




Neurasec Newsletter – 13th February 2026

This week felt like a reminder that AI isn't just "cool models" anymore — it's becoming infrastructure (policy, chips, power, security... the lot).

A few things that stood out:


 Global governance is getting more formal The UN General Assembly approved a 40-member scientific panel focused on AI impacts and risks — and it passed over US objections. That's a meaningful signal: more countries want a shared, science-led baseline for understanding AI's societal and economic impact.

 AI is now an energy + water + grid conversation In the US, the administration is reportedly pushing a voluntary "AI data centre compact" — basically: build the compute, but don't dump costs onto households or strain local water and power infrastructure. This is the "AI boom" meeting real-world constraints.

 Big "deep thinking" upgrades aimed at science + engineering Google announced a major upgrade to Gemini 3 Deep Think, positioning it for messier, real-world research and engineering problems (not just neat Q&A). Availability is tied to Gemini app access (AI Ultra) and early access via the API for interested orgs.

 Security is pivoting hard to "agentic AI" protection Two big signals here:

- Cisco rolled out major updates to Cisco AI Defense, leaning into *AI supply chain governance* and *runtime protections* for agent/tool use.
- Proofpoint announced it's acquiring Acuvity to extend AI security and governance across the "agentic workspace".

 The money is still pouring in (and politics is following it) Anthropic reportedly raised \$30bn, taking its valuation to \$380bn, and also pledged \$20m to support political efforts backing AI oversight. (Whatever your view on regulation, this shows how "political" AI has become.)

 Chips + toolchains remain the strategic choke point

- US lawmakers urged tighter controls on China's access to advanced chipmaking tools (and even maintenance support), framing it as a national security issue.
- Meanwhile, Applied Materials' upbeat forecast was explicitly tied to AI-driven demand and memory/packaging dynamics — another reminder that the "model race" is also a *manufacturing + supply chain race*.

UK note: The UK's Minister for AI and Online Safety published a Founders Forum speech this week — useful for the "UK direction of travel" narrative.

This week's key reads (9–13 Feb 2026):

<http://www.apnews.com/article/un-us-artificial-intelligence-scientific-panel-8936f242689792be7a7ab97e841cade8>

<http://www.reuters.com/business/us-wants-firms-commit-new-ai-data-center-compact-politico-reports-2026-02-09>

<http://www.reuters.com/technology/anthropic-valued-380-billion-latest-funding-round-2026-02-12>

<http://www.reuters.com/world/us/us-lawmakers-push-curb-chinas-access-chipmaking-tools-2026-02-11>

<http://www.reuters.com/business/applied-materials-forecasts-second-quarter-sales-above-estimates-2026-02-12>

My takeaway: AI is moving from *feature* → *platform* → *infrastructure*. And that means the winners won't just have the best models — they'll have the best governance, security, compute strategy, and supply chain resilience.

#AI #GenAI #AIGovernance #CyberSecurity #DataCentres #Semiconductors #DigitalTransformation