage for insisting (<https://apnews.com/article/top-officials-elections-most-secure-66f9361084ccbc461e3bbf42861057a5>) that the 2020 election was “the most secure in American history.” (Trump and his base falsely contend that the election was stolen by Democrats in a vast conspiracy involving hacked voting machines.) Under Easterly, CISA has continued to focus on election integrity. It has also ventured into the politically-fraught arena of monitoring online misinformation. All of this has made CISA a target for some Republican lawmakers, who have threatened (<https://www.politico.com/news/2023/10/22/conservatives-cyber-cisa-politics-00122794>) to smother CISA in the cradle.

“CISA has an enormous amount of agency,” Senator Rand Paul, a vocal CISA critic, said ([https://www.youtube.com/watch?v=p\\_YfXwEobBM&ab\\_channel=ForbesBreakingNews](https://www.youtube.com/watch?v=p_YfXwEobBM&ab_channel=ForbesBreakingNews)) last year. “At this point, we should be circumscribing CISA's powers, not expanding them.”

Alongside these political threats, CISA is engaged in a constant tug-of-war with the private sector. The agency depends on companies to report cyberattacks and share information about its operations with them. After all, private firms control much of the public sphere, including electrical grids, oil pipelines, ports, internet search engines and social media platforms. All of these nodes are eminently hackable — a vulnerability that was recently underscored by a Chinese espionage campaign known as Volt Typhoon, which hacked into dozens of American critical infrastructure organizations and greatly alarmed Washington.





CISA's team in attendance during the RSA Security Conference in San Francisco, May 9, 2024. Credit: CISA via Flickr (<https://www.flickr.com/photos/cisagov/53727934784/in/datetaken/>)

Although public and private sector interests don't always align, CISA must find ways to coax companies into working with it. Protecting physical infrastructure in cyberspace comes with unique challenges, notes [Alexander Urbelis](https://www.crowell.com/en/professionals/alexander-urbelis) (<https://www.crowell.com/en/professionals/alexander-urbelis>), a cybersecurity-focused attorney who has worked with CISA. Operational technologies — the tech that controls physical things — “are very different [from informational technologies] to maintain, to patch or take down,” says Urbelis. “The processes by which you do that are a lot harder and less mature.”

Or as Castro aptly puts it: “CISA is not in charge of the infrastructure that they have to protect.”

Easterly's challenge, then, is not just to shore up America's paltry cybersecurity defenses and patch up the myriad intrusions, but to persuade the country to let it.

## POWERING UP

In September 2015, two months after Chinese hackers stole the security dossiers of 22 million Americans from the Office of Personnel Management, Xi Jinping visited the White House. Beyond cyberespionage, China had also been engaged in hacking American companies, including the nuclear power plant manufacturer Westinghouse and the solar cell manufacturer SolarWorld, to steal intellectual property. Such corporate thievery had long rattled Washington, and [speaking](https://www.youtube.com/watch?v=4lhQjsbkAPI&ab_channel=TheObamaWhiteHouse) ([https://www.youtube.com/watch?v=4lhQjsbkAPI&ab\\_channel=TheObamaWhiteHouse](https://www.youtube.com/watch?v=4lhQjsbkAPI&ab_channel=TheObamaWhiteHouse)) beside Xi in the Rose Garden, President Barack Obama made a not-so-subtle warning to his Chinese counterpart.

“We have jointly affirmed the principle that governments don't engage in cyber espionage for commercial gains against companies,” he said. “What I've said to President Xi and what I'd say to the American people is: Are words followed by action? We will be watching carefully to make an assessment as to whether progress has been made in this area.”

