Hearing on *China's Campaign to Steal America's AI Edge*

Before the United States House of Representatives
Select Committee on the Chinese Communist Party

April 16, 2026

Written Statement of Dmitri Alperovitch
CoFounder and Executive Chairman of Silverado Policy Accelerator

---

Chairman Moolenaar, Ranking Member Khanna, and distinguished members of the Committee, thank you for the opportunity to testify today on how China is acquiring, through both legal and illicit channels, advanced U.S. artificial intelligence technology.

We are in a race, and the stakes could not be higher. Artificial intelligence will transform every industry, every battlefield, and every government, and whoever fields the best models running on the best infrastructure will likely win not just the AI race itself but the 21st Century. The single most important input to winning is compute — the processing power used to train and run AI models.

Let me say that plainly, because it is the finding that should anchor everything the Congress and this Committee do on AI policy: the binding constraint in this competition is not talent, it is not data, and it is not cash. Both the United States and China have talented researchers and financial resources. And we have learned frontier models trained on generic data routinely outperform smaller models trained on more specialized data.

It all comes down to compute.

At its core, compute is based on chips - how many a country has, how powerful they are, and how well they work together. The exponential scaling of that chip power is what has driven virtually every meaningful improvement in AI over the last decade. This is not a secret. And China understands it as clearly as we do.

DeepSeek's founder said it succinctly: "our problem has never been funding; it's the embargo on high-end chips." Because they cannot access the best technology, DeepSeek needs "twice the computing power to achieve the same results" as their international competitors. [1]

---

[1] Lennart Heim, "The Rise of DeepSeek: What the Headlines Miss," RAND Corporation Commentary (January 28, 2025), available at https://www.rand.org/pubs/commentary/2025/01/the-rise-of-deepseek-what-the-headlines-miss.html.

But if any doubt remains about how seriously China takes this, the lengths to which it is willing to go to acquire compute should settle the question. In the last several months, the Department of Justice has unsealed indictments involving billions of dollars in illicitly exported Nvidia chips routed through Southeast Asia. The most significant case involves the co-founder of Super Micro Computer, charged with allegedly diverting approximately $2.5 billion in AI servers to China through front companies. China is doing this because it knows that chips are the race, and it will do whatever it takes to close the gap.

The stakes of that gap could not be higher. There is a moment coming in AI development — a threshold of what is called recursive self-improvement, when AI systems begin to meaningfully accelerate their own improvement. The country that crosses that threshold first will enjoy a compounding advantage that may never be closed.

The good news is that we have a chokepoint and export controls have prevented China from closing the compute gap. But we are not fully exploiting it, and in some cases, we are actively undermining it.

To ensure the United States remains ahead and China cannot catch up, my recommendations condense into two overarching imperatives: **don't arm the enemy**, and **don't create another Strait of Hormuz**.

To ensure that we do not arm the enemy, we need to **first hold the line on export controls, close the loopholes, and ensure penalties effectively deter violations.** Providing China with cutting-edge AI chips is the modern equivalent of selling rockets to the Soviets during the space race. No one in 1962 would have seriously entertained licensing our best rocket technology, or even our second-best technology to Moscow just for business returns or for the ridiculous notion that it would get the Soviets "addicted" to our space tech stack! The strategic stakes today are just as clear. We should not be any more willing to hand China the tools it needs to beat us in this race than we were to hand them to the Soviets in that one.

There should be no licenses granted for advanced AI chips to China, period. To that end, the AI Overwatch Act offers a sound framework: mandatory congressional notification before any such export is approved, verifiable safeguards preventing military end-use, and a guarantee that chip exports do not come at the expense of domestic availability. Any persons found to have knowingly violated export controls must be held accountable to the fullest extent of the law. A more robust and effective set of civil penalties, which require less evidence and a lower standard of proof than criminal enforcement, can increase overall deterrence against violations.

Strengthening Military End-User Controls

One dimension of the export control architecture that deserves great stringency is the treatment of military end-user controls. Historically export controls have been designed for industries with relatively clear distinctions between civilian and military applications. This distinction is rapidly

collapsing in the context of AI and robotics. The industries of the future are inherently dual-use in ways that older-generation technologies were not.

This has direct implications for how we think about Chinese technology companies as end-users. Major Chinese technology firms, including Tencent, have been designated as Military End Users (MEUs) by the Department of Defense.[2] The implications of this are straightforward: providing electronics of any type to a designated PRC MEU should be prohibited, full stop. No exceptions, no licenses, no workarounds.

