

The Export That Never Leaves

America's export controls were built to stop chips at the border. Chinese AI has learned to connect instead - and Washington's response will remake economic statecraft itself.



By Andrew Horton

In rented server racks across Johor, Bangkok and Jakarta, Nvidia's most advanced processors are training Chinese artificial intelligence tonight - legally, profitably and beyond the reach of any customs officer on Earth. The silicon remains where it was manufactured. The capability flows across networks. What looks like a routine cloud transaction has become one of the most serious strategic vulnerabilities confronting the Western alliance.

This month the Bureau of Industry and Security (BIS), the enforcement arm of Washington's export control regime, began a [systematic review](#) of how Chinese technology firms gain access to advanced Nvidia processors hosted in third countries through cloud infrastructure and remote rental arrangements. The investigation reflects a recognition that the strategic battleground has shifted. The issue is no longer the movement of chips. It is the movement of access.

The catalyst was a stark demonstration of Chinese capability. In July, Beijing-based Moonshot AI released Kimi K3, a model that performed within

striking distance of leading American systems, and White House officials publicly alleged that Moonshot had accessed Nvidia's advanced hardware [through infrastructure located in Thailand](#). Whether or not every allegation proves accurate, the strategic lesson remains the same. Four years of export controls focused heavily on physical shipments, transshipment networks and hardware diversion. Artificial intelligence has now exposed the limits of a framework built around physical borders.

For two decades, Western legal doctrine operated on the [assumption that providing cloud computing services to a foreign customer did not constitute an export](#). That assumption held when cloud platforms stored payroll systems, enterprise software and databases. The emergence of frontier artificial intelligence transformed compute into a strategic resource. A microchip remains a physical object subject to inspection and interdiction. A remote AI training run is a permissioned connection that can traverse continents without attracting the attention of customs authorities.

Recognising this vulnerability, the US House of Representatives passed the Remote Access Security Act in January by [369 votes to 22](#), and a [bipartisan companion bill](#) is now advancing through the Senate. The objective is straightforward: bring remote access to export-controlled technologies within the scope of American export control law. If Washington can restrict the physical export of strategic technology, it increasingly believes it must also govern remote access to that same technology.

The scale of the challenge is visible across Southeast Asia, where Chinese demand for high-performance computing has become a [powerful driver of the region's data-centre construction boom](#). Advanced AI development now depends less on ownership of hardware than on access to processing power; the strategic value resides in the connection. Investigations have meanwhile revealed [increasingly sophisticated corporate arrangements](#) involving cloud providers, intermediary entities and offshore structures designed to obtain advanced processing capability while remaining beyond the reach of existing regulatory frameworks. These arrangements exploit a simple reality: modern export control architecture was designed for hardware moving between jurisdictions, not compute flowing across networks.

The question confronting Washington is therefore no longer whether China can manufacture the world's most advanced processors. The question is whether China can achieve frontier artificial intelligence capability while never possessing a single restricted chip. If the answer is yes, traditional export control theory has already been overtaken by technological reality.

The Western alliance has encountered this strategic challenge before. After September 2001, Washington discovered that power within the global financial system did not come from controlling banknotes. It came from controlling access to the networks through which global finance flowed. The US Treasury

transformed correspondent banking, dollar clearing and financial compliance into instruments of statecraft. When BNP Paribas processed transactions involving sanctioned jurisdictions, the United States did not intercept cargo ships or seize assets at borders. It imposed a [US\\$8.9 billion penalty](#) and temporarily restricted the bank's access to the dollar-clearing system. Access itself became the source of power.

Artificial intelligence is now undergoing the same transformation. What is emerging through BIS enforcement activity, congressional legislation and evolving export control doctrine is a new principle of statecraft: compute clearing. Under this model, strategic authority flows from determining who may connect to advanced processing power rather than who owns the hardware. Compute becomes a governed network. Access becomes a privilege. Exclusion becomes a penalty.

Export controls were designed as perimeter defences. Compute clearing operates as network governance: access becomes a privilege, and exclusion becomes a penalty.

The implications are substantial. Under a mature compute-clearing regime, BIS would evolve into the technological equivalent of the Office of Foreign Assets Control. Data-centre operators would become the correspondent banks of the intelligence age, with customer onboarding held to robust verification standards: high-end compute providers would need to understand not only who rents capacity but who ultimately benefits from it. Host jurisdictions would acquire new strategic weight. Malaysia, Japan, Australia, Singapore and the Gulf states would become critical nodes in an allied AI infrastructure network, their access to frontier processors increasingly dependent on their willingness to enforce agreed security standards and compliance obligations.

Critics raise two objections. The first asserts that sophisticated ownership structures make meaningful enforcement impossible. History suggests otherwise. Financial sanctions have always experienced leakage, and their effectiveness has never depended on perfection: network power succeeds because exclusion carries greater costs than compliance. The same logic applies to advanced compute. The second argues that tighter controls will accelerate Chinese technological self-sufficiency. That risk is real. Excessive restriction can encourage alternative ecosystems, just as aggressive financial sanctions encouraged Beijing to invest in alternative payment infrastructure. Effective policy therefore requires selective discrimination rather than indiscriminate denial. The goal is strategic advantage, not strategic isolation.

For democratic nations hosting significant AI infrastructure, these developments create obligations as well as opportunities. Governments should treat high-capacity GPU infrastructure as a strategic utility subject to enhanced



licensing and bank-grade customer identification, and trusted jurisdictions should establish mutual recognition arrangements across AUKUS, the G7 and other allied frameworks, creating a compute-clearing architecture that rewards compliance.

Australia, for example, is exceptionally well placed to help shape this emerging order. Sydney-headquartered Firmus recently secured a [US\\$2 billion funding round](#) with Nvidia among its investors, to expand AI infrastructure across Australia and the wider Asia-Pacific, placing the country among the leading trusted host jurisdictions for next-generation compute. Just as Australia helped build the modern architecture of financial integrity, it now has the opportunity to co-author the rules governing trusted compute networks.

The broader significance extends far beyond semiconductors. For more than a century, economic power flowed from control of physical goods. In the decades that followed, strategic influence increasingly belonged to those who controlled global financial networks. Artificial intelligence is inaugurating a third era, in which power flows through compute networks and the states that govern access to advanced processing will shape innovation, military capability and geopolitical alignment across entire regions. The countries that write the rules of compute clearing will occupy the commanding heights of the next international order. Those that hesitate will discover that sovereign capability can erode without a single ship changing course, a single factory changing ownership or a single chip crossing a border. Naval powers commanded the era of maritime trade. Financial architects commanded the era of dollar clearing. In the age of artificial intelligence, strategic leadership will belong to the alliance that governs access to compute itself.