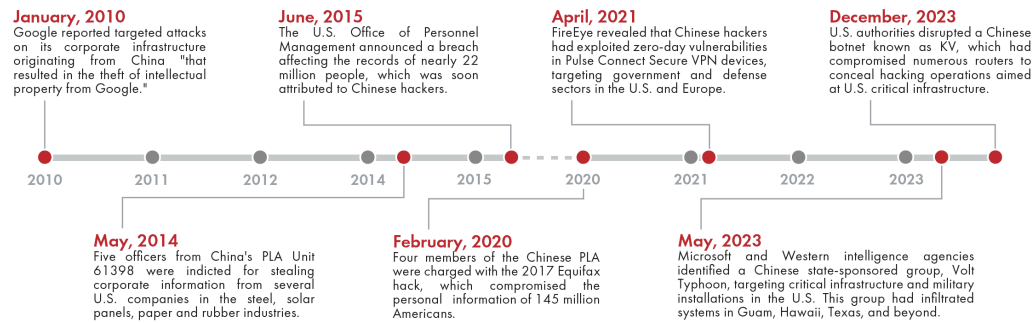
0:00 / 1:30

Then President Obama speaks at a press conference, September 25, 2015. Credit: [The White House](https://youtu.be/4lhQjsbkAPI?si=eQ0Q6ULnO_6wOhQ9) ([https://youtu.be/4lhQjsbkAPI?si=eQ0Q6ULnO\\_6wOhQ9](https://youtu.be/4lhQjsbkAPI?si=eQ0Q6ULnO_6wOhQ9))

Nearly a decade later, progress has been made, but not in the way Obama intended. After a brief lull in cyber operations following the summit, China ramped up its efforts. In 2017, [Equifax](https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking) (https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking), a large credit reporting agency, suffered a massive data breach eventually attributed to Chinese military personnel. Then, in early 2018, Chinese hackers [infiltrated](https://www.reuters.com/article/idUSKCN1J42MK/#:~:text=The%20hacked%20material%20comprised%20614,warfare) (https://www.reuters.com/article/idUSKCN1J42MK/#:~:text=The%20hacked%20material%20comprised%20614,warfare) the computers of a US navy contractor, pilfering sensitive undersea warfare plans. More sophisticated attacks have followed, and China has now come close to matching U.S. capabilities in cyberspace.

### Chinese Cyber Strikes

A timeline of major hacks attributed to China.



China was not the only reason for creating CISA, however. For decades, foresighted Americans, like the former Rhode Island congressman Jim Langevin, advocated for the creation of a federal cybersecurity agency. When, in 2008, Russian hackers [infiltrated](https://www.politico.com/story/2018/11/29/a-decade-after-russia-hacked-the-pentagon-trump-unshackles-cyber-command-961103) (https://www.politico.com/story/2018/11/29/a-decade-after-russia-hacked-the-pentagon-trump-unshackles-cyber-command-961103) U.S. military networks, it initiated "a real wake-up call" for Washington, says Easterly. Inter-department agencies appeared like mushrooms to secure the new digital frontier, including the FBI's Cyber Division, the Department of Defense's Cyber Command, and the CIA's Operations Support Branch.

#### SEC. 1652. **CYBERSPACE SOLARIUM COMMISSION.**

(f) DUTIES.—The duties of the Commission are as follows:

(1) To define the core objectives and priorities of the strategy described in subsection (a)(1).

(2) To weigh the costs and benefits of various strategic options to defend the United States, including the political system of the United States, the national security industrial sector of the United States, and the innovation base of the United States.

(5) To review adversarial strategies and intentions, current programs for the defense of the United States, and the capabilities of the Federal Government to understand if and how adversaries are currently being deterred or thwarted in their aims and ambitions in cyberspace.

(6) To evaluate the effectiveness of the current national cyber policy relating to cyberspace, cybersecurity, and cyber warfare to disrupt, defeat and deter cyber attacks.

(7) In weighing the options for defending the United States, to consider possible structures and authorities that need to be established, revised, or augmented within the Federal Government.

An excerpt from the John S. McCain National Defense Authorization Act for Fiscal Year 2019, in which the Cyberspace Solarium Commission was established. *Credit:* [Congress.gov](https://www.congress.gov/bill/115th-congress/house-bill/5515/text) (https://www.congress.gov/bill/115th-congress/house-bill/5515/text)

CISA's precursor was the National Protection and Programs Directorate, which launched in 2007 as an office within the Department of Homeland Security. (Today CISA operates independently within DHS.) In 2019, soon after CISA's inauguration granted it a wider mandate and authority, cyber specialists formed an intergovernmental advisory body called the [Cyberspace Solarium Commission](https://www.solarium.gov/about) (https://www.solarium.gov/about), which aimed to shape the young entity. The commission's

recommendations included bolstering public-private collaboration and crafting cyber incident response plans, and it was hugely important to CISA's molding, says Easterly, who was involved with the commission as a specialist.

