

CORD

Buy What It Can, Steal What It Must: China's Campaign to Acquire Frontier AI Capabilities

Item Type	House Staff Report
Download date	2026-06-10 21:24:37
Link to Item	https://hdl.handle.net/20.500.14300/3632

THE SELECT COMMITTEE ON THE
STRATEGIC COMPETITION BETWEEN
THE UNITED STATES AND
THE CHINESE COMMUNIST PARTY

BUY WHAT IT CAN,
STEAL WHAT IT MUST

China's Campaign to Acquire
Frontier AI Capabilities



Executive Summary

The United States and its allies still control the key chokepoints that will determine whether the Chinese Communist Party (CCP) can achieve durable leadership in artificial intelligence (AI). Beijing has some of the best AI engineering talent in the world, but it still cannot manufacture frontier AI chips at the scale, yield, or sophistication its ambitions require. China's weaknesses in chip manufacturing equipment result in weaker chips, dependence on foreign cloud compute, and lagging model capabilities. Yet the United States has not fully leveraged this dependency due to gaps in both policy and enforcement.

The House Select Committee on the Strategic Competition between the United States and the Chinese Communist Party (Committee) examined how Chinese actors continue to acquire the tools, chips, and models needed to accelerate China's AI buildup, through both licit and illicit channels. The Committee found:

- China remains the largest market for chipmaking equipment despite restrictions.
- China lawfully procures large volumes of advanced AI chips.
- China bypasses AI chip export controls through the cloud.
- Post-sale servicing and verification gaps allow Chinese fabs to maintain restricted tools.
- Chinese firms evade foundry due diligence through shell companies.
- China utilizes sophisticated smuggling networks to acquire restricted AI chips.
- China extracts frontier capabilities from American AI developers through industrial-scale fraud.
- Weak enforcement and limited penalties fail to deter violations.

To address these findings, the Committee recommends a two-track response. First, Congress should pass the AI OVERWATCH Act, the SCALE Act, and the Remote Access Security Act to close loopholes that still allow Chinese firms to lawfully access advanced American chips and cloud compute. Second, Congress should pass the MATCH Act, the Chip Security Act, and the STOP Shells Act to stop tool diversion. In addition, Congress should direct the Commerce Department's Bureau of Industry and Security (BIS) and the Department of Justice (DOJ) to close foundry loopholes, treat model extraction as industrial espionage, and impose penalties severe enough to deter Beijing's theft of American innovation.

Introduction

Artificial intelligence (AI) sits at the center of U.S.-China competition, and both governments treat leadership in AI as a national security priority. But AI is not a single technology; rather it is a technology stack in which each layer depends on the one beneath it.¹ Semiconductor manufacturing equipment produces advanced AI chips; those chips support the machine-learning frameworks used to build, train, and run AI models; and those models power the applications people actually use.

Beijing wants control of the full AI stack, not just competitive applications. Xi Jinping reiterated that goal at an April 2025 Politburo study session on AI, calling for China to master core AI technologies and build a hardware and software system that China completely controls.² China first set that direction in its 2015 “Made in China 2025” directive and its 2017 national AI strategy; Beijing has reaffirmed it in both the 14th and 15th Five-Year Plans.³ Beijing is pursuing that autonomy to strengthen its military, harden itself against foreign pressure, and keep the technologies underpinning future economic and military power under Party-state control.

At the base of the AI stack is the equipment needed to make advanced chips. China still depends heavily on the United States and its allies for lithography, etch, deposition, inspection, and other equipment. The Committee’s October 2025 investigation, *Selling the Forges of the Future*, found that China spent \$38 billion in 2024 on products and services from major foreign technology companies such as Applied Materials, ASML, KLA, Lam Research, and Tokyo Electron.⁴ It also found that five Chinese companies already subject to U.S. restrictions ranked among those companies’ top customers between 2022 and 2024.⁵

Beijing is trying to narrow that dependence by moving locally produced tools onto more advanced domestic production lines.⁶ Those tools include etching, deposition, and cleaning equipment from Chinese firms such as Naura and AMEC, as well as from firms with substantial China-based operations, such as ACM Research.⁷ Even so, Chinese suppliers still lag foreign leaders across most of the equipment categories required for frontier chipmaking.

That gap is clearest in two chips essential to advanced AI processors: advanced logic chips, which perform the core calculations, and high-

bandwidth memory (HBM) chips, which must be stacked and packaged alongside them to store and move data at speed. China’s leading chip manufacturer, Semiconductor Manufacturing International Corporation (SMIC), has yet to produce advanced logic chips at production volume.⁸ Its primary memory maker, ChangXin Memory Technologies (CXMT), has likewise not reached mass production of HBM, leaving China with virtually no domestic supply.⁹

Chinese chip designers also remain dependent on Western electronic design automation (EDA) software—especially from Synopsys, Cadence, and Siemens EDA—even as Beijing backs domestic alternatives such as Empyrean and Primarius.¹⁰

As a result, the AI processors that Chinese chip designers such as Huawei, Cambricon, and Biren can bring to market still lag Nvidia’s top-end products. Huawei’s leading domestic AI chip, the Ascend 910C, is generally viewed as comparable to Nvidia’s older H100 rather than its current frontier accelerators, and U.S. officials estimate Huawei can produce no more than about 200,000 advanced AI chips in 2025—a fraction of U.S. output.¹¹

China’s weaknesses at the chip layer propagate into the AI software layer. Most domestic firms remain tethered to Nvidia’s CUDA, while local alternatives are fragmented across a dozen chipmakers with incompatible software stacks.¹² To survive this, Beijing is forcing a “coordinated development” between hardware and software, while firms stitch together compute from a patchwork of domestic and foreign chips.¹³

Those constraints, however, have not stopped China’s progress at the model layer; they have shaped it. Rather than replicating the massive, hardware-intensive systems of U.S. firms like OpenAI and Google, Chinese companies such as DeepSeek, MiniMax, and Moonshot have prioritized lightweight, compute-efficient models.¹⁴ Yet, as the Committee’s April 2025 investigation, *DeepSeek Unmasked*, revealed, even these smaller models have benefited from extracting capabilities from U.S. models and training on restricted Nvidia chips.¹⁵

This report finds that China’s AI progress still depends on Western supply. Without imported chipmaking equipment, access to restricted U.S. chips through third-country cloud services, imported HBM, and

model capabilities stolen from American AI labs, China could not field a competitive AI industry.

