US spy agency using Anthropic AI tech for cyberwar against China and Iran

Description

Anthropic

The US National Security Agency (NSA) is allegedly using Anthropic software to wage cyberwar against Iran and China. The AI war firm is currently locked in a legal battle with the Trump administration to stop certain military uses. Anthropic bosses previously complained when their tech was used in the 3 January Venezuela raid.

The NSA is the US equivalent of the UKâ??s Government Communications Headquarters (GCHQ). Its remit includes surveillance and cyberwarfare.

The *Financial Times* (FT) reported on 4 June:

> Anthropic is helping the US National Security Agency deploy its powerful Mythos AI model for offensive cyber operations, embedding engineers inside the agency despite an ongoing legal battle with the Pentagon.

Adding

> The San Francisco-based company had installed about half a dozen staff within the NSA as so-called forward-deployed engineers to guide the use of the technology and customise models for specific applications, two people familiar with the arrangement said.

But the embedding suggests that Anthropic is contravening its own rules. As *the Canary* reported in February 2026:

> Anthropic has strict rules on military usageâ?¦ usage guidelines prohibit Claude [an Anthropic software] from being used to facilitate violence, develop weapons or conduct surveillance.

Mythos is Anthropicâ??s most advanced AI system. The firm has said

> Mythos is too dangerous to release publicly.

The *FT* said

> It remains unclear whether Anthropicâ??s engineers are assisting the NSA in active operations. However, one person close to the situation said Mythos would be useful for infiltrating the networks of nations such as China or Iran.

A source close to the firm said

> The best way to build a good defence is [with] a good attack.
>
> If [Mythos] is not used to build attack agents, adversaries will find a way to do it.

Anthropicâ??s row with Trump and Hegseth

The row between Anthropic and the Trump administration has been so intense that defence secretary Pete Hegseth threatened to take over the technology by diktat. He even pledged to designate the firm as a â??supply chain riskâ?? in February 2026 if bosses did not comply with a demand to:

> give the military unfettered access to its Claude AI model by Friday evening or else have the government label it a â??riskâ?• to the supply chain.

The designation is:

> typically reserved for foreign firms with ties to U.S. adversaries, could ban companies that work with the government from partnering with Anthropic.

Anthropic responded

> No amount of intimidation or punishment from the Department of War will change our position on mass domestic surveillance or fully autonomous weapons. We will challenge any supply chain risk designation in court.

Beijing is clearly a target for US AI operations. The FT said that in February 2026:

> the Pentagon was seeking to create AI-powered cyber tools to identify infrastructure targets in China as part of an effort to improve US capabilities in any future military conflict with Beijing.

And on 2 June

> President Donald Trump signed an executive order outlining a voluntary framework in which AI companies can submit their new models for security reviews before they are publicly released.

Anthropic software also meshes with Palantir technology in some US uses. The *Canary* reported with regard to the January 2026 US attack on Venezuela:

> The deployment of Claude occurred through Anthropicâ??s partnership with data company Palantir Technologies, whose tools are commonly used by the Defense Department and federal law enforcement.

Anthropicâ??s programs can be used:

> for everything from summarizing documents to controlling autonomous drones.

The UK is deeply and dangerously enmeshed with Palantir. The Commons technology committee warned on 3 June that the UK should divest from Palantir, which has taken over swathes of British national infrastructure.

Anthropic (at least rhetorically) subscribes to a form of corporate ethics. Palantirâ??s vision is openly far-right. That said, there should be no place for AI firms in intelligence, warfare, surveillance or policing â?? whatever the ideology their CEO claims to follow.

Featured image via Chance Yeh/Getty Images for HubSpot

By Joe Glenton

Source link

CATEGORY

1. News

Category

1. News