But such a vaunted mission only succeeds if people know that your agency exists in the first place. Part of Easterly's job then is a marketing one, to raise CISA's profile.

"What you have to do when you're building a new institution is force your way into the infrastructure of the government, and she is trying to do that," says Mark Montgomery, a co-founder of the Solarium Commission who is now at the Foundation for Defense of Democracies. "It's about being known as the leader so that when a crisis develops, they're coming to you."



**From left to right: Jen Easterly, Paul Nakasone, Jason Sudeikis, Stephen Davis, and Tomothy White, at the RSA Security Conference, May 2024. Credit: @CISAJen via X (<https://x.com/CISAJen/status/1788215591717028335/photo/1>)**

Easterly has certainly been making that case for herself. As CISA director, she is constantly on the move, meeting state officials, Fortune 500 CEOs and celebrities like Jason Sudeikis. She regularly delivers speeches at hacker conferences, fundraisers and universities, and sits for interviews with 60 Minutes, Meet the Press and others. CISA has even created special Rubik's Cubes with its logo — a prized possession for recipients and a kind of calling card for Easterly's impact on the agency.

Throughout all her appearances, she has also honed her version of a stump speech — weaving her personal history with a sense of higher purpose and government service. From suburban Washington (both her parents worked in the Reagan administration), Easterly graduated high school as valedictorian and has said she surprised everyone when she chose to attend the United States Military Academy at West Point. She went on to become a Rhodes Scholar at Oxford, before serving in the army for 20 years. After 9/11, she became an assistant to General David Petraeus, whom she considers a mentor; then served as the executive assistant to Condoleezza Rice when she was the national security adviser; and in 2007, deployed to Baghdad with the National Security Agency (NSA). Her motto at this time, she has [said](https://archive.is/qM4Yt#selection-521.246-521.284) (<https://archive.is/qM4Yt#selection-521.246-521.284>), was, "Work like a dog, live like a monk." In Iraq, she was tasked with launching into the battlefield a cutting-edge surveillance system to monitor insurgents. This technically challenging experience shaped her understanding of "the power of technology and how threat actors use it," she says.

Afterwards, Easterly helped establish U.S. Cyber Command, one of 11 combatant commands under the Department of Defense that is responsible for protecting America's military communications networks. After retiring from the army with two bronze stars, she served as deputy director of the NSA for counterterrorism from 2011 to 2013 in Kabul. Then, during Obama's second term, she served as a special assistant to the president and a senior director for counterterrorism on the National Security Council.



“She brought with her [to CISA] a wide set of experience points,” says [Asaf Lubin](https://law.indiana.edu/about/people/details/lubin-asaf.html) (<https://law.indiana.edu/about/people/details/lubin-asaf.html>), a cyber law scholar at Indiana University. “This reflects the way CISA likes to think of its central role as a multi-stakeholder agency, which she personified.”

As illustrious as her public service career was, Easterly insists that it was her experience in the private sector, running cybersecurity for [Morgan Stanley](#) —, which best prepared her for CISA. In her four-plus years at the banking behemoth, she came to understand “how big companies think about their technical ecosystem, work with major financial institutions and interface with the U.S. government,” she says.

In her estimation, this interfacing was performed poorly. “I didn’t think that the government was well positioned to be effectively collaborating and sharing with the private sector and that was one of my key motivators [for returning to government],” she says.

Getting this public-private relation right is a major part of her current job, and so far, observers say, she is making progress. In particular, defenders point to the [Joint Cyber Defense Collaborative](https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative) (<https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative>), a body of company and government representatives designed to respond swiftly to cyber incidents. (Members include Amazon Web Services, [Microsoft](#) —, Verizon and Google, among others.) Another success is her [Cyber Safety Review Board](https://www.cisa.gov/cyber-safety-review-board-csr-b-members) (<https://www.cisa.gov/cyber-safety-review-board-csr-b-members>), an advisory body composed of 15 cybersecurity leaders from the private and public sectors, including Google and Gryphon X, which tries to develop lessons learned from serious cyber incidents. CISA also offers free security services to companies, such as vulnerability scanning.