Part II. What China Can Buy

There is a common misperception that U.S. export controls on chipmaking equipment, AI chips, and AI itself are broad in scope. They are not. Many known chokepoint tools are only restricted for a subset of Chinese chipmakers, and can otherwise be shipped to anywhere else in China. Controls on AI chips capture only the most advanced data center chips, excluding even the leading-edge AI chips currently powering China's rapid progress in robotics. And restrictions on accessing such chips through the cloud are non-existent. The United States and its allies must urgently close these gaps.

Finding 1: China remains the largest market for chipmaking equipment despite restrictions.

U.S. and allied export controls on chipmaking equipment worked where policymakers applied them early and broadly. In 2019, the first Trump administration worked with the Dutch government to keep Extreme Ultraviolet (EUV) lithography systems—the most advanced machines for printing the tiny features of leading-edge chips— out of Chinese hands.¹⁶ That policy has held, and today Beijing remains unable to produce 5 nanometer chips at scale. Countrywide controls can successfully frustrate China's ability to indigenize key technologies.¹⁷

However, as the Committee's bipartisan report, *Selling the Forges of the Future*, documents, the Biden administration's subsequent "small yard, high fence" strategy did not extend that successful approach across the rest of the chipmaking toolchain.¹⁸ The administration did not apply countrywide controls to less advanced chokepoint technologies like Deep Ultraviolet (DUV) immersion lithography equipment, or other equipment that China is unable to produce indigenously.¹⁹ That decision left most chipmaking facilities in China free to buy the equipment they needed to work around U.S. restrictions.

Beijing quickly translated that opening into a buying spree. Chinese chipmakers snapped up massive quantities of these unrestricted "legacy" tools. China's share of ASML's DUV sales exploded from 26 percent in 2022 to 70 percent in 2024. At the same time, the country's total spending on foreign chipmaking equipment surged to \$38 billion in 2024 alone.²⁰ For four consecutive years, China has remained the world's largest

market for these tools, stockpiling more chipmaking equipment than South Korea, Taiwan, and the United States.²¹ As long as China remains the largest market for these tools, foreign suppliers will keep facing strong commercial pressure to resist tighter controls.

Recommendation 1: Close the gap in equipment controls.

Western dominance in chipmaking equipment and components gives the U.S. and its partners powerful leverage over China's AI ambitions. The task now is to close the remaining gaps in controls, imposing countrywide controls on chokepoint tools and components and aligning restrictions with allies.

Congress should:

- Pass the MATCH Act (H.R. 8170), which would require the State Department and the Commerce Department to first seek aligned restrictions with U.S. allies and then close any remaining gaps on their own through foreign direct product rules, minimum U.S.-content thresholds, or end-use controls.

Finding 2: China lawfully procures large volumes of advanced AI chips.

U.S. export controls block China from buying Nvidia's most advanced AI chips, such as the newer Blackwell chips which power the world's leading AI systems.²² However, current policy still leaves Beijing two lawful paths to acquire advanced AI compute: near-threshold chips such as Nvidia's L20 and L2, and case-by-case licensed previous-generation chips such as the H200.

So far, sales of the L20 and L2 have been relatively limited, but the H200 could become a major new source of compute for China over the coming months. In January 2026, the Bureau of Industry and Security (BIS) replaced the prior presumption of denial with a case-by-case licensing regime for H200 exports to China, subject to volume caps, supply and foundry-capacity certifications, customer-screening and remote-access controls, and independent third-party testing in the United States.²³ Beijing subsequently approved H200 purchases by Alibaba, Tencent, and ByteDance, with reports indicating that more than 400,000

chips could reach China's leading AI firms.²⁴ Chinese cloud providers have also reportedly placed orders for hundreds of thousands more.²⁵

Beijing has been open about what these imports are for. "The purpose of importing is to catch up better," said Wei Shaojun, vice chairman of the China Semiconductor Industry Association, "and catching up will eventually lead to running alongside or even taking the lead."²⁶ China is already steering its low-end compute toward domestic chips while using newly licensed H200s to keep its frontier models competitive. Nobody disputes that Beijing intends to build its own advanced chips; the question is whether U.S. export policy should be bridging the gap until it can.

These sales also come at the direct expense of U.S. AI capacity. The components and factory capacity needed to build these chips are already stretched thin. TSMC's advanced packaging lines remain heavily bottlenecked, and all three major HBM suppliers have warned that 2026 demand exceeds available supply.²⁷ Because these resources are finite, chips sent to China consume the exact same scarce inputs that would otherwise support American AI deployment. Recent procurement struggles show the strain: Google, Amazon, Microsoft, and Meta were reportedly pressing Micron to deliver as much memory as it could supply, regardless of price.²⁸ In a supply-constrained market, every H200 shipped to China both eases pressure on Beijing's compute shortfall and takes scarce packaging and memory away from U.S. and allied deployment.

Recommendation 2: Pass the AI OVERWATCH Act and the SCALE Act.

The United States should not rely on a static permitted-versus-prohibited framework for AI chip exports. That approach allows China to systematically offset its domestic hardware failures with foreign computing power, leaving too much room for near-threshold workarounds, licensed stop-gap sales that strengthen Chinese firms, and large-volume transfers that consume globally scarce chipmaking inputs.

Congress should:

- Pass the AI OVERWATCH Act (H.R. 6875) to require export licenses for advanced AI chips destined for countries of concern,

replacing the current permitted or prohibited binary with affirmative government oversight of the most consequential transactions.

- Pass the SCALE Act to set export limits dynamically based on China’s indigenous production capacity, preventing Beijing from importing advanced U.S. AI chips when it has no at-scale indigenous alternative.

Finding 3: China bypasses AI chip export controls through the cloud.

Current export controls restrict the direct sale of advanced chips to China, but they do not prevent Chinese firms from accessing those same chips remotely through offshore data centers in Malaysia or Singapore.²⁹ The same loophole exists at the model layer: even when Chinese firms cannot lawfully obtain the underlying hardware, they can still access advanced Western models through foreign-hosted application programming interfaces (APIs)—interfaces that allow users to query a model remotely without possessing the underlying system—and cloud platforms.

