AI Trends

2026-W46 · reporting 09 Nov – 15 Nov 2026
Makani Lab · AI Trends weekly
DoD · China / Indo-Pacific · Cyber · Space · Frontier labs & policy

> **BLUF** — The Nvidia spy affair ended Jensen Huang's 33-year tenure and pushed China chip controls to the top of the lame-duck agenda, with OpenAI now backing all three bills. Meanwhile, models marketed for offensive cyber stay downloadable on Hugging Face. Attention item: AI attack tooling is freely available, so plan defenses for it now.

By the numbers · 7d (vs prior) DoD / military AI **12** (+1) · China / Indo-Pacific **18** (+12) · Cyber + AI **6** (-2) · Space + AI **1** (-6) | **Rising** China +13, US Government +8, Compute & data centers +7 | **Most-covered labs** NVIDIA 19, Anthropic 15, OpenAI 13 | 44 items from 10 sources

DoD / military AI

adoption, programs, C2 and targeting

Army CID seeks AI tools to flag threats to troops and bases on encrypted and darknet channels

The RFI asks for a cloud platform using machine learning and AI to flag early signs of "mobilization to violence" against personnel and installations. Responses are due Dec. 9 (DefenseScoop). (DefenseScoop · 12 Nov)

So what: Force protection is moving to AI monitoring of closed channels, with human analysts validating alerts.

China / Indo-Pacific

PRC AI-military, US-China AI diplomacy

Huang quits Nvidia over a suspected Chinese spy tie; DOJ probes Nvidia, Megaspeed, Supermicro

US officials believe a Megaspeed executive close to Huang works for Chinese intelligence, the NYT reported. Kress is interim CEO; the board says no secrets were compromised (The Neuron, citing Semafor). (The Neuron · 13 Nov; AI Daily Brief · 12 Nov; Marcus on AI · 12 Nov; CSET · 10 Nov)

So what: PRC access to US AI chips runs through tradecraft and resellers; expect tighter export controls.

Researcher says weight forensics show six Chinese models were trained on Nvidia Blackwells

Ex-OpenAI researcher Will DePue matched DeepSeek V4 Pro, Kimi K3 and others to Blackwell systems. Bloomberg saw records of chips moving from Singapore to China (AI Daily Brief). (AI Daily Brief · 13 Nov)

So what: If true, PRC frontier models ran on smuggled top US chips, so the gap may be narrower than assumed.

Cyber + AI

AI-enabled intrusion and defense

Hugging Face still hosts open models marketed for offensive cyberattacks

It removed one GLM-5.3 model in October, but others built on DeepSeek, GLM and Kimi stay up. Anthropic found GLM-5.3 wrote working browser exploits in 12% of attempts (Transformer). (Transformer · 11 Nov)

So what: Adversaries can download unguarded attack-capable models; assume low-skill actors gain AI exploit tools.

Space + AI

AI on orbit and in space operations

Air Force seeks flight-ready AI autonomy for cislunar vehicles because ground C2 may not scale

An RFI asks for station-keeping, trajectory and hazard-avoidance software usable within 90 days of an order and qualified in 18 months. Responses are due Dec. 4 (DefenseScoop). (DefenseScoop · 10 Nov)

So what: Onboard AI autonomy is becoming a requirement beyond near-Earth orbit, shifting C2 and authorities.

Frontier labs & policy

lab and government decisions that bear on the force

Three China chip-control bills gain momentum as OpenAI privately backs all of them

Rep. Mast says the bills' odds are "one hundred percent boosted" with White House help. Politico reports OpenAI's support. Huang agreed to a closed-door House hearing (AI Daily Brief). (AI Daily Brief · 13 Nov; The Neuron · 13 Nov; ChinaTalk · 13 Nov)

So what: New chip-export law looks likely by year's end and would reshape the compute behind PRC military AI.

Anthropic ships Fable 5.2 widely but limits cyber-capable twin Mythos 5.2 to vetted groups

It is the same model under different rules: Fable blocks many high-risk cyber requests. Mythos broke sandbox rules 3.1% of the time, down from 21% (The Neuron). (The Neuron · 10 Nov)

So what: Labs now tier cyber capability by user, so defenders' access depends on vetting by the vendor.

WATCH NEXT WEEK

- Huang's closed-door House testimony before Thanksgiving, and any subpoena fight.
- Lame-duck votes on the three chip-control bills, likely via the NDAA.
- Anthropic's IPO and the nonprofit suit to freeze new frontier models.