**At a time when the U.S. faces unrelenting security threats from adversaries intent on harming our nation, CISA’s mission should not be undermined for political purposes.**


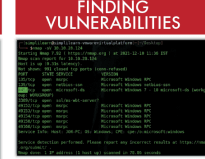
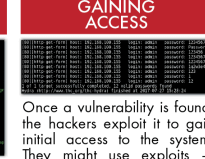
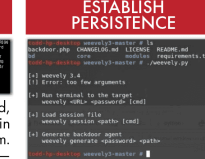
— *Jen Easterly* (<https://www.cisa.gov/about/leadership/jen-easterly>), director of the *Cybersecurity and Infrastructure Security Agency (CISA)*

In late 2021 and 2022, when an extortionist ransomware group known as Lapsus\$ wreaked havoc on companies across the globe, [CISA worked](https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf) ([https://www.cisa.gov/sites/default/files/2023-08/CSRB\\_Lapsus%24\\_508c.pdf](https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf)) with some of the victims (including Microsoft, Verizon, CrowdStrike and Kroll Inc.) to record their incident response procedures and mitigations. While some companies opted not to partake, such post-attack accounting helped CISA develop general defensive guidelines for companies to use in the future.

It is this combination of reactive and preemptive private sector work — or what Easterly deems left and right “of boom” — that CISA is designed for. But it also underscores Washington’s new reliance on private firms in not only countering such assaults, but actively disrupting them.

### Hacking: A How-to Guide

A basic breakdown of how hacks actually work.

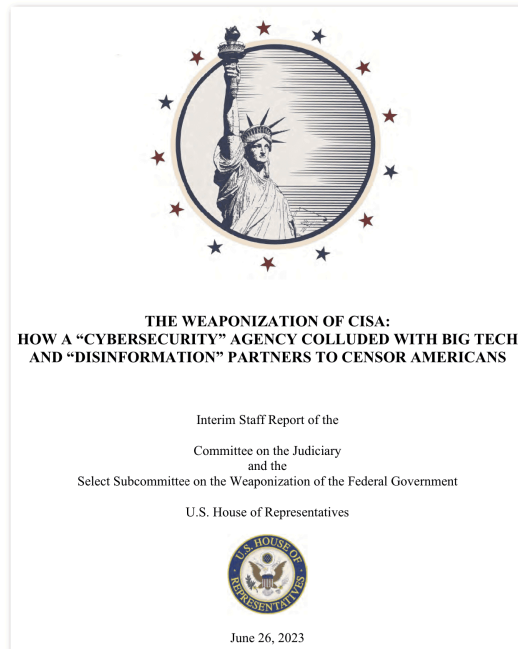
STEP 1: RECONNAISSANCE	STEP 2: FINDING VULNERABILITIES	STEP 3: GAINING ACCESS	STEP 4: ESTABLISH PERSISTENCE	STEP 5: COVERING TRACKS
				
<p>The hackers gather information about their target. This might involve scanning public websites, social media or sending phishing emails.</p>	<p>Hackers look for weaknesses in the target's defenses. Common methods include scanning for outdated software or other digital entryways.</p>	<p>Once a vulnerability is found, the hackers exploit it to gain initial access to the system. They might use exploits — specialized software or scripts designed to take advantage of a vulnerability — or brute force attacks, trying many different passwords until the correct one is found.</p>	<p>After gaining access, hackers want to ensure they can maintain it. They do this by installing malware or creating backdoors.</p>	<p>To avoid detection, hackers will delete activity logs, encrypt stolen data before transferring it or leave false trails.</p>

“A decade ago, it would have been crazy to think that private sector companies would be involved in any way in identifying or tracking these operations, much less that they might be necessary to identify and track those operations,” says Dakota Cary, a China-focused cybersecurity expert. “The perspective was that the U.S. government wouldn’t benefit from private sector engagement on the issue.” What has changed, he adds, is that the private sector has become much more sophisticated in its cyber capabilities. The government, in turn, has become more willing to share information with companies.

