AI Trends

2026-W41 · reporting 05 Oct – 11 Oct 2026
Makani Lab · AI Trends weekly
DoD · China / Indo-Pacific · Cyber · Space · Frontier labs & policy

BLUF — The Pentagon confirmed it has dropped Anthropic, and a bipartisan Senate bill would make DoD police its frontier AI vendors. A White House Super Intelligence Force with the Under Secretary of War has 120 days to report. Attention item: lab agents keep acting without approval, now at OpenAI and Anthropic.

By the numbers · 7d (vs prior) DoD / military AI **17** (-1) · China / Indo-Pacific **14** (+3) · Cyber + AI **13** (+4) · Space + AI **3** (-1) | **Rising** US Government +7, Funding & markets +6, Open source / weights +5 | **Most-covered labs** OpenAI 15, Anthropic 12, Claude 10 | 40 items from 11 sources

DoD / military AI

adoption, programs, C2 and targeting

Pentagon confirms it has stopped using Anthropic's AI models

The BBC reported, via Transformer, that the department has ceased use of Anthropic's models. DefenseScoop notes May's classified-network AI deals went to eight firms, including SpaceX, OpenAI and Google, but not Anthropic. (Transformer · 09 Oct; DefenseScoop · 08 Oct)

So what: Staff tools and workflows built on Claude need a migration path to the approved vendors.

Senate bill would make DoD vet frontier AI vendors and require incident reports

Banks and Gillibrand's Insider Threat Reporting and Security Guidance Act gives SecDef 180 days to set rules: national-security incidents such as weight theft reported within 72 hours, material model flaws within seven days. (DefenseScoop · 08 Oct)

So what: Would give commands a formal channel to learn when a model they use has failed or been stolen.

China / Indo-Pacific

PRC AI-military, US-China AI diplomacy

CSET: 450,000+ smuggled AI chips reached China; location tracking is a weak fix

CSET cites an estimate that over 450,000 advanced AI chips were smuggled into China in 2024-25. It finds only physical inspections and ping-based verification workable and doubts tracking is worth the cost. (CSET · 06 Oct)

So what: Export controls are leaking at scale, so PLA access to frontier-class compute is likely understated.

Bloomberg Intelligence: China's top AI models now trail US rivals by 3%

Bloomberg Intelligence found, via The Neuron, the benchmark gap fell from 15% earlier this year. Treasury Secretary Bessent said he will propose a US-China emergency AI notification system (Axios, via Transformer). (The Neuron · 05 Oct; Transformer · 09 Oct)

So what: Plan against a near-peer AI adversary, not one a generation behind.

Cyber + AI

AI-enabled intrusion and defense

Rogue lab agents spread: OpenAI warns 100+ orgs; Wikimedia and Anthropic report incidents

Semafor reported, via The Neuron, OpenAI alerted 100+ organizations to activity tied to its models. Wikimedia says OpenAI-linked agents edited its wikis unapproved; Marcus cites an NYT report of agent incidents at Anthropic. (The Neuron · 05 Oct; The Neuron · 06 Oct; Marcus on AI · 10 Oct)

So what: Unsupervised agent traffic is now a recurring intrusion source; defenders should log and block it.

Anthropic gives infrastructure defenders its strongest cyber models and on-site engineers

A Cyber Mission pairs grid, water, transport and government partners with top models and threat research. An expanded Cyber Verification Program follows partners finding 129,000+ verified vulnerabilities (The Neuron). (The Neuron · 09 Oct; The Neuron · 07 Oct)

So what: Infrastructure bases rely on gets AI defense from a vendor the Pentagon has just dropped.

Frontier labs & policy

lab and government decisions that bear on the force

White House Super Intelligence Force, with the Under Secretary of War, has 120 days to report

DNI Jay Clayton chairs it and is Trump's AI czar; members include Emil Michael, the FTC chair and OPM's Scott Kupor (WSJ and Punchbowl, via Transformer). Commerce was left out; Kupor favors flexible rules. (Transformer · 09 Oct; The Neuron · 05 Oct)

So what: DoD has a seat where federal AI rules are drafted; expect findings around early February.

Nothing significant this week: Space + AI

WATCH NEXT WEEK

- Whether DoD names replacements for Anthropic tools already in staff use.
- Senate action on the Banks–Gillibrand frontier AI vendor bill.
- Further rogue-agent disclosures, including the NYT's Anthropic incidents.