However, there are additional challenges due to China's legal system. Under Chinese law, any company operating in China can be compelled to cooperate with Chinese military and intelligence authorities. There is no meaningful civilian or private sector when national security interests are invoked. This reality has direct consequences for how U.S. export control law should be applied. Section 744.6 of the Export Administration Regulations prohibits persons from providing any form of "support" to prohibited end users, including nuclear weapons development, biological and chemical weapons programs, and military intelligence activities.[3] Given the compulsory cooperation requirements embedded in Chinese law, providing advanced AI chips to any Chinese company has the potential to support the prohibited end uses.

Legislation should account for the fact that exports of advanced AI chips and related technology to Chinese companies, regardless of their civilian status, carry an inherent risk of supporting prohibited military end uses and empower BIS to exercise all of its existing authorities to neutralize this risk.

Moving Beyond Criminal Enforcement: Building a Robust Civil Penalty Regime

The current export control enforcement system focuses heavily on criminal prosecution. This is appropriate for egregious violations but criminal prosecution is a slow process that requires a higher standard of proof and significant government resources. In addition, the U.S. should build a more robust and more actively deployed set of civil penalties. Under civil enforcement, the standard of proof is lower, the evidentiary requirements are less demanding, and the range of penalties is broader. A company that cannot be criminally prosecuted for an export control violation could still be hit with substantial civil fines, have its export privileges revoked, be removed from approved vendor lists and government procurement programs, and publicly named as a violator. Each of these consequences imposes real financial, reputational and operational costs.

---

[2] U.S. Department of Defense, *Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. ("Mac") Thornberry National Defense Authorization Act for Fiscal Year 2021* (Public Law 116-283) (January 7, 2025), available at https://media.defense.gov/2025/Jan/07/2003625471/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES.PDF.

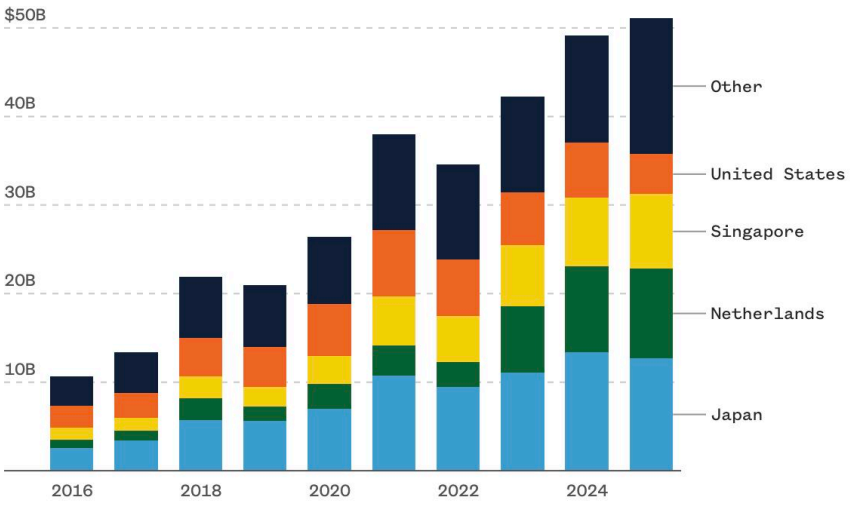
[3] 15 C.F.R. § 744.6, *Restrictions on Certain Activities of U.S. Persons*, Export Administration Regulations, Bureau of Industry and Security, U.S. Department of Commerce, available at https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744/section-744.6.

Second, **stop supplying China with the equipment to build its own chips.** Export controls on finished chips mean little if the U.S., Netherlands and Japan continue selling China the semiconductor manufacturing equipment to eventually produce them domestically. The MATCH Act is a strong step forward and I am glad to support it. But we need to extend controls to DUV lithography equipment as well, ensure we have and are willing to use diplomatic and backstopping tools like the foreign direct product rule (FDPR) to align our export controls with those of other countries supply China, and prioritize the sale of scarce equipment to domestic fabs first. No one should have been surprised at the news a few years ago that Huawei had been able to produce chips at the 7nm level using only DUV machines since TSMC had demonstrated that very capability in 2019. It was inevitable that China would eventually figure it out.

