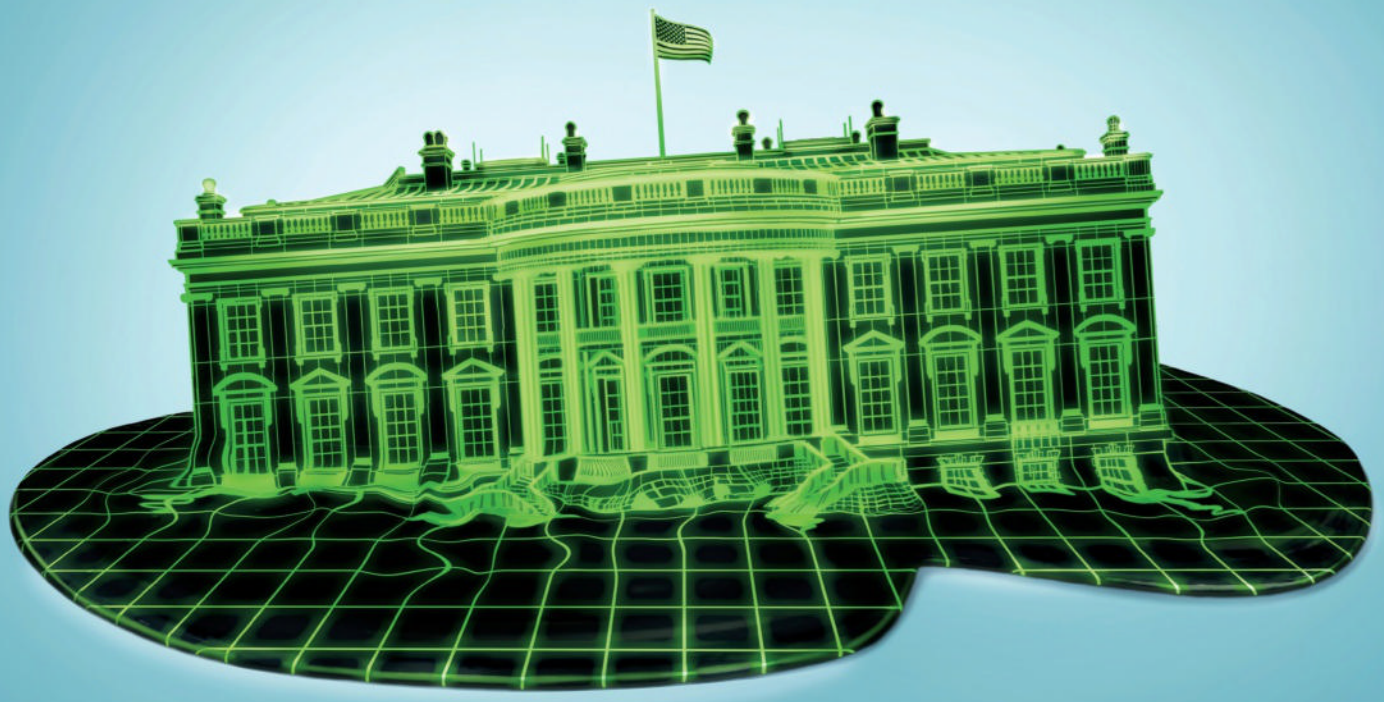

THE CYBER CONUNDRUM

Allies fear Washington is retreating from leadership at the worst possible time.

BY RISHI IYENGAR

In October 2025, representatives from dozens of countries gathered in Singapore for the annual meeting of the International Counter Ransomware Initiative (CRI). Founded by the United States in 2021, the global collective is aimed at combating ransomware, an increasingly prevalent type of cyberattack in which hackers lock victims out of their computer systems unless they agree to pay a hefty sum. It has since grown to include 74 member states and organizations.

For the first time in five years, the initiative's annual gathering was not held in Washington, and U.S. representation was noticeably lacking.

"Traditionally, we have a huge contingent from the U.S.," David Koh, the head of Singapore's Cyber Security Agency, told an audience at a cybersecurity conference in Washington a few weeks later, sitting onstage with his counterparts from Australia and Japan. "This year was different because almost no one from the U.S. administration came."

