www.politico.com /news/2024/02/06/far-right-washington-private-hackers-00139413

The far right is scaring away Washington's private hacker army

By John Sakellariadis 02/06/2024 05:00 AM EST Link Copied ⁝ 10-13 minutes

The Cybersecurity and Infrastructure Security Agency launched the initiative — known as the Joint Cyber Defense Collaborative — in 2021 to enlist outside tech pros in the fight against cybercrime gangs and state-backed hacking outfits following a series of high-profile breaches. | Getty Images

Some of the country's top cybersecurity experts who've been helping protect critical networks say they're quietly retreating from a highly touted government partnership, citing frustrations with its management and pressure from conservative critics.

The Cybersecurity and Infrastructure Security Agency launched the initiative — known as the Joint Cyber Defense Collaborative — in 2021 to enlist outside tech pros in the fight against cybercrime gangs and state-backed hacking outfits following a series of high-profile breaches.

The threat-sharing hub allows elite corporate hackers to quickly exchange signs of suspicious activity with the U.S. government and IT workers defending key parts of the economy, including schools, water facilities, hospitals and pipelines, to respond to or prevent hacks. Participants hail from tech giants like Microsoft, Amazon and Google, as well as infrastructure operators, foreign governments, nonprofits and midsize security firms.

But five external computer security professionals involved in the JCDC told POLITICO they and many colleagues have stopped contributing or have significantly pared back their involvement.

The JCDC "has been dead for a while now," said Juan Andres Guerrero-Saade, a senior technical analyst at SentinelOne, a billion-dollar security firm that participates in the program.

While many of their complaints stem from how the program is organized, the discontent also represents another indirect impact of Donald Trump's 2020 election fraud claims, now threatening to hamper largely apolitical cybersecurity work: CISA's efforts to combat disinformation ahead of the 2020 election has made it a favorite target of conservatives, who accuse it of trying to censor their views online.

Even though the JCDC plays no role in online content moderation, the amped-up scrutiny of CISA has increasingly ensnared the agency's external partners, making JCDC participants fearful they could be caught in the crosshairs.

"There is a huge chilling effect going on," said Marc Rogers, the founder of a nonprofit cyber defense group, the CTI-League, that worked with the agency before the formation of the JCDC. "There is a big worry now in the cybersecurity industry that there is a witch hunt going on against us.

The pullback spells particular trouble for the government because most U.S. networks run on hardware and software that is privately owned. That means CISA often has to lean on tech firms and external cyber specialists to fulfill its core mandate: protecting sensitive government data and critical U.S. infrastructure from hacks.

It also comes at a critical moment for the country's digital defenses. Four of Washington's top cybersecurity officials warned lawmakers Wednesday that Chinese hackers are aggressively burrowing into American infrastructure in preparation for a conflict — and that public-private cooperation, the JCDC specifically, was essential to combating it.

"This has reached a crunch point, where private sector folks are reassessing whether they want to be engaged with the government," Rogers said.

"We absolutely need this type of collaboration," said a senior threat analyst at a half-billion-dollar security firm, who like others interviewed for this story was granted anonymity as a condition of speaking candidly on the matter. "But right now, CISA, JCDC, is a dumpster fire."

CISA Executive Assistant Director Eric Goldstein said the agency had not noticed any significant decrease in outside participation within the JCDC**.** He also argued that aside from the work with external analysts to detect immediate threats, the JCDC's long-term cyber defense planning efforts with industry and agencies like the NSA and FBI remain strong.

Still, Goldstein said external partnerships are essential to daily threat detection, and CISA is keen on finding ways to make sure outsiders feel supported.

"We are eager to work toward an environment where researchers are able to contribute to our common good and our national security without fear for their own safety," he said.

JCDC was born after hacks from Russian cyber-criminal gangs and China-linked operators wreaked havoc on a major gas pipeline, a slew of U.S. hospitals and widely used Microsoft mail servers. The idea was to pair the technical resources and expertise of the private sector with the government's legal authorities, convening power and intelligence insights.

Traditionally, concerns about regulation have made industry hesitant about sharing threat data with the government. Federal agencies have likewise struggled to relay timely information outside their walls due to sensitivities around classified information. CISA, which sits outside the intelligence community and has no regulatory authority, has touted its JCDC as a breakthrough solution to those long-standing problems.