China imported a record $51.1 billion of semiconductor manufacturing equipment during 2025 from a diversifying set of countries. That total follows years of consistent import growth since imports totaled just $10.7 billion in 2016. China has stated its intent to indigenize its semiconductor industry in the coming years and siphoning technology and knowledge to produce the most advanced chips through obtaining manufacturing equipment is critical to that objective. U.S. export controls alone are not sufficient given the U.S. share of China's imports have fallen from 23 percent in 2016 to 9 percent in 2025. We need to incentivize our partners to take complementary actions to prevent China from its domestic and global semiconductor market share targets.

China's chip-making equipment imports

The country imported more than $50 billion in semiconductor manufacturing equipment last year, much of it from Japan and the Netherlands.



Source: Silverado Policy Accelerator analysis of Global Trade Tracker data.
Graphic: Joe Murphy / NBC News

Third, **invest in verification and enforcement to counter smuggling.** Export controls govern legal trade. They do not stop smugglers. The surge of recent Department of Justice enforcement actions related to smuggling show its threat.

The scale of the problem is best understood through the recent case record. In the last several months alone, the DOJ has unsealed a series of indictments that together paint a picture of a systemic, well-resourced effort to divert advanced American AI technology to China.

In November 2025, the DOJ charged four individuals with conspiracy to illegally export advanced Nvidia GPUs to China through a Florida-based front company. The individuals are accused of shipping 400 Nvidia A100 GPUs to Chinese end-users, routed through Malaysia and Thailand. The defendants received nearly $4 million in wire transfers from the PRC to fund the operation.[4]

In December 2025, the DOJ publicly announced "Operation Gatekeeper," an investigation that dismantled a China-linked smuggling network operating across the U.S., Singapore, Malaysia, and Hong Kong. A Texas-based businessman and his company exported or attempted to export at least $160 million worth of Nvidia H100 and H200 Tensor Core GPUs to China. The businessman and company received more than $50 million in wire transfers from China to fund the illegal scheme. In separate arrests, two other individuals were charged with conspiring to circumvent U.S. export controls.[5]

In January 2026 a former Google software engineer was convicted on seven counts of economic espionage and seven counts of theft of trade secrets for stealing more than 2,000 pages of confidential information related to Google's custom Tensor Processing Unit chips, GPU systems documentation, and SmartNIC network interface card designs.[6]

In March 2026, the highest-profile case to date: an indictment was unsealed in Manhattan federal court charging Yih-Shyan "Wally" Liaw, co-founder of Super Micro Computer, along with Supermicro's Taiwan general manager Ruei-Tsang "Steven" Chang and a third-party fixer, with allegedly working to divert billions of dollars in Supermicro AI servers to China in violation of

[4] Department of Justice, "U.S. Citizens and Chinese Nationals Arrested for Exporting Artificial Intelligence Technology" (November 2025), available at https://www.justice.gov/opa/pr/us-citizens-and-chinese-nationals-arrested-exporting-artificial-intelligence-technology.

[5] Department of Justice, "U.S. Authorities Shut Down Major China-Linked AI Tech Smuggling Network" (December 2025), available at https://www.justice.gov/opa/pr/us-authorities-shut-down-major-china-linked-ai-tech-smuggling-network.

[6] Department of Justice, "Former Google Engineer Found Guilty of Economic Espionage and Theft of Confidential AI Technology" (January 2026), available at https://www.justice.gov/opa/pr/former-google-engineer-found-guilty-economic-espionage-and-theft-confidential-ai-technology.

U.S. export controls. The alleged operation yielded approximately $2.5 billion in sales since 2024. Servers were shipped to a Southeast Asian front company before going on to China.[7]

The common thread across many of these cases is the use of Southeast Asian intermediaries for transhipment to Chinese end-users. The transhipment route is not a recent discovery as it has been documented and flagged by analysts and the Commerce Department. However, it continues to operate because of failures in enforcement.

Closing the illicit channel requires a dedicated enforcement infrastructure and the most promising near-term tool is chip geolocation technology as contemplated in the Chip Security Act, advanced by the House Foreign Affairs Committee. The language in the bill is not an enforcement mechanism on its own. It is not a kill switch and it does not prevent chips from functioning in certain locations. Instead, it is an investigative tool - it is designed to expose more data to chip exporters and potentially to the Bureau of Industry and Security (BIS) where chips are being used after sale, in order to enhance investigators of transshipment violators. Notably, I have proposed one technical solution for chip location verification that can be easily implemented by AI chip designers, which is not onerous and will not require GPS receivers or communications functionality inside the chip.[8]

Fourth, **strengthen protection against AI model distillation attacks that enable theft from leading U.S. AI frontier models.** AI model distillation attacks pursued by Chinese actors seeking to steal the outputs from U.S. frontier models requires strengthened oversight and action. At a minimum, Congress should prioritize enforcement such as by instructing the Federal Bureau of Investigation (FBI) to coordinate with leading U.S. frontier AI companies and hyperscalers to identify, prosecute and disable attempts to fund creation of bot accounts that send in millions of queries to U.S. AI models.