The Biden administration made multilateral cyber-engagement one of its key policy priorities, appointing the United States' first-ever ambassador-at-large for cyberspace and digital policy to head a new State Department bureau focused on international cyber- and technology cooperation. It supplemented its leadership of the CRI with a multilateral pledge to curb the misuse of commercial spyware, put forward an international cyberspace and digital strategy, and oversaw a significant expansion of the Cybersecurity and Infrastructure Security Agency (CISA), tasked with defending the United States from cyberthreats. But widespread cuts to the U.S. government workforce under President Donald Trump over the past year have impacted nearly all of those efforts.

In explaining why that matters, Koh did not mince words. "You can't look people in the eye if you're not showing up," he said. "My concern is that if we don't do enough of it, then someone else will take the narrative."

That someone else, he made clear during his remarks, is China. The world's second-largest economy has positioned itself as a formidable technological rival to the United States, establishing a near-equal footing (and in some cases, leading) in critical technologies such as semiconductors, artificial intelligence, batteries, biotechnology, and quantum computing. On many of those fronts, Beijing is now providing countries in the middle with viable alternatives. And at the same time, China has emerged as the prime cyber-adversary to the United States and its traditional allies.

"The U.S. plays a unique role because of the global space we operate on across law enforcement, diplomatic, cyber-defense, and intelligence," said Anne Neuberger, who served as the deputy national security advisor for cyber and emerging technology in the Biden administration—a role in which she created and spearheaded the CRI. "So, when we step back, it clearly has an impact."

In assessing the nature of this impact, I spoke to more than a dozen current and former diplomats and government officials from the United States and a half-dozen other countries. Many spoke on the condition of anonymity because they were not authorized to speak on the record. Just about all of them share a nascent but nagging concern: that amid mounting cyberthreats around the world, Washington is pulling back from leadership at the worst possible time.

IN 2024, A GROUP OF CYBERATTACKERS linked to the Chinese government and dubbed Salt Typhoon infiltrated at least eight major U.S. telecommunication networks. The group's attack included targeting cellphones used by then-candidates Donald Trump and J.D. Vance months before the election that put them in the White House.

Ultimately, that hack not only stole the data of millions of Americans but also targeted "telecommunications, government, transportation, lodging, and military infrastructure networks" globally, according to a joint update issued by more than a dozen countries last year. Even with China's long history of cyber-espionage and data theft, Salt Typhoon was seen as unprecedented in scale and scope.

That's not the only "typhoon" (an industry naming convention applied to Chinese hacking groups) giving U.S. officials sleepless nights over the past few years. In 2023, Microsoft revealed that a group it named Volt Typhoon had infiltrated several critical infrastructure networks across the United States, including water, energy, and transportation providers. U.S. security agencies have described its objectives as "pre-positioning" to disrupt those key sectors in the event of a conflict.

Australia's spy chief, Mike Burgess, called out those groups as recently as last November in a speech in Melbourne. "Imagine the implications if a nation-state took down all the networks?" Burgess said. "Or turned off the power during a heat wave? Or polluted our drinking water? Or crippled our financial system?" (Beijing has repeatedly denied any involvement in malicious cyberactivity.)

Despite that growing threat, the Trump administration has pulled back from measures that would have made life more difficult for Chinese hackers. The Federal Communications Commission in November rescinded a Biden administration rule put in place after Salt Typhoon that sought to impose minimum cybersecurity requirements on telecom companies. The Trump administration also reportedly nixed the imposition of sanctions on China's top spy agency over the Salt Typhoon hack weeks after Trump and Chinese President Xi Jinping reached a trade truce in

Illustration by MONA EING and MICHAEL MEISSNER

October, sparking concerns that Trump is compromising U.S. national security in search of deals.

In November 2023, a month into the Israel-Hamas war, an Iran-linked hacking group called "CyberAv3ngers" targeted products made by the Israeli company Unitronics, many of which happened to be used in water treatment plants across the United States.

It was a new type of attack, said Jennifer Lyn Walker, the director of infrastructure cyberdefense at the Water Information Sharing and Analysis Center, an industry body that helps water utilities protect themselves from external threats. "Fast-forward, and we have self-proclaimed hacktivists targeting devices that are managing the flow and quality of our water."

