ANDREW R. GARBARINO, NEW YORK
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Nineteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

November 26, 2025

Mr. Eddy Zervigon
Chief Executive Officer
Quantum Xchange
3 Bethesda Metro Center #700
Bethesda, MD 20814

Dear Mr. Zervigon:

The Committee on Homeland Security (Committee) is closely examining how advances in artificial intelligence (AI), quantum computing and related technologies, and hyperscale cloud infrastructure are reshaping both defensive capabilities and the operational tradecraft available to state-sponsored cyber actors. Recent disclosures by Anthropic,[1] combined with public reporting indicating that state-sponsored cyber actors from the People's Republic of China (PRC) manipulated Claude-based tools to automate substantial portions of a sophisticated cyber-espionage campaign,[2] underscore the urgent need to understand how emerging AI-driven capabilities and the cloud systems that increasingly enable them can be misused against the United States. This development has direct implications for national security, as adversaries conducting AI-enabled intrusions today may seek to pair these techniques with future quantum decryption capabilities, enabling "harvest-now, decrypt-later" operations that put government, defense-industrial, and critical infrastructure data at long term risk.

As Congress evaluates the risks highlighted by the Anthropic incident, particularly the prospect that adversaries may seek to pair AI-enabled tradecraft with emerging quantum capabilities to undermine today's cryptographic protections, your insight into integrating quantum-resilient technologies into existing cybersecurity systems, managing cryptographic agility at scale, and preparing federal and commercial networks for post-quantum threats will be critical to the Committee's examination. Accordingly, we request that you testify at a joint hearing before the Committee's Subcommittee on Cybersecurity and Infrastructure Protection and Subcommittee on Oversight, Investigations, and Accountability titled, "*The Quantum, AI, and Cloud Landscape: Examining Opportunities, Vulnerabilities, and the Future of Cybersecurity*," on Wednesday, December 17, 2025, at 10:00 a.m. in 310 Cannon House Office Building. Please confirm your attendance by December 3, 2025.

***

[1] Anthropic. *Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign.* Nov. 13, 2025, https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf.
[2] Schechner, Sam, and Robert McMillan. *Chinese Hackers Used Anthropic's AI to Automate Cyberattacks*. The Wall Street Journal, Nov. 13, 2025, https://www.wsj.com/tech/ai/china-hackers-ai-cyberattacks-anthropic-41d7ce76.

According to Anthropic's November 2025 report, *Disrupting the first reported AI-orchestrated cyber espionage campaign*, the company's Threat Intelligence team identified a highly sophisticated operation in mid-September 2025 conducted by a PRC state-sponsored group it designated "GTG-1002."[3] The campaign involved multiple, near-simultaneous intrusion attempts against approximately 30 targets, including major technology firms, financial institutions, chemical manufacturers, and government agencies, and Anthropic's investigation confirmed several successful compromises before the activity was disrupted.[4] During the ten-day response period, Anthropic reportedly mapped the scope of the operation, banned relevant accounts, notified impacted entities, and coordinated with authorities as actionable intelligence was developed.[5]

Anthropic's report and subsequent press coverage describe GTG-1002 as a significant inflection point in adversary tradecraft.[6] Rather than relying on AI solely to draft materials or suggest tactics, the threat actor constructed an autonomous attack framework around Claude Code, using it as both the orchestrator and execution engine across the intrusion lifecycle.[7] This framework leveraged Model Context Protocol (MCP) tools and commodity security utilities to enable Claude to break down complex operations into discrete technical tasks, such as scanning infrastructure, validating vulnerabilities, harvesting credentials, moving laterally, and triaging exfiltrated data, that appeared routine in isolation.[8] Anthropic's analysis and telemetry indicated that Claude executed approximately 80 to 90 percent of the tactical workload at a speed and scale unattainable for human operators, who intervened primarily at strategic decision points, including escalation to exploitation and decisions about which information to exfiltrate.[9]

Alarmingly, Anthropic further concluded that GTG-1002 represents the first documented case of an AI-orchestrated cyberattack largely executed without human intervention at scale, with agentic AI successfully gaining access to confirmed high-value intelligence targets and performing a broad range of post-exploitation activities.[10] At the same time, the company noted that Claude's offensive use exhibited important limitations, including instances in which the model overstated its progress or generated fabricated credentials and findings that did not withstand verification.[11]

This incident is consequential for U.S. homeland security because it demonstrates what a capable and well-resourced state-sponsored cyber actor, such as those linked to the PRC, can now accomplish using commercially available U.S. AI systems, even when providers maintain strong safeguards and respond rapidly to signs of misuse. GTG-1002 shows that agentic AI can function as an operational force multiplier, accelerating timelines, enabling simultaneous multi-vector intrusions, and reducing the resources required to sustain sophisticated espionage campaigns. For cloud providers that host the infrastructure on which these AI systems are developed, deployed, and integrated into enterprise operations, the incident illustrates how

[3] *Id* at 1.
[4] *Id* at 1.
[5] *Id* at 1.
[6] *Id* at 1.
[7] *Id* at 1.
[8] *Id* at 1.
[9] *Id* at 1.
[10] *Id* at 1.
[11] *Id* at 1.

similar autonomous techniques could be directed at, or carried out within, large scale cloud environments. The same characteristics that make AI attractive to state-sponsored cyber actors, including automated analysis, scalable orchestration, and high-speed execution, are similarly critical for strengthening detection, defense, and resilience. Understanding this dual-use balance is essential as Congress assesses the risks, opportunities, and policy implications of advanced AI.

***

To facilitate your appearance and to ensure timely coordination ahead of the hearing, please direct your staff to contact Roland Hernandez with the Committee on Homeland Security Majority Staff at (202) 226-8417 with any scheduling matters or additional questions related to this request.

Per Rule X of the U.S. House of Representatives, the Committee on Homeland Security is the principal committee of jurisdiction for overall homeland security policy and has special oversight of "all Government activities relating to homeland security."

Thank you for your attention to this important matter and your prompt reply.

Sincerely,

ANDREW R. GARBARINO
Chairman
Committee on Homeland Security

ANDY OGLES
Chairman
Subcommittee on Cybersecurity and Infrastructure Protection

JOSH BRECHEEN
Chairman
Subcommittee on Oversight, Investigations, and Accountability

cc: The Honorable Bennie Thompson, Ranking Member
Committee on Homeland Security

The Honorable Eric Swalwell, Ranking Member
Subcommittee on Cybersecurity and Infrastructure Protection

The Honorable Shri Thanedar, Ranking Member
Subcommittee on Oversight, Investigations, and Accountability