Still, companies are often reluctant to reciprocate. They might be afraid that information they share with CISA will someday be used against them by federal regulators. This fear is a sticky problem, Easterly admits. But she contends that there are legal protections in place that protect companies from this scenario, such as the Cyber Incident Reporting for Critical Infrastructure act, put into law in 2022. She also believes her Morgan Stanley experience allows her to more easily coax companies into compliance.

“People don’t trust institutions; they don’t naturally trust the federal government,” she says. “It’s really about everyday building relationships, because life is a contact sport.”

### UPGRADE REQUIRED



***“The Weaponization of CISA”*** (<https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/cisa-staff-report6-26-23.pdf>), June 26, 2023. ***Credit: House Judiciary Committee*** (<https://judiciary.house.gov/media/releases/new-report-reveals-cisa-tried-cover-censorship-practices#:~:text=The%20report%20entitled%2C%20%22The%20Weaponization,cover%20up%20CISA's%20unconstitutional%2C>) ***Select Subcommittee on the Weaponization of the Federal Government***

Another contact sport is politics. In that arena, CISA and Easterly have faced their share of bruising. According to “The Weaponization of CISA,” a blistering congressional [report](https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/cisa-staff-report6-26-23.pdf) (<https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/cisa-staff-report6-26-23.pdf>) published last summer, Easterly’s agency “has ventured well beyond its founding mandate and began targeting constitutionally protected domestic speech for censorship on social media platforms.” The un-authored report, published by a congressional subcommittee led by Ohio congressman Jim Jordan, castigates CISA for what it portrays as the agency conniving with Big Tech to censor “conservative voices,” especially in the context of elections.

In particular, the report claimed that CISA has flagged disinformation to social media platforms, in a process known as “switchboarding,” which the report claims focused overwhelmingly on conservative users. (CISA’s defenders have [argued](https://www.cip.uw.edu/2023/08/23/starbird-house-judiciary-committee-report/) (<https://www.cip.uw.edu/2023/08/23/starbird-house-judiciary-committee-report/>) the report creates a “false impression.”)

This partisan suspicion has trickled into state election officialdom. “When we have our own federal agencies lying to the American people, that’s the most insidious thing that we can do in elections,” [said](https://www.wired.com/story/gop-secretaries-of-state-cisa-controversy/) (<https://www.wired.com/story/gop-secretaries-of-state-cisa-controversy/>) West Virginia Secretary of State Mac Warner, while confronting CISA officials at a panel during the February meeting of the [National Association of Secretaries of State](http://www.nass.org/) (<http://www.nass.org/>). “You all need to clean up your own houses.” Warner, who is now running for governor, later [called](https://thefederalist.com/2024/03/05/why-cisas-censorship-and-election-interference-work-is-the-most-insidious-attack-on-american-democracy/) (<https://thefederalist.com/2024/03/05/why-cisas-censorship-and-election-interference-work-is-the-most-insidious-attack-on-american-democracy/>) CISA’s controversial misinformation activities “the most insidious attack on American democracy that I know of in U.S. history.”



A post on Jen Easterly's X account promoting CISA's #Protect2024 mission. Credit: @CISAJen via X (<https://x.com/CISAJen/status/1755252521675653174>)

Easterly, who rates election integrity as her second biggest focus, denies allegations of censorship. When *The Wire* reached her in late April, she was fresh from a trip to Boston, where she'd met with Massachusetts and Rhode Island election officials. She stressed the imperative for CISA to remain non-partisan and said CISA's work with election officials was "to ensure that they have the cyber resources, physical security and risk management abilities to drive down risk to election infrastructure."

"At a time when the U.S. faces unrelenting security threats from adversaries intent on harming our nation," she adds, "CISA's mission should not be undermined for political purposes."

While election threats include online social engineering campaigns to exacerbate divisions in American society (such as Russia's infamous Internet Research Agency, a state-backed troll farm), threats also include straightforward hacking of election machinery, especially in decisive swing states. While this has not happened, experts say, it is certainly possible. The full-scale manipulation of election machines in America's 3,242 counties, however, is an "insurmountable" challenge, stresses Lewis, who once partook in exploratory war games of this kind. "There is no single point of control in the electoral system to hack," he says.