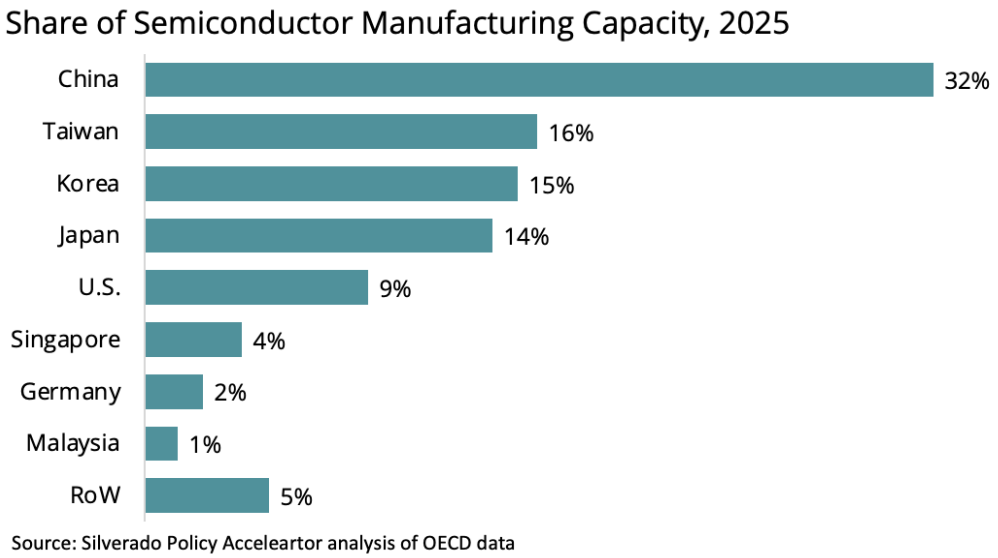
Fifth, establish Know Your Customer (KYC) rules for cloud customers to ensure that Chinese companies cannot train using chips outside of China. Recent plans by Chinese company ByteDance to assemble computing power in Malaysia using the Nvidia Blackwell system and Singapore's Aolani Cloud to meet growing global demand for AI from its customer base highlights the need for cloud providers to have greater visibility into their customers.

Finally, **we need to ensure that we do not create a semiconductor Strait of Hormuz.** A chokepoint where a strategic adversary can disrupt global supply and constrain U.S. policy choices. The United States must address a longer-term strategic risk: China's drive to dominate foundational or so-called "legacy" chip markets. While the United States and allies lead on

[7] Department of Justice, "Three Charged with Conspiring to Unlawfully Divert Cutting-Edge U.S. Artificial Intelligence Technology" (March 19, 2026), available at https://www.justice.gov/opa/pr/three-charged-conspiring-unlawfully-divert-cutting-edge-us-artificial-intelligence.
[8] Dmitri Alperovitch, "Chip Security Act: How Geolocation Can Enhance U.S. Export Control Enforcement," X (formerly Twitter), July 16, 2025, available at https://x.com/DAlperovitch.

advanced chips, China is pursuing foundational chip dominance through the same state-backed non-market policies it has deployed in steel, solar, and electric vehicles.

China's ambitious, publicly stated targets are to capture 80 percent of domestic market share and 56 percent of the global semiconductor market by 2030. Even if mainland production expansion only approaches those targets, China will still have gained important market power that it can exploit to coercive ends. Manufacturing capacity expansion is increasing to produce at scales to meet its targets and China already has the largest manufacturing capacity in the world, exceeding that of even Taiwan and Korea.



Ceding that market would undermine U.S. military readiness, concentrate critical supply chains in the hands of an adversary, and most consequentially, give Beijing the leverage to retaliate against the very export controls on advanced chips that this testimony recommends. That is the definition of a national security threat, and the Administration or Congress should respond with component tariffs that follow Chinese chips into downstream products and an early-warning monitoring regime for foundational chip overcapacity.

Following these recommendations can ensure the United States keeps its lead in the most consequential technological race of our time. A race defined by compute, and one where the United States still holds a critical advantage, but one that can be easily squandered away.

Thank you very much for the opportunity to present my views today.