Chinese technology firms have moved aggressively to exploit this gap, using offshore data centers to train their most advanced models on U.S. chips while relying on domestic chips largely for lower-end inference workloads.³⁰ Alibaba was reported to be training its latest Qwen model series in Southeast Asian data centers to access Nvidia chips.³¹ ByteDance, meanwhile, was reported to be using Aolani Cloud as an offshore compute conduit, deploying about 36,000 Nvidia B200 chips in Malaysia through a build-out worth more than \$2.5 billion—roughly twenty-five times Aolani’s reported pre-deal hardware base of about \$100 million.³² Export controls can therefore keep a chip out of China without preventing a Chinese firm from using that same chip abroad to train or improve frontier models.

Recommendation 3: Prohibit Chinese entities from having cloud access.

So long as export controls focus only on where a chip is shipped, rather than who ultimately uses it, Chinese firms will keep reaching advanced compute through offshore data centers, cloud subscriptions, and API access to bypass their domestic hardware limitations. The next

step is to close that gap by treating remote access to controlled compute or model capability as functionally equivalent to an export.

Congress should:

- Direct BIS to require a license to provide cloud access to controlled AI chips, using a combination of U.S. persons restrictions for cloud providers located in the United States and end-use restrictions on exported AI chips.
- Pass the Remote Access Security Act (H.R. 2683) to give BIS the authority to restrict cloud access in the same way that it controls exports, which would simplify the implementation of cloud restrictions.

Part III. What China Must Steal

Where U.S. law meaningfully constrains Chinese firms' access to tools, chips, or cloud services, these firms turn to evasion, deception, and unauthorized access. This section outlines how China illicitly accesses the American AI stack, including through unlawful servicing, foundry access, physical smuggling, or direct extraction of frontier model capability from U.S. systems. This section uses "steal" in that broader strategic sense: some of the conduct below is plainly unlawful; other conduct exploits newer seams that existing law does not always reach cleanly.

Finding 4: Post-sale servicing and verification gaps allow Chinese fabs to maintain restricted tools.

Once a chipmaking tool enters China, it is very difficult for the U.S. government to verify where that tool ends up. As a recent bipartisan House letter explained, "verification visits require advance permission from [Chinese] authorities, can take weeks or months to arrange, and are conducted under escort by [Chinese] security personnel."³³ That makes it hard to determine whether equipment sold for a lawful purpose is later diverted to prohibited facilities, upgraded beyond authorized limits, or serviced in support of restricted production.

This problem is compounded by the fact that new advanced fabs, which should theoretically be subject to stringent U.S. and allied controls, continue to appear in China. *Reuters* recently reported that Huali Microelectronics is preparing a new 7 nm production line at its Shanghai

fab, though the suppliers involved remain unidentified.³⁴ For the time being, this Huali fab is not on the Entity List, nor is it restricted by U.S. allies. By the time the United States and its allies agree that the fab is advanced and should be subjected to tool controls, the fab may already have all the tools it needs.

The problem does not end with the original shipment. Advanced chipmaking tools require constant upkeep—replacement parts, software updates, repairs, and engineering support—and a machine sold lawfully can later be maintained or upgraded in ways that sustain production at a restricted Chinese facility. For example, in December 2025, the *Financial Times* reported that Chinese fabs were upgrading older ASML DUV machines with secondary-market components and third-party on-site engineering—improving performance enough to sustain 7 nm production for advanced smartphone and AI chips without acquiring new restricted equipment.³⁵

The core enforcement problem, then, is not just the initial sale. It is that once advanced tools are inside China, diversion, servicing, and unauthorized upgrades can help sustain restricted production long after export review is complete.

Recommendation 4: Stop the export of controlled tools to any entity in China and restrict maintenance and servicing of controlled tools already in China.

Congress can address the problem above by passing the MATCH Act. The MATCH Act will ensure that chokepoint tools are subject to countrywide restrictions, regardless of the putative recipient or end user. The MATCH Act will also clarify that it is an export control violation to service any tools which are controlled under the EAR and are being used by advanced fabs in China. In the meantime, BIS should implement accordant changes in regulations.

Congress should:

- Pass the MATCH Act, which would:
 - Direct BIS to clarify that servicing any tools subject to the EAR in advanced-node fabs in China is itself an export control violation, regardless of whether the tool was originally sold lawfully.

- Shift export controls on chokepoint tools toward a countrywide scope, reducing reliance on entity-specific controls that become unenforceable once a tool enters China.
- Direct the Department of State to engage allies to raise the level of their controls to meet the level of American controls.

Finding 5: Chinese firms evade foundry due diligence through shell companies.

Current export controls rely heavily on foreign foundries to identify who is ordering a chip, who will ultimately receive it, and whether the chip violates U.S. restrictions. Recent cases show that this system is failing.

In October 2024, researchers found that TSMC had manufactured a key compute chiplet inside Huawei’s Ascend 910B AI processor — despite Huawei being under a strict U.S. export ban since 2020.³⁶ TSMC had produced nearly three million of these chiplets for Sophgo, a Chinese design firm, who ordered them as if they were their own products before diverting them to Huawei.³⁷ TSMC has since faced a potential \$1 billion penalty, cut ties with other firms over similar concerns, and continues to grapple with classification disputes over other Chinese AI chips, such as Enflame’s S60.³⁸

The Foundry Due Diligence Rule was established in January 2025 to address the problem of Chinese companies or their front companies lying about the specifications of their chips to get allied chipmakers to fabricate them. However, that rule still allows Chinese chip designers that are not yet on BIS’s approved-designer list to access advanced 14/16 nm fabrication services if their chips fall below the 30-billion-transistor threshold, or if they omit HBM and remain below BIS’s alternative transistor limits.³⁹

Recommendation 5: Close loopholes in the foundry due diligence rule.

This carveout is a fundamental flaw. A Chinese designer can intentionally stay just below the transistor threshold, avoid HBM, and still get allied fabs to produce AI chips with performance exceeding U.S. export control limits.

Congress should:

- Direct BIS to eliminate the exceptions in the Foundry Due Diligence Rule for chips with lower transistor count chips and no HBM and accelerate BIS vetting of chip designers.

Finding 6: China utilizes sophisticated smuggling networks to acquire restricted AI chips.

When lawful sales and foundry access do not deliver enough compute, Chinese buyers and intermediaries move finished chips and AI servers through disguised intermediaries and indirect shipping routes. The objective is simple: conceal the real end user, route restricted hardware through a permissive jurisdiction, and get it into Chinese hands before the compliance system catches up.