But a growing conservative backlash to CISA's separate work has participants in JCDC worried. A case before the Supreme Court initiated by Republican attorneys general accuses CISA of First Amendment violations for its efforts to fight disinformation largely during the Covid-19 pandemic and the 2020 election, when it forwarded tips about hoaxes it received from state and local election authorities to companies such as Facebook and X.

Three Stanford University researchers who helped CISA address disinformation have faced legal challenges and online harassment. In December, the CTI-League's founders, including Rogers, received death threats after media reports claimed they helped hone CISA's alleged censorship strategy — a charge the group denies.

The reports prompted a pair of hearings in the conservative-led House and a wave of harassing emails, texts and social media posts against the group's founders and volunteers.

CISA did not offer any support to the CTI-League in the wake of the backlash, CTI-League members say, even though the vast majority of the group's work was focused on protecting hospitals and emergency rooms from

cyberattacks — not fighting disinformation.

That left some outside partners uneasy about what would happen if conservative activists targeted them.

“While CISA has loved to name-drop private working group names for street cred, the lack of any statement about the CTI-League has given me a lot of hesitation about a future working relationship,” said Silas Cutler, a cyber threat analyst who participates independently in the JCDC and works for security startup Stairwell.

An executive from a multimillion-dollar cyber intelligence firm said the CTI-League incident prompted their company to pare back a deal to provide CISA with data on ransomware threats, which involve scrambling victims’ data and networks until an extortion payment is made.

“There’s really not the benefit that would justify essentially putting our careers on the line, and helping this agency that doesn’t seem to want to help itself,” the person said. They added their firm will still share that data with other agencies and nongovernmental partners, and would consider scaling back up the partnership with CISA if it offered “a significant showing of support for the community.”

CISA’s Goldstein did not refute the claim that the agency failed to reach out to CTI-League researchers. He pointed out that the group’s work predated the JCDC, though as a general matter, he said the agency recognizes the challenges facing its employees and external partners.

Arlington County Police are currently investigating a false 911 call against the personal residence of CISA Director Jen Easterly in late December. While it remains unclear if the incident was politically motivated, fraudulent police calls — known as swatting attacks — have become a popular weapon for hacking gangs and petty criminals.

“We are well aware that too many researchers do their work under both personal and professional peril,” Goldstein said.

JCDC contributors also question whether the program is effective due to its structure.

The senior threat analyst said CISA once took months to relay a tip that their company had passed along about an imminent ransomware attack. By the time the agency finally reached out, the person said, the victim, a U.S. company, had already been struck.

POLITICO could not independently confirm that account because the person declined to give identifying information on the specific company or a timeline of the incident. But they said their firm now goes around CISA when it has threat data regarding ransomware attacks.

Another major complaint is that the JCDC lacks technical talent from within CISA: every individual interviewed for this story said the agency appears to have staffed it overwhelmingly with lawyers and policy specialists, who can manage relationships with big name firms but aren’t effective at identifying or analyzing tips that get passed to them through a CISA-organized Slack channel.

One former CISA official said only a dozen of the roughly 200 CISA staff members working in the JCDC are technical specialists — something that has hampered its work.

“The JCDC is good at government relations-type work,” the person argued. “But it is not living up to its stated mission” of being a cutting-edge hub to combat hackers.

CISA’s Goldstein pushed back against those claims. Technical experts from other parts of the agency regularly contribute to the JCDC, he said. He also said building effective partnerships required a diverse set of skills and “first working with the company at more of a senior engagement level.”

Goldstein also argued the JCDC continues to help the country mitigate some of the most pressing digital threats, including a sophisticated Chinese campaign to penetrate U.S. infrastructure and potential digital spillover from the wars in Gaza and Ukraine.

Bryan Ware, CISA’s former assistant director for cybersecurity, said he was not surprised by the frustrations some outside security experts felt with the JCDC.

But Ware, who left the agency in 2020 and has since participated in the initiative on the industry side, cautioned against rushing to judgment given how hard the work is.

“This is not easy, there’s no playbook for it,” he said.