In January 2024, cyberattackers breached multiple local water utilities in rural Texas, resulting in one small-town water tank overflowing for 30 to 45 minutes. The prominent cybersecurity firm Mandiant later attributed that hack to a group in Russia, revealing that the hackers had also claimed credit for an attack on a water provider in Poland during the same time.

Alongside nation-states, ransomware groups are pulling off some of the biggest attacks in recent memory. Russian groups were behind the 2021 Colonial Pipeline hack that shut down much of the U.S. East Coast's fuel supply for a week, leading to long lines at gas stations, as well as the 2024 hack of the insurance payments platform Change Healthcare that impacted nearly 200 million people.

For Washington's European allies, threats from China and other adversaries persist, but the Russian cyberthreat is far more immediate. Russian cyberattacks against NATO countries increased by 25 percent in 2025, according to a recent report from Microsoft. The problem is particularly acute in countries near Ukraine, where Moscow's yearslong ground war has been supplemented by constant cyberattacks against the country and its supporters.

Take Ukraine's neighbor Poland. In 2024, the country's three national Computer Security Incident Response Teams, or CSIRTs, together handled more than 110,000 cyberincidents, according to Rafal Rosinski, the undersecretary of state in the country's Ministry of Digital Affairs. As of November 2025, the biggest of the three CSIRTs had faced more than 224,000 incidents.

"Since the outbreak of Russia's war against Ukraine, we have identified a significant increase in attempted attacks on the transportation sector," Rosinski said.

The attack surface has never been larger, and the threat landscape has never been greater.

"How often have you ever heard anyone speak to you when you've asked about the threat landscape and they say, 'No, it's getting better, actually'?" said Tobias Feakin, who served as Australia's first-ever cybersecurity ambassador between 2017 and 2023. "It never does."

The borderless nature of cyberattacks, coupled with the increasingly digital nature of nearly every aspect of our societies, means that international cooperation and information sharing are more important than ever. When everything is connected, everyone is vulnerable.

"Folks sometimes treat cyber as a separate domain. Countries like China and Russia view it as integrated with the geopolitical competition and into their approach to warfare," Neuberger said. "There's no longer this line between battlegrounds and homeland."

Most cybersecurity officials I spoke to stressed the need to temper the alarmism about a possible U.S. pullback. Every new U.S. administration undergoes a transition period, coordination continues at the operational level where it's most needed, and Washington has remained engaged in a few multilateral forums, such as the Pall Mall Process, a grouping of 25 countries led by France and the United Kingdom aimed at combating commercial spyware. The Trump administration's participation in the CRI, while scaled back, has also not gone the way of the Paris Agreement on climate change, for example.

Trump's proclivity for bilateral engagement has also made its way into cybersecurity, with mentions of cooperation in recent engagements with Thailand, Japan, and South Korea. Washington also went ahead with the 10th annual Japan-U.S. Cyber Dialogue in June 2025.

Still, driving particular concern among many foreign partners are the enormous cuts the Trump administration has made to the United States' own cybersecurity agencies.

CISA, the country's top cyberdefense agency, has been hit with several rounds of layoffs and departures, including further cuts during the recent U.S. government shutdown that reportedly slashed the agency's Stakeholder Engagement Division, tasked with working with international partners. Trump's nominee for CISA director, Sean Plankey, has not yet been confirmed by the Senate, and the agency continues to operate under acting leadership.

Also operating under acting leadership are the Defense Department's Cyber Command and the National Security Agency, whose former head, Gen. Timothy Haugh, Trump abruptly fired in April 2025.

The shuttering of the U.S. Agency for International Development (USAID) by the Trump administration cut more than $175 million worth of cybersecurity assistance to U.S. partners that the agency oversaw.

Multiple diplomats also called out the impact of Trump's downsizing of the National Security Council as curtailing a key avenue for U.S. engagement on cybersecurity.

But the biggest loss by far is being felt at the State Department. Its Bureau of Cyberspace and Digital Policy (CDP)—set

up in 2022 by the Biden administration with Nathaniel Fick as the first U.S. cybersecurity ambassador—gave allies and partners a "good entry point and a clear interlocutor in the system," one diplomat said. That bureau was split up and significantly diminished as part of a broader reorganization of the State Department that eliminated hundreds of jobs. The bureau's cybersecurity functions have been moved into the new Bureau of Emerging Threats, which also oversees policies on artificial intelligence and bioweapons.