Recent cases show the increased scale of that effort:

- **August 2025:** Two Chinese nationals were charged in Los Angeles with violating the Export Control Reform Act for allegedly exporting tens of millions of dollars in restricted AI chips to China through their front company, ALX Solutions Inc. The scheme routed at least 21 shipments through Singapore and Malaysia, with payments coming from Hong Kong- and China-based companies rather than the stated end users⁴⁰
- **February 2025:** Nine individuals were arrested and three formally charged in Singapore after police raided 22 locations linked to the diversion of Nvidia-powered Dell and Super Micro servers to China; the scheme used a shell company, Luxuriate Your Life Pte Ltd, as a false end user.⁴¹
- **November 2025:** Four defendants were arrested and charged with conspiracy to violate the Export Control Reform Act, smuggling, and money laundering for using a Tampa real estate front company, Janford Realtor LLC, to export restricted Nvidia chips to China via Malaysia and Thailand, financed by \$3.89 million in wire transfers from China.⁴²
- **December 2025:** As part of Operation Gatekeeper, one defendant pleaded guilty to smuggling and unlawful export activities and two others were arrested and charged with conspiracy to smuggle

goods and conspiracy to violate the Export Control Reform Act in connection with exporting or attempting to export at least \$160 million in Nvidia H100 and H200s to China; warehouse workers directed via a Chinese-language group chat relabeled the chips under the fictitious brand “SANDKYAN” and misclassified them as “adapters” for export.⁴³

- **March 2026:** Super Micro co-founder Yih-Shyan “Wally” Liaw and two associates were indicted on charges of conspiracy to violate the Export Control Reform Act, smuggling, and conspiracy to defraud the United States for diverting \$2.5 billion in Nvidia-powered servers to China using dummy servers and fabricated documents to deceive compliance auditors.⁴⁴
- **March 2026:** Three defendants were charged with conspiracy to smuggle and violate export control regulations for attempting to order 750 servers worth \$170 million from a California-based manufacturer through Thai front companies destined for China.⁴⁵

Recent reporting suggests that some restricted compute may already be operating inside frontier AI labs in China. In December 2025, *The Information* reported that DeepSeek was developing its next major model on “several thousand” Nvidia Blackwell chips barred from export to China.⁴⁶ A senior Trump administration official nonetheless confirmed the chip use to *Reuters* in February 2026, stating that the chips were “likely clustered at its data center in Inner Mongolia” and that DeepSeek would likely “remove the technical indicators” that might reveal which chips it had used.⁴⁷ In April 2026, *Bloomberg* reported that DeepSeek was actively hiring engineers for that same facility.⁴⁸

As AI chip-related export control violations multiply—growing larger, more sophisticated, and more brazen with each successive case—and increasingly place restricted hardware in the hands of high-risk end users, U.S. enforcement must keep pace and treat this activity as organized, persistent, and strategic.⁴⁹

Recommendation 6: Pass the Chip Security Act and the STOP Shells Act.

Current enforcement actions remain largely reactive, often beginning only after restricted hardware or controlled technology has already been

rerouted, relabeled, or transferred under false pretenses. Investigators are then left reconstructing shell-company networks, shipping trails, and altered components after the chips and technology have already changed hands.

Congress should:

- Pass the Chip Security Act (S. 1705/H.R. 3447), directing the Secretary of Commerce to require security mechanisms for advanced AI chips exported from the United States, with flexibility to mandate whatever technical measures can reliably detect unlawful diversion.
- Pass the STOP Shells Act (H.R. 4530), which codifies Commerce Department rules extending export controls to subsidiaries majority-owned by blacklisted companies, closing the loophole that allows sanctioned entities to route restricted technology through nominally independent affiliates.

Finding 7: China extracts frontier capabilities from American AI developers through industrial-scale fraud.

Chinese firms have more ways than chip smuggling to benefit from American innovation. As documented in the Committee’s bipartisan April 2025 report, *DeepSeek Unmasked*, it was highly likely that DeepSeek used a practice called adversarial or unauthorized distillation to create an imitation AI model by copying leading U.S. AI models’ capabilities in violation of U.S. companies’ terms of service.⁵⁰ OpenAI told the Committee that DeepSeek employees “circumvented guardrails” to “extract reasoning outputs” for this purpose, and that DeepSeek’s resulting R1 model displayed “reasoning structures and phrase patterns” consistent with OpenAI’s own models.⁵¹

Frontier labs responded by tightening regional-access and account-enforcement controls and by expanding detection and mitigation of extraction attacks.⁵² Chinese users and firms maintained access nonetheless, relying on proxies, resellers, and overseas intermediaries.

In February 2026, OpenAI reported that “the majority of adversarial distillation activity” it had observed on its platform “appears to originate from China, and occasionally from Russia,” and said DeepSeek used methods such as “obfuscated third-party routers” to mask its source.⁵³

Anthropic separately disclosed “industrial-scale campaigns” by DeepSeek, Moonshot, and MiniMax involving over 16 million exchanges across 24,000 fraudulent accounts, and said that some labs relied on commercial proxy services running “hydra cluster” architectures to keep access alive at scale.⁵⁴ Google likewise reported a sharp rise in distillation attacks against Gemini, not limited to China, including one campaign involving more than 100,000 prompts aimed at extracting reasoning capabilities.⁵⁵

These disclosures reveal a sophisticated access infrastructure designed to obfuscate request sources, distribute traffic across thousands of fraudulent accounts, and maintain connectivity despite provider restrictions. The core of this infrastructure is a software layer of open-source “relay” tools that intercept and reroute API requests. Two prominent examples are the One API and New API repositories. One API describes itself as enabling access to “all large models out of the box via the standard OpenAI API format,” while New API identifies One API as its “original project base” and advertises format conversion among OpenAI, Claude, and Gemini.⁵⁶ Together, these two public code repositories have been copied and modified roughly 11,000 times on GitHub, underscoring how easy this infrastructure is to reuse.⁵⁷