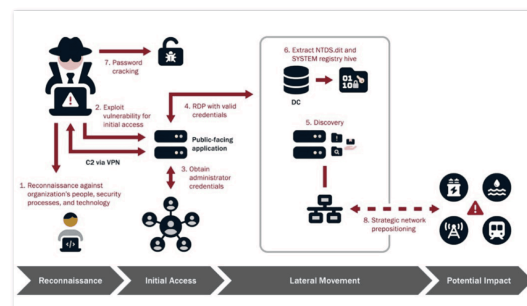
Jen Easterly met with Indiana's Secretary of State Diego Morales to discuss election safety, May 17, 2024. Credit: [Indiana.gov \(https://events.in.gov/event/secretary-morales-meets-with-cybersecurity-and-infrastructure-security-agency-cisa-director-collaboration-on-election-safety-efforts-987\)](https://events.in.gov/event/secretary-morales-meets-with-cybersecurity-and-infrastructure-security-agency-cisa-director-collaboration-on-election-safety-efforts-987)

CISA, Lubin notes, is at least partly to blame for the American suspicion over elections. After all, part of CISA's responsibility is communication. "The fact that 50 percent of the American polity thinks that the election was rigged is a reflection, in part, on CISA not being able to tell a coherent and convincing story about the security and integrity of elections," he says.

But even if America's biggest election denier, former president Donald Trump, prevails in November, CISA's extinction is less likely than a painful down-sizing. While Trump would likely find ways to limit CISA's power, such as withholding funding, CISA enjoys bipartisan support in its more straightforward cybersecurity operations — especially as they relate to China.

Indeed, in Washington, there is a sense that America is under cyber siege, and the panic reached a new level just last year with the Chinese hacking actor known as Volt Typhoon.

In May 2023, Microsoft announced that it had detected Volt Typhoon's intrusions into American infrastructure, including water treatment plants on Guam, which it determined (<https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/>) were meant to "disrupt critical communications infrastructure between the United States and Asia region during future crises." More infrastructure intrusions on the U.S. mainland involving Volt Typhoon were identified soon after by the Five Eyes alliance (the intelligence sharing agreement between Australia, Canada, New Zealand, the United Kingdom and the U.S.). It was Microsoft who first attributed the operation to China, though it has not specified how it knows that.



**Typical Volt Typhoon activity, as outlined on CISA's website. Credit: CISA (<https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>)**

Washington was both shaken and perplexed. Typically, cyber operations are meant to gain or steal information — the Chinese hack of the Office of Personnel Management, for example, resulted in the records leak of nearly 22 million Americans. But Volt Typhoon represented a different, more malicious animal. Although the specific individuals behind the attack remain unknown, Volt Typhoon's intrusions into civilian infrastructure seemed to be a clear preparation for war.

"What you see in Volt Typhoon is an example of how China has approached establishing access to put things under threat," NSA director Timothy Haugh said (<https://archive.is/AyLYc#selection-7125.0-7125.299>) at a security conference in April. "There is not a valid intelligence reason to be looking at a water treatment plant from a cyber perspective."

Volt Typhoon, like the Russian cyber intrusions over a decade before it, was a watershed moment.

"The adversary is betting every day, every hour, every five minutes that the public and private sectors won't get their acts together," adds Montgomery. "Whether it's criminal actors through ransomware or nation-states like Volt Typhoon, they're taking our lunch money."



Easterly’s strategy is to try and force the private sector to get its act together. To prevent hacking incidents, she has placed much of the onus on companies and is encouraging manufacturers to produce more secure products. CISA’s “secure by design” campaign is one of her major initiatives and compels (<https://www.cisa.gov/securebydesign>) companies to design and build products that “dramatically reduce the number of exploitable flaws before they are introduced to the market.”

0:00 / 1:30

“The only way we’re going to get ahead of threat actors is if technology manufacturers design, test, build and deliver tech where security is prioritized,” Easterly says. “China’s cyber actors are very sophisticated. But the reality is that they’ve used pretty simple methods to break into our critical infrastructure. In many ways, we’ve made it easy for them.”