International engagement has suffered in the reshuffle.

"There is a serious question about capacity," said Adam Segal, who served as a senior advisor in CDP from April 2023 to June 2024 and led its international cyberspace and digital policy strategy. Given the cuts, he said, there is a "question about how much manpower and bandwidth and attention these things can get with few people there."

A current State Department employee, who also spoke on condition of anonymity because they weren't authorized to speak to the press, said the uncertainty prevails internally as well. "The reorganization didn't give us clarity on where cyber would live and who would run it," the employee said. "It feels like we've just stopped talking about it."

The cuts have also made it "very hard to get anything done. Every bureaucratic process has just gotten much more difficult," the employee added—and "you've just lost the people who knew how to do it."

EVEN IF THE U.S. CYBER-SHAKEUP can send a disconcerting signal, to many partners all that matters is that the work gets done. "The real measure at the end is the investment and buildup of capabilities and what those capabilities are able to do," one European official said. "It's not so important whether we have some cyber ambassadors and what their exact title is."

In addition, the Trump administration has argued that some correction and consolidation are necessary. This represents a sharp reversal from the Biden administration, where the many prominent cybersecurity officials and agencies each had their own—albeit sometimes intersecting and overlapping—remit.

"If there's a broader effort to streamline that and make policy clearer, that's probably not a bad thing," said Jennifer Ewbank, who served as the CIA's deputy director for digital innovation from 2019 to 2024. "But I'm concerned about the loss of cyber-defenders at a time when we do need them."

According to CyberSeek, a U.S. government-backed tool that tracks the cybersecurity workforce in the United States, there are 74 employees for every 100 open jobs, with more than half a million job openings across the country.

It's a problem that Sean Cairncross, the Trump administration's top cybersecurity official, seems acutely aware of. "There is a huge gap in the cyber workforce," he said at the same Washington conference where Singapore's Koh spoke, adding that the U.S. government was working on an initiative to bridge that gap as one of the pillars of its upcoming National Cybersecurity Strategy, expected to be published in January.

The Trump administration released its National Security Strategy—typically a precursor to the cybersecurity strategy—in early December, hinting at the "espionage" and "cybersecurity" risks that come with Chinese foreign assistance in Latin America and outlining a U.S. government plan to help U.S. companies "harden" networks in the region.

As for cybersecurity, it's all about U.S. companies. The "U.S. Government's critical relationships with the American private sector help maintain surveillance of persistent threats to U.S. networks, including critical infrastructure," the strategy said, while the government focuses on defending those networks.

Largely absent in the strategy is any emphasis on cyber-cooperation with allies, save for "encouraging Europe to take action to combat … technological theft, cyber espionage, and other hostile economic practices."

Cairncross, who was confirmed as the national cyber director by the Senate in August, has largely stuck to those themes in his public comments thus far.

"We're focused on … partnership with industry and streamlining the regulatory environment," he said at the Washington conference. He did not provide an exact timeline for releasing the cybersecurity strategy but said that "it's going to be focused on shaping adversary behavior, introducing costs and consequences."

Cairncross also did not mention allies and partners or how the United States plans to engage them, though he has done so—if somewhat cursorily—in previous public comments since assuming his role. "I'm committed to marshaling a unified, whole-of-nation approach on this, working in lockstep with our allies who share our commitment to democratic values, privacy, and liberty," he said at another Washington cybersecurity conference in early September, his first public remarks after getting confirmed. On the diplomatic side, Cairncross said during another public appearance in late October that the Trump administration's goal is to "push the clean American tech stack" to counter China's "attempt to export a surveillance state across planet Earth."

Cybersecurity diplomats around the world are hoping that the United States will not just remain engaged but revert to playing the traditional leadership role it has somewhat pulled back from over the past year.

"The U.S. leaves a uniquely sized gap if and when they are not present," one diplomat said. "We go into 2026 being more aware than ever about that uniquely sized gap." ■

RISHI IYENGAR is a staff writer at FOREIGN POLICY.