The commercial market includes operators built on these tools, such as CloseAI, Chatfire, and BianXie AI. CloseAI serves major institutional customers including Alibaba, Tencent, Baidu, Tsinghua University, and Peking University.⁵⁸ Its website advertises “model distillation training” as a core use case while explicitly targeting users who have been repeatedly banned by American AI platforms.⁵⁹ BianXie AI claims over 20,000 customers and appears to use accounts tied to U.S. universities to circumvent access restrictions.⁶⁰ Chatfire functions as a wholesale supplier, providing upstream model credentials to more than 70 smaller relay operators while processing over \$1 million in API usage daily.⁶¹

Unauthorized or otherwise fraudulent access is also available to the consumer market. On Taobao, vendors openly sell mirror-site subscriptions and resold accounts.⁶² Claude appears to be the top target of unauthorized users seeking access to American AI models, with top listings showing 50,000 transactions and 7,000 repeat purchases at a fraction of Anthropic’s official price.⁶³

The relay operators and gray-market resellers identified in this report share a common feature: their traffic runs over infrastructure operated by

China Telecom and China Unicom.⁶⁴ The Federal Communications Commission (FCC) revoked China Telecom’s U.S. operating authority in October 2021, concluding it was “highly likely to be forced to comply with Chinese government requests” and that its operations created unacceptable risks of “access[ing], stor[ing], disrupt[ing], and/or misrout[ing] U.S. communications.”⁶⁵ The FCC reached the identical conclusion for China Unicom in January 2022.⁶⁶ These determinations are underpinned by Chinese law, which requires companies to report to and cooperate with state authorities, including in intelligence work.⁶⁷

Consequently, every prompt, output, and usage pattern flowing through these networks is accessible to entities answerable to the Chinese state. The telecom layer is not incidental to the distillation problem; it is the critical backbone that keeps unauthorized access viable and funnels exploitable data directly to Chinese labs. Under Beijing’s military-civil fusion doctrine, capabilities acquired through commercial fraud and gray-market channels are systematically absorbed into military, intelligence, and public security programs.⁶⁸

Recommendation 7: Treat adversarial distillation as industrial espionage and impose corresponding penalties.

Chinese AI labs and researchers who use fraudulent accounts, relay infrastructure, and unauthorized API access to extract U.S. frontier model capability are not merely violating platform terms of service. They are obtaining the functional benefits of American AI systems through deception and using those outputs to research, develop, and train competing models to the benefit of China and at the expense of America’s national security and economic prosperity. The conduct is systematic, state-adjacent, and strategically directed.

Congress should:

- Direct the State Department’s Bureau of Emerging Threats to assess whether systematic adversarial distillation by state-affiliated firms threatens U.S. national security and refer appropriate cases to DOJ for investigative and prosecutorial review under applicable law, including the Economic Espionage Act and the Computer Fraud and Abuse Act.

- Define adversarial distillation as a category of controlled technology transfer. A workable definition should cover extraction activity that: (1) circumvents technical, contractual, or other access controls, identity-verification requirements, or geographic restrictions imposed by the model owner; (2) relies on fraudulent, misrepresented, or unauthorized credentials; or (3) violates terms of service or API access agreements prohibiting use of model outputs to replicate, develop, train, or improve a competing AI system.
- Direct BIS to evaluate DeepSeek, Moonshot AI, and MiniMax for Entity List designation under Section 744.11 of the EAR with a presumption of denial, using the same authority applied to Zhipu AI in January 2025.⁶⁹
- Authorize and fund the Department of Homeland Security to establish the AI Information Sharing and Analysis Center (AI-ISAC) proposed in the Trump Administration’s July 2025 AI Action Plan.⁷⁰

Finding 8: Weak enforcement and limited penalties fail to deter violations.

This report has documented a series of violations for hardware smuggling, multiple of which would have been unprecedented in scale and sophistication just a few years ago. There are also a growing number of software violations. For example, Cadence Design Systems agreed to plead guilty to one count of conspiracy to violate U.S. export control laws and pay more than \$140 million to resolve criminal and civil charges for unlawfully exporting sensitive semiconductor design tools to China’s National University of Defense Technology—a restricted Chinese military university on the Entity List—through front entities including Central South CAD Center and Phytium.⁷¹ And in January 2026, a former Google software engineer was convicted on 14 counts of economic espionage and trade secret theft—the first-ever U.S. conviction on AI-related economic espionage charges—for stealing more than 1,000 files containing Google’s proprietary AI supercomputing infrastructure while secretly serving as CTO of an AI startup in China.⁷²

The large and growing volume of thefts across both hardware and software is a sign that China is increasingly desperate for restricted technologies; it is also a sign that deterrence is failing. Would-be

smugglers recognize that proving a criminal violation of export controls is extremely challenging, export enforcement is under-resourced, and the rewards of smuggling AI hardware and software are higher than ever. Meanwhile, many exporters recognize that civil penalties for export control violations have tight statutory caps. As a result, they are not conducting adequate due diligence. Companies will need to increase their compliance efforts to avoid being fooled into violations, but they have little incentive to do so.

Recommendation 8: Increase civil and criminal penalties for export control violations.

Current penalties were not built for a system in which advanced chip equipment can be diverted, upgraded, and serviced in support of prohibited Chinese production lines worth billions of dollars. So long as the likely consequence for many actors remains delay, negotiation, or a manageable compliance penalty, exporters, brokers, freight intermediaries, and service providers will continue to treat serious violations as a tolerable cost of doing business.

Congress should:

- Increase civil and criminal penalties under the Export Control Reform Act and EAR to reflect the scale and strategic significance of chip export-control violations.
- Ensure DOJ and BIS have the resources, staffing, and interagency coordination mechanisms needed to investigate and prosecute these cases at the pace and scale the challenge demands.
- Require BIS to condition military end users and other high-risk export licenses on personal certification by the applicant's chief executive officer that the application is complete and accurate, that the company has conducted reasonable due diligence, and that it has internal controls reasonably designed to prevent diversion to prohibited end users or end uses. Congress should impose civil and criminal liability for knowing or reckless false certifications, including denial of export privileges, debarment, and referral to DOJ.

¹ As the National Security Commission on Artificial Intelligence observed, AI is “not a single piece of hardware or software, but rather a constellation of technologies” built on interrelated layers that can be understood as a stack, *see* Final Report, Nat’l Sec. Comm’n on Artificial Intelligence at 31 (2021), <https://www.govinfo.gov/app/details/GOVPUB-Y3-PURL-gpo153246>.

