'It is a Riddle, Wrapped in a Mystery, inside an Enigma': The Geopolitics behind the Regulation of Frontier AI

Ravi Nayyar

13 July 2026

In June, I analysed an open letter from Australia's corporate and financial markets regulator, the Australian Securities and Investments Commission ('ASIC'). ASIC urged first principles cyber risk management in the age of frontier artificial intelligence ('AI') systems. A few weeks later, cyber security agencies from the Five Eyes countries (Australia, New Zealand, Canada, the UK and US) signed a joint statement on cyber risks from frontier AI, also advocating for first principles.

While such measured advice is welcome, organisations cannot merely adopt basic cyber risk management to tackle operational risks involving frontier AI.

These systems are dual-use technologies with significant implications for international and national security. The development and accessibility of these systems are subject to intense competition between governments looking to further their strategic interests. Organisations' AI procurement decisions occur in this fractious context.

The protracted period during which most directors and senior executives built their careers is long gone. The relative simplicity of business management has faded. Churchill's quote from October 1939 regarding Russia, borrowed in the title of this commentary, is an apt descriptor for the present challenges of regulating frontier AI.

As deployment of these systems continues apace, business leaders must track the geopolitics behind the regulation of their development and distribution more than the actual regulatory frameworks themselves.

The Allegory of Mythos and Fable

A case in point is the Trump Administration's rapidly evolving regulation of access to the Mythos 5 and Fable 5 large language models (LLMs) developed by the American vendor, Anthropic.

Merely a few weeks after issuing an executive order which expressly disclaimed 'mandatory governmental licensing, preclearance [sic], or permitting requirement[s]', Washington subjected Mythos 5 and Fable 5 to export controls without consulting allies like the Five Eyes and NATO countries. Press reporting suggested that the government acted on national security grounds due to the LLMs' capabilities, Fable 5 being vulnerable to jailbreaking and Anthropic's provision of access to Mythos to a China-linked South Korean telecommunications company without the Administration's prior approval.

Anthropic subsequently disabled access to both LLMs for all customers as it could not limit access to US nationals as required by the export controls.

Businesses and governments looking to US frontier AI companies as 'trusted' vendors were caught off guard. While hosting the recent G7 Leaders' Summit, the French President condemned the export controls as 'strictly nationalist' and called for democracies to 'move forward together' under the auspices of 'a smooth government-to-government relationship'.

When asked on 19 June if he viewed Anthropic and its CEO as national security threats, President Trump said 'not now, but a week ago, maybe'. This further confused overseas stakeholders as to the American regulatory posture.

On 24 June, public reporting indicated that the US removed the export controls for Mythos because Anthropic had developed sufficient guardrails in partnership with the Trump Administration and limited the distribution of Mythos 5 to 'certain trusted partners'. Those 'partners' are apparently over 100 US companies and government agencies.

A week later, the US lifted the export controls for Fable 5 after working with Anthropic to 'analyse and approve [the LLM] … to ensure alignment across the US Government and strengthen America's leadership in AI'. Unlike Mythos 5, Fable 5 can now be distributed to all Anthropic customers.

Tangentially, one should also note reports that, despite its legal dispute with the Pentagon, Anthropic had embedded a number of engineers at the National Security Agency (NSA) to help the latter deploy Mythos. The NSA had been apparently using Mythos since April. In early July, the Cybersecurity and Infrastructure Security Agency was reported as using Mythos to scan US government code repositories for vulnerabilities.

The Anthropic case study captures the capricious regulatory landscape which non-US customers of US frontier AI vendors operate in as the Trump Administration grapples with the geopolitical importance of their offerings.

Consistently Unclear

One should note that unilateralism is hardly confined to the Trump Administration. In January 2025, the Biden Administration issued the *Framework for Artificial Intelligence Diffusion*. Highly controversial, this rule restricted the export of advanced semiconductors used in training LLMs even to NATO allies like Portugal and Austria. The Trump Administration rescinded the rule in May 2025. The Department of Commerce's Bureau of Industry and Security (BIS) also refused to enforce certain licensing requirements for advanced chip exports to Chinese companies since May 2025. Even when it issued guidance on this topic in May 2026, the BIS still failed to clarify which of the export controls it would actually enforce.

