

# United States Senate

WASHINGTON, DC 20510

December 2, 2025

Director Sean Cairncross  
National Cyber Director  
Office of the National Cyber Director  
1600 Pennsylvania Avenue NW  
Washington, DC 20500

Dear Director Cairncross,

We write regarding a recent report by Anthropic stating that, in September 2025, Chinese state-sponsored hackers successfully directed the company's AI system to autonomously conduct a sophisticated cyberattack campaign against 30 entities, including government agencies in multiple countries.<sup>1</sup> According to Anthropic, this was "the first documented case of a cyberattack largely executed without human intervention at scale."<sup>2</sup> Given your office's role in countering cyberattacks against the U.S. government, we urge you to continue coordinating with Congress and other federal agencies to address this emerging national security threat.<sup>3</sup>

In September 2025, a well-resourced foreign organization used Claude Code, an advanced agentic AI coding tool from Anthropic, to design cyberattacks against major technology corporations, financial institutions, chemical manufacturing companies, and government agencies across multiple countries.<sup>4</sup> Anthropic's report on these attacks states "with high confidence" that this foreign organization was "a Chinese state-sponsored group."<sup>5</sup> In this sophisticated cyber campaign, the Claude AI system executed 80 to 90 percent of the operation without any human involvement and at speeds that are "physically impossible" for human hackers.<sup>6</sup>

Further, these autonomous AI cyberattacks were successful against several targeted entities.<sup>7</sup> In one case, "the threat actor induced Claude to autonomously discover internal services, map complete network topology across multiple IP ranges, and identify high-value systems including databases and workflow orchestration platforms."<sup>8</sup>

The emerging threat to U.S. cybersecurity posed by foreign adversaries deploying autonomous AI systems requires a robust response from your office and other federal agencies. Accordingly, we request responses to the following questions by January 9, 2026.

---

<sup>1</sup> Anthropic, *Disrupting the First AI-orchestrated Cyber Espionage Campaign*, 2025, p. 3, <https://www.anthropic.com/news/disrupting-AI-espionage>.

<sup>2</sup> Ibid.

<sup>3</sup> *William M. (Mac) Thornberry National Defense Authorization Act*, 6 U.S.C. § 1500 (2021).

<sup>4</sup> Anthropic, *Disrupting the First AI-orchestrated Cyber Espionage Campaign*, 2025, pg. 3, <https://www.anthropic.com/news/disrupting-AI-espionage>.

<sup>5</sup> Ibid.

<sup>6</sup> Ibid.

<sup>7</sup> Ibid.

<sup>8</sup> Ibid., p. 9.

1. Anthropic stated in its report that this operation took place in mid-September 2025.<sup>9</sup> At what point did the company notify the Office of the National Cyber Director, or one of the agencies it coordinates with, about the attack?
2. Which U.S. government agencies have been involved in the investigation and response to this attack? How specifically are these agencies assisting Anthropic and any impacted entities?
3. Is there any evidence that this group targeted U.S. government agencies or contractors? If so, were any of those attacks successful?
4. Is the Office of the National Cyber Director aware of any other cases in which an autonomous AI agent was used in a similar way to conduct a cyberattack?
5. How will your office collaborate with the private sector, and specifically AI technology companies, to limit autonomous AI cyberattacks and mitigate damage from these attacks if and when they occur?
6. How can Congress best support the Office of the National Cyber Director in countering this emerging threat?

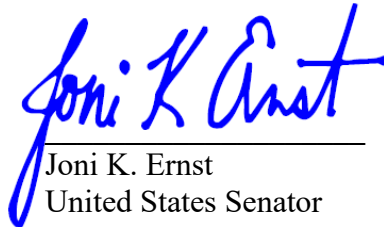
We appreciate your consideration of this issue, and continued work to ensure that the government and people of the United States are protected from cyberattacks.

Sincerely,



---

Margaret Wood Hassan  
United States Senator



---

Joni K. Ernst  
United States Senator

---

<sup>9</sup> Ibid., p. 3.