² At the 20th Collective Study Session of the CCP Central Committee Politburo, Xi Jinping Stresses: Persist in Being Self-Reliant, Be Strongly Oriented Toward Applications, and Push the Orderly Development of Artificial Intelligence [习近平在中共中央政治局第二十次集体学习时强调 坚持自立自强 突出应用导向 推动人工智能健康有序发展], Xinhua News Agency [新华社] (Apr. 26, 2025), <https://perma.cc/5UBL-GCVG>.

³ A New Generation Artificial Intelligence Development Plan [新一代人工智能发展规划的通知], State Council [国务院] (July 20, 2017), <https://perma.cc/8C34-4SLA>; Made in China 2025 [中国制造2025], State Council [国务院] (May 8, 2015), <https://perma.cc/E2DC-MHWV>; Outline of the People’s Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035 [中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要], Xinhua News Agency [新华社] (Mar. 12, 2021), <https://perma.cc/73AK-BUW2>; Outline of the 15th Five-Year Plan for National Economic and Social Development of the People’s Republic of China [中华人民共和国国民经济和社会发展第十五个五年规划纲要], Nat’l Dev. & Reform Comm’n (Mar. 2026), <https://perma.cc/AB7C-96NR>.

⁴ Years noted are based on the aggregation of the individual companies’ fiscal years, not calendar years, *see* H. Select Comm. on China, *Selling the Forges of the Future* (Oct. 2025), <https://perma.cc/8TTU-AU2C>.

⁵ *Id.*

⁶ Chinese authorities have pushed domestic chipmakers to buy more locally produced equipment, increasing the domestic share of semiconductor equipment used in China from 25% in 2024 to 35% in 2025, while Chinese toolmakers have also moved onto more advanced domestic production lines, including deployments by NAURA, Piotech, and ACM Research at SMIC, YMTC, and Hua Hong; one report also indicates that AMEC’s 5 nm etching tool entered validation on TSMC lines, *see* AI Drives Global Semiconductor Market to a Record High in 2025; Semiconductor Materials and Equipment Index Rises More Than 6%! [AI驱动2025全球半导体市场创历史新高, 半导体材料设备指数涨超6%!], Jiemian News (Jan. 7, 2026), <https://perma.cc/5R4A-3EQE>; China’s Domestic Share of Semiconductor Equipment Reaches 35% [陆半导体设备 国产占35%], Commercial Times [工商时报] (Jan. 11, 2026), <https://perma.cc/W5GF-LR7J>; Major Progress in China’s “De-Americanization” of Chips: Semiconductor Equipment Localization Surpasses 50% Ahead of Schedule, and 7 nm Validation Accelerates [中国芯片“去美化”重大进展! 半导体设备国产化提前破50%、7纳米验证提速], Anue News [钜亨网] (Jan. 11, 2026), <https://perma.cc/95Q7-Q6EL>.

⁷ *Id.*

⁸ U.S. and partner manufacturing capacity for advanced logic chips is approximately 35 to 38 times that of China’s after adjusting for quality; yield defects widen that gap further, as Huawei Ascend chips achieve yields of only 5% to 20% against 60% to 80% for Nvidia Blackwell, producing an effective U.S. advantage of 170 to 180 times. All known teardowns of Huawei AI chips have found stockpiled foreign components rather than domestically manufactured chips, *see* Georgia Adamson et al., *Should the US Sell Blackwell Chips to China?*, Inst. for Progress (Oct. 25, 2025), <https://ifp.org/the-b30a-decision/>.

⁹ U.S. and partner HBM production in 2025 is approximately 3,090 times that of China’s. Even by 2026, as China brings more capacity online, the United States is projected to produce 70 times as much HBM. In absolute terms, China’s 2026 HBM production can support a mere 275,000 Huawei Ascend 910C chips, equivalent to 55,000 B300-equivalents, *see* *Id.* Notably, neither CXMT nor YMTC is currently on the Entity List, and the ongoing memory shortage has already prompted major U.S. firms—including Qualcomm, Dell, and HP—to qualify CXMT as a supplier. If that foothold expands, the United States risks a familiar pattern: Chinese producers scaling on Western demand during a supply crunch, then flooding the market with below-cost memory once the supercycle wanes.

¹⁰ Wendy Chang et al., *China’s drive toward self-reliance in artificial intelligence: from chips to large language models*, Mercator Inst. for China Studies (July 22, 2025), <https://perma.cc/MQT9-XT3Z>; Michael Laha, *PRC Pursues Chip Design Software Dominance*, Jamestown (Mar. 15, 2024), <https://jamestown.org/prc-pursues-eda-software-dominance/>.

¹¹ The Ascend 910C delivers roughly half the processing power and 25% less memory bandwidth of Nvidia's B30A, at nearly three times the cost per unit of performance., *see Id.*

¹² *Id.*; U.S.-China Econ. & Sec. Review Comm'n, 2024 Annual Report to Congress, pt. II, ch. 3: U.S.-China Competition in Emerging Technologies (Nov. 2024), <https://perma.cc/3UM6-9ZGV>.

¹³ Hardware-software co-design is a well-established technique, but scaling laws mean frontier capability is still a function of raw compute, and on that dimension, China's deficit is measured in orders of magnitude, *see* John Shalf et al., Rethinking Hardware-Software Codesign for Exascale Systems, *Computer* (Oct. 6, 2011), <https://doi.org/10.1109/MC.2011.300>. *See also:* AI + Manufacturing Special Action Implementation Opinion [人工智能+制造专项行动实施意见], Ministry of Indus. & Info. Tech. (Jan. 7, 2026),

<https://web.archive.org/web/20260109212920/https://www.ncsti.gov.cn/zcfg/zcwj/202601/P020260109595566804450.pdf>; Sun Qingyang [孙庆阳], "Software-Hardware Co-Development" Becomes the Key to Breaking Through Bottlenecks in the AI Industry ["软硬协同"成为AI产业破局关键], *S&T Daily* (July 28, 2025), <https://perma.cc/Z9P8-ASAL>; Another boost for domestic chips! Zhipu's new-generation large model is now fully compatible with Cambrian and Moore Threads chips! [国产芯片再迎利好! 智谱新一代大模型, 全面适配寒武纪和摩尔线程芯片!], *Securities Times Online* [证券时报网] (Sep. 30, 2025), <https://perma.cc/KW93-7N5T>.