Such factors create further uncertainty for overseas stakeholders as to what the US position actually is on the regulation of the AI stack.

It is not surprising that European stakeholders, already seeking to reduce their dependencies on American technology stacks, are agitating for sovereign European AI capability. The French frontier AI vendor, Mistral, is being positioned as a European champion, and allows enterprise and government customers to build bespoke LLMs trained on their own data.

That said, the valuations and capabilities of US competitors' offerings dwarf those of Mistral. Through July 2025, the US was also estimated to control 74 per cent of AI supercomputer capacity, far greater than the EU's 4.8 per cent.

The Core Question

So, how do non-US organisations navigate AI regulation from the jurisdiction hosting the vendors that dominate frontier AI when that regulation consistently comprises executive actions, including ad hoc interventions, fashioned without proper stakeholder consultation?

Given the growing geopolitical salience of frontier AI, the US will only seek to advance its edge in this critical technology, even at the cost of its own allies and partners. Organisations headquartered outside the US must recognise that allowing the concentration of American vendors in their networks introduces serious supply chain risks and jeopardises business continuity as they increasingly integrate US LLMs into operations.

That recognition will only come from an awareness of how, in this case, the US views its regulatory tools as (albeit blunt) instruments of geoeconomic contestation. Corporate leaders should pay heed to the French President's warning about US vendors, 'from one day to the next, … just turn[ing] off the switch'.

Not as Simple as Swapping with China

Nonetheless, the solution is not as simple as replacing proprietary American LLMs with Chinese models. This would arguably replace one set of concentration and foreign influence risks with another, with Chinese models trained to comply with Chinese law (including with respect to topics sensitive to Beijing) and most likely sending data back to Chinese servers. Beijing was also reported in early July to have held talks with major Chinese vendors including Alibaba, ByteDance and Z.ai about restricting overseas entities' access to the country's most advanced LLMs and strengthening screening of foreign investment in local AI startups.

With Chinese techno-nationalism echoing that of the US, organisations considering procurement of Chinese AI solutions face a similar set of 'known and unknown unknowns' in terms of regulatory risk. This is inherent to the geopolitical contestation driving national regulatory frameworks for the development and distribution of frontier AI.

That said, many organisations are prioritising economics, rather than geopolitics and turning to Chinese alternatives. These are cheaper (backed by generous state subsidies and alleged distillation of US models) and closing the performance gap with those of US vendors.

Open Source Risks

Additionally, organisations need to be careful when considering open source LLMs, both for tasks not as complex as those requiring frontier models and as alternatives to proprietary solutions that can be 'switched off' by US or Chinese regulatory action.

The most attractive open source solutions are Chinese, carrying similar sorts of supply chain risks as proprietary Chinese LLMs.

At a systemic level, if more organisations route tasks to Chinese open source models, the latter will process a significant volume of compute powering commerce and public services, becoming the 'default layer' which other LLMs trust and AI users build upon. Even if enterprises avoid proprietary LLMs, they risk contributing to potential Chinese dominance in the global digital economy and accompanying FOCI risks overshadowing their own operations.

Even the Trump Administration's AI action plan from July 2025 recognised that open source LLMs could be entrenched as global standards via network effects. It was arguably to further *its own strategic interests* that the US committed to 'create a supportive environment for open models'.

That even *open source* models are already the subject of geopolitical contestation underlines the importance of corporate leaders being alive to how that contestation shapes the regulation of the AI systems they procure.

'You May not Be Interested in Geopolitics …'

This commentary started with calls from government for industry to perform first principles cyber risk management in the age of frontier AI.

It will close with another call from government: an open letter issued in June 2026 by the Australian Prudential Regulation Authority (APRA) on management of geopolitical risks.

APRA specifically flagged that: 'Reliance on critical third parties [AI vendors], often located overseas, … makes it more difficult to assess, mitigate and manage these risks'.

The regulation of frontier AI by jurisdictions like the US and China will continue to be shaped by growing geopolitical contestation. Hence, corporate leaders cannot treat AI procurement as a typical technology supply chain risk management issue. They must approach it through a geopolitical lens.