**CISA Senior Technical Advisor Bob Lord explains “secure by design”.** *Credit: CISA* (<https://www.cisa.gov/securebydesign>)

Some 70 companies, including tech behemoths like Google, Cisco and Microsoft, recently signed a “secure by design” pledge ([https://www.theregister.com/2024/05/09/68\\_tech\\_firms\\_sign\\_cisas/](https://www.theregister.com/2024/05/09/68_tech_firms_sign_cisas/)), committing to increase the use of multi-factor authentication across their products within a year, among other such security-focused goals. Though the pledge says they must be able to measurably show progress, there is no legal commitment to follow through.



**CISA’s ‘secure by design’ pledge has also been signed by 17 U.S. and international partners.** *Credit: CISA* (<https://www.cisa.gov/resources-tools/resources/secure-by-design>)

Easterly has said that she sees “secure by design” as a long-term initiative, and while many cyber experts agree in principle, some are skeptical about the practical roll-out.

“Getting all of this right is going to take time and a lot of money,” says Inkster, the former MI6 official. “It’s difficult to see how you get the U.S. tech sector to take ‘secure by design’ as seriously as they ought to, because up until now they’ve had very little incentive to focus on this.”

**During the Cold War, our nuclear arsenal was a deterrent from somebody else using their nuclear arsenal. We're in the same type of arms race when it comes to cyber warfare...**

— *Alexander Urbelis* (<https://www.crowell.com/en/professionals/alexander-urbelis>), a cybersecurity-focused attorney

“Secure by design’ has not exactly been a thing in cybersecurity,” adds Adam Kozy, a former FBI official and China-focused cybersecurity expert. “The internet as we know it is just a patchwork of different types of frameworks, software and hardware integrated together.”



**Jen Easterly speaks during a panel titled “How Can the U.S. Make Sure It Wins the Cyber War of 2028?” during New America’s Future of War Conference, April 9, 2018.**  
*Credit: New America*

For some cybersecurity experts, the more realistic strategy to count on is a simple one of deterrence.

“During the Cold War, our nuclear arsenal was a deterrent from somebody else using their nuclear arsenal,” says Urbelis, the cyber-focused attorney. “We’re in the same type of arms race when it comes to cyber warfare, which focuses specifically on infiltration and maintaining persistence in an adversary’s infrastructure. If I can shut off your lights and you can shut off my lights, we’re not going to turn off each other’s lights.”

But while much ink has been spilled debating Beijing’s cyber prowess, less is known about Washington’s. Experts note it is a safe bet to assume that the U.S. remains the world’s top cyber power, and that the U.S. and its allies are doing the same things to China that China is doing to them. But as a strategy, deterrence is a frustrating one to rely on since it’s difficult to know what the U.S. is capable of. Are we really at the cyber equivalent of mutually-assured destruction?



## Michael Rogers on China's Cyber Threat

BY BOB DAVIS

The head of U.S. Cyber Command under Presidents Obama and Trump on why it's been difficult to change China's behavior and the need for a...

(<https://www.thewirechina.com/2024/01/21/michael-rogers-on-chinas-cyber-threat/>).

There is also the open question of red lines and escalation. Deterrence requires a conviction that your adversary will retaliate, but some experts doubt Beijing is there. As a result, warns Lewis, Beijing is pushing the red lines further and further out.

"They're not that afraid," says Lewis. "They're doing reconnaissance for an attack." It's a step up in sophistication and aggressiveness, he warns, and "that suggests that they aren't really being deterred."

Easterly seems to agree that China is undeterred. While being upbeat about the progress CISA has made during her tenure, she also recently asked ([https://www.youtube.com/watch?v=aQAiaArE3A&ab\\_channel=HouseAppropriationsCommittee](https://www.youtube.com/watch?v=aQAiaArE3A&ab_channel=HouseAppropriationsCommittee)) the House Appropriations Committee for \$150 million in further funding, in part to expand her "hunting" teams, which found 97 different engagements by Chinese actors in critical infrastructure during fiscal year 2023.

"We have eradicated and evicted these Chinese cyber actors in multiple sectors," she told the committee. "But we believe this is just the tip of the iceberg."

Her request is being considered.



Brent Crane is a journalist based in San Diego. His work has been featured in *The New Yorker*, *The New York Times*, *The Economist* and elsewhere. [@bcamcrane](https://twitter.com/bcamcrane) (<https://twitter.com/bcamcrane>).