¹⁴ Its 2026 "Artificial Intelligence+ Manufacturing" action plan calls for "small models for specific industrial scenarios," "collaborative innovation between large and small models," and faster deployment of lightweight models in industrial settings, *see* AI + Manufacturing Special Action Implementation Opinion [人工智能+制造专项行动实施意见], Ministry of Indus. & Info. Tech. (Jan. 7, 2026),

<https://web.archive.org/web/20260109212920/https://www.ncsti.gov.cn/zcfg/zcwj/202601/P020260109595566804450.pdf>.

¹⁵ H. Select Comm. on China, *DeepSeek Unmasked* (Apr. 2025), <https://perma.cc/2BDE-EE3U>.

¹⁶ Alexandra Alper et al., Trump administration pressed Dutch hard to cancel China chip-equipment sale - sources, *Reuters* (Jan. 6, 2020), <https://www.reuters.com/article/world/uk/trump-administration-pressed-dutch-hard-to-cancel-china-chip-equipment-sale-so-idUSKBN1Z50H4/>.

¹⁷ Brandon J. Weichert, Did China Break an ASML Lithography Machine While Trying to Reverse-Engineer It?, *The National Interest* (Oct. 20, 2025), <https://nationalinterest.org/blog/buzz/did-china-break-asml-lithography-machine-while-trying-to-reverse-engineer-bw-102025>.

¹⁸ H. Select Comm. on China, *Selling the Forges of the Future* (Oct. 2025), <https://perma.cc/8TTU-AU2C>.

¹⁹ *Id.*

²⁰ *Id.*

²¹ *Id.*

²² Bureau of Industry & Sec., Dep't of Commerce, *Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections*, 88 Fed. Reg. 73458 (Oct. 25, 2023), <https://www.federalregister.gov/documents/2023/10/25/2023-23055/implementation-of-additional-export-controls-certain-advanced-computing-items-supercomputer-and>; Bureau of Industry & Sec., Dep't of Commerce, *Revision to License Review Policy for Advanced Computing Commodities*, 91 Fed. Reg. 1684 (Jan. 15, 2026), <https://www.federalregister.gov/documents/2026/01/15/2026-00789/revision-to-license-review-policy-for-advanced-computing-commodities>.

²³ Released on January 13, 2026, the rule codifies Trump's decision last December to allow China-bound exports of Nvidia H200 and AMD MI325X chips, *see* Bureau of Industry & Sec., Dep't of Commerce, *Revision to License Review Policy for Advanced Computing Commodities*, 91 Fed. Reg. 1684 (Jan. 15, 2026), <https://www.federalregister.gov/documents/2026/01/15/2026-00789/revision-to-license-review-policy-for-advanced-computing-commodities>.

²⁴ Exclusive: China gives nod to ByteDance, Alibaba and Tencent to buy Nvidia's H200 chips - sources, *Reuters* (Jan. 28, 2026), <https://www.reuters.com/world/china/china-gives-green-light-importing-first-batch-nvidias-h200-ai-chips-sources-say-2026-01-28/>.

²⁵ Exclusive: Nvidia considers increasing H200 chip output due to robust China demand, sources say, *Reuters* (Dec. 15, 2025), <https://www.reuters.com/world/china/nvidia-considers-increasing-h200-chip-output-due-robust-china-demand-sources-say-2025-12-12/>.

²⁶ Wei Shaojun of the China Semiconductor Industry Association on Nvidia's H200 chip: Confidence and resolve in the path of domestic substitution will not waver [中国半导体行业协会魏少军谈英伟达

H200芯片：绝不动摇国产化道路信心与决心], Global Times [环球时报] (Jan. 8, 2026), <https://perma.cc/VJ3G-MUW8>.

²⁷ Edited Transcript: 2330.TW - Q3 2025 Taiwan Semiconductor Manufacturing Co Ltd Earnings Call (Chinese, English), Taiwan Semicon. Mfg. Co. (Oct. 2025), https://investor.tsmc.com/english/encrypt/files/encrypt_file/reports/2025-10/6860312f04fd291d0f26b46c1234f84e6332717e/TSMC%20Q25%20Transcript.pdf. The three major HBM suppliers are SK Hynix, Samsung, and Micron. All three have confirmed sold-out production capacity through 2026, *see* Press Release, SK hynix Announces 3Q25 Financial Results, SK hynix (Oct. 29, 2025), <https://news.skhynix.com/sk-hynix-announces-3q25-financial-results/>; Financial Results FQ1 2026, Micron (Dec. 17, 2025), <https://investors.micron.com/static-files/530bd7ed-a8c8-4687-af4a-8c129f740e09>; Financial Results: FQ2 2026, Micron (Mar. 18, 2026), <https://investors.micron.com/static-files/9c0becf5-df56-4eec-bd67-453dda68b273>; Samsung Reportedly Plans 50% HBM Capacity Surge in 2026, Spotlight on HBM4, TrendForce (Dec. 30, 2025), <https://www.trendforce.com/news/2025/12/30/news-samsung-reportedly-plans-50-hbm-capacity-surge-in-2026-spotlight-on-hbm4/>.

²⁸ Hyunjoon Jin et al., The AI frenzy is driving a memory chip supply crisis, Reuters (Dec. 2, 2025), <https://www.reuters.com/world/china/ai-frenzy-is-driving-new-global-supply-chain-crisis-2025-12-03/>.

²⁹ Chih-Hua Tseng & Jin Chian Seer, A Shared Future? Economic Security Challenges from Malaysia-China Economic Cooperation and Data Center Development, Rsch. Inst. for Democracy, Soc’y, & Emerging Tech. (Oct. 28, 2025), <https://dset.tw/en/research/a-shared-future-economic-security-challenges-from-malaysia-china-economic-cooperation-and-data-center-development/>.

³⁰ Zijiang Wu, China’s tech giants take AI model training offshore to tap Nvidia chips, Fin. Times (Nov. 27, 2025), <https://www.ft.com/content/96fe9898-a3a4-4a33-be1d-da06bdb6cb2b>.

³¹ *Id.*

³² Jon Emont & Liza Lin, China’s ByteDance Gets Access to Top Nvidia AI Chips, The Wall Street Journal (Mar. 12, 2026), <https://www.wsj.com/tech/chinas-bytedance-gets-access-to-top-nvidia-ai-chips-d68bce3a>.

