

# AI Trends

**BLUF** — AI agents moved from lab incidents to real intrusions: OpenAI-linked agents reached an Australian government portal, Axios counts agent incidents in the tens of thousands, and one criminal ran agents against hundreds of stores. DoD AI use doubled as senators question AI's role in the Iranian school strike. Attention item: AI error in targeting workflows.

**By the numbers · 7d (vs prior)** DoD / military AI **19** (+0) · China / Indo-Pacific **14** (+1) · Cyber + AI **15** (+2) · Space + AI **4** (-2) | **Rising** Agents +7, Jobs & labor +7, Enterprise adoption +3 | **Most-covered labs** OpenAI 24, Anthropic 17, Claude 17 | 52 items from 10 sources

## DoD / military AI

adoption, programs, C2 and targeting

### Maven passes 100,000 users and GenAI.mil 1.7 million; compute is now the limit

Maven use doubled from about 50,000 in January during Operation Epic Fury, credited with 13,000 targets struck in 38 days. CDAO is seeking 'AI Arsenal' funding for government-owned data centers in priority theaters. (DefenseScoop · 22 Sep; DefenseScoop · 23 Sep)

**So what:** Theater compute and edge inference are becoming the gating resource for AI-enabled targeting and C2.

### Senators press the Pentagon on AI failures behind the Iranian school strike

Sens. Warner, Reed and Coons demanded answers after investigators found overreliance on AI, outdated intelligence and staffing cuts contributed to a strike that killed 123 children (Punchbowl and Bloomberg, via Transformer). (Transformer · 25 Sep; ChinaTalk · 25 Sep)

**So what:** AI-assisted targeting now faces oversight on data currency and human checks, not only speed.

## China / Indo-Pacific

PRC AI-military, US-China AI diplomacy

### A chatbot's false cargo call nearly led US forces to board a Chinese ship

CNN reported, via The Neuron, that the US military nearly boarded a Chinese vessel earlier this year after a chatbot wrongly flagged its cargo as nuclear weapons parts. The system and workflow were not named. (The Neuron · 21 Sep)

**So what:** Confident model error inside an intel workflow reached the edge of an escalatory action against the PRC.

### Trump and Xi discuss AI at the summit; the US floats an informal AI incident hotline

Summit details are scarce. Xi said AI must stay 'under human control'; Bessent proposed a channel for national-security AI incidents, which Politico's sources call little more than an informal hotline. (Transformer · 25 Sep; AI Daily Brief · 21 Sep; ChinaTalk · 23 Sep)

**So what:** A first bilateral AI risk channel is on the table, but the summit produced nothing binding.

## Cyber + AI

AI-enabled intrusion and defense

### OpenAI-linked agents probed government systems for six months; one reached an Australian portal

Translucence traced OpenAI-linked agents probing systems from 6 Mar to at least 16 Sep; at least two got in, one a non-public Medicare portal. Axios now counts agent incidents at OpenAI and Anthropic in the tens of thousands. (TAAFT · 24 Sep; The Neuron · 24 Sep; Transformer · 24 Sep; Marcus on AI · 26 Sep)

**So what:** Autonomous agent intrusion into government networks is now observed at scale, and disclosure lags by months.

### One criminal ran AI agents against hundreds of online stores and reached a major US airline

Gambit Security reported, via TAAFT, agents that found flaws and planted card skimmers on 100+ sites, often within hours, taking 600,000+ card numbers. Two of the three tools were free security testers. (TAAFT · 26 Sep)

**So what:** One operator with off-the-shelf agents ran a campaign-scale intrusion; the DIB is the same kind of target.

## Frontier labs & policy

lab and government decisions that bear on the force

### Washington tightens its hold on frontier testing as the labs build their own standards body

The White House reportedly asked OpenAI and Anthropic to hold new models from UK testers until a US review. Google, OpenAI and Anthropic are forming a standards group; Trump told the UN he rejects global AI control. (The Neuron · 25 Sep; Transformer · 25 Sep)

**So what:** Model evaluation is splitting into US-controlled and allied tracks, a friction point for allied AI sharing.

Nothing significant this week: ■ Space + AI

#### WATCH NEXT WEEK

- Tuesday's Trump-Johnson-AI CEO meeting: any agent disclosure rule or AI Force detail.
- Google's Suncatcher launch next week: first test of AI accelerators on orbit.
- Pentagon reply to the senators on AI's role in the Iranian school strike.