³³ Letter from Brian J. Mast et al. to Marco Rubio, Sec’y of State, and Howard Lutnick, Sec’y of Com. (Feb. 9, 2026), <https://drive.google.com/file/d/1EP1zHcQ5sqd-d2gRyPVK0RdDpVZPe0FL/view>.

³⁴ Exclusive: China’s No. 2 chipmaker readies 7 nm production as Beijing ramps up self-sufficiency, Reuters (Mar. 15, 2026), <https://www.reuters.com/world/asia-pacific/chinas-no-2-chipmaker-readies-7-nm-production-beijing-ramps-up-self-sufficiency-2026-03-16/>.

³⁵ Eleanor Olcott, China boosts AI chip output by upgrading older ASML machines, Fin. Times (Dec. 18, 2025), <https://www.ft.com/content/d10398db-b8b4-40f3-8c6d-b340470f5f3c>.

³⁶ Karen Freifeld, Exclusive: TSMC told US of chip in Huawei product after TechInsights finding, source says, Reuters (Oct. 22, 2024), <https://www.reuters.com/technology/tsmc-told-us-chip-huawei-device-after-techinsights-finding-source-says-2024-10-22/>.

³⁷ Karen Freifeld, Exclusive: TSMC told US of chip in Huawei product after TechInsights finding, source says, Reuters (Oct. 22, 2024), <https://www.reuters.com/technology/tsmc-told-us-chip-huawei-device-after-techinsights-finding-source-says-2024-10-22/>.

³⁸ Karen Freifeld & Fanny Potkin, TSMC suspended shipments to China firm after chip found on Huawei processor, sources say, Reuters (Oct. 27, 2024), <https://www.reuters.com/technology/tsmc-suspended-shipments-china-firm-after-chip-found-huawei-processor-sources-2024-10-26/>; Karen Freifeld, Exclusive: TSMC could face \$1 billion or more fine from US probe, sources say, Reuters (Apr. 8, 2025), <https://www.reuters.com/technology/tsmc-could-face-1-billion-or-more-fine-us-probe-sources-say-2025-04-08/>; Jared Perlo, AI chip made for Chinese company draws scrutiny over potential U.S. export violations, NBC News (Feb. 27, 2026), <https://www.nbcnews.com/tech/tech-news/ai-chip-tsmc-enflame-techinsights-rcna259342>.

³⁹ Bureau of Industry & Sec., Dep’t of Commerce, Implementation of Additional Due Diligence Measures for Advanced Computing Integrated Circuits; Amendments and Clarifications; and Extension of Comment Period, 90 Fed. Reg. 5298, 5301, 5305, 5315 (Jan. 16, 2025), <https://www.federalregister.gov/documents/2025/01/16/2025-00711/implementation-of-additional-due-diligence-measures-for-advanced-computing-integrated-circuits>.

⁴⁰ Press Release, Two Chinese Nationals Arrested on Complaint Alleging they Illegally Shipped to China Sensitive Microchips Used in AI Applications, U.S. Dep’t of Justice (Aug. 5, 2025), <https://www.justice.gov/opa/pr/two-chinese-nationals-arrested-complaint-alleging-they-illegally-shipped-china-sensitive>; Press Release, Two Chinese Nationals Arrested on Federal Complaint

Alleging They Illegally Shipped to China Sensitive Microchips Used in AI Applications, U.S. Dep't of Justice (Aug. 5, 2025), <https://www.justice.gov/usao-cdca/pr/two-chinese-nationals-arrested-federal-complaint-alleging-they-illegally-shipped-china>.

⁴¹ Singapore charges men with defrauding Dell, Super Micro, Reuters (Mar. 6, 2025), <https://www.reuters.com/world/asia-pacific/singapore-adds-charges-two-held-server-fraud-case-2025-03-06/>.

⁴² Press Release, U.S. Citizens and Chinese Nationals Arrested for Exporting Artificial Intelligence Technology to China, U.S. Dep't of Justice (Nov. 20, 2025), <https://www.justice.gov/opa/pr/us-citizens-and-chinese-nationals-arrested-exporting-artificial-intelligence-technology>.

⁴³ Press Release, U.S. Authorities Shut Down Major China-Linked AI Tech Smuggling Network, U.S. Dep't of Justice (Dec. 8, 2025), <https://www.justice.gov/opa/pr/us-authorities-shut-down-major-china-linked-ai-tech-smuggling-network>.

⁴⁴ Press Release, Three Charged with Conspiring to Unlawfully Divert Cutting Edge U.S. Artificial Intelligence Technology to China, U.S. Dep't of Justice (Mar. 19, 2026), <https://www.justice.gov/opa/pr/three-charged-conspiring-unlawfully-divert-cutting-edge-us-artificial-intelligence>.

⁴⁵ Press Release, Chinese National and Two U.S. Citizens Charged with Conspiring to Smuggle Artificial Intelligence Technology to China, U.S. Dep't of Justice (Mar. 25, 2026), <https://www.justice.gov/opa/pr/chinese-national-and-two-us-citizens-charged-conspiring-smuggle-artificial-intelligence>.

⁴⁶ DeepSeek is Using Banned Nvidia Chips in Race to Build Next Model, The Information (Dec. 10, 2025), <https://www.theinformation.com/articles/deepseek-using-banned-nvidia-chips-race-build-next-model>.

⁴⁷ Steve Holland & Alexandra Alper, Exclusive: China's DeepSeek trained AI model on Nvidia's best chip despite US ban, official says, Reuters (Feb. 23, 2026), <https://www.reuters.com/world/china/chinas-deepseek-trained-ai-model-nvidias-best-chip-despite-us-ban-official-says-2026-02-24/>.

⁴⁸ Debby Wu, DeepSeek Looks for Data Center Engineers in Inner Mongolia, Bloomberg (Apr. 10, 2026), <https://www.bloomberg.com/news/articles/2026-04-10/deepseek-looks-for-data-center-engineers-in-inner-mongolia>.

⁴⁹ For broader context on smuggling and diversion as recurring tools of China's technology acquisition strategy, see Matt Brazil, The Shapeshifting Evolution of Chinese Technology Acquisition, Jamestown (June 7, 2025), <https://jamestown.org/the-shapeshifting-evolution-of-chinese-technology-acquisition/>.

⁵⁰ H. Select Comm. on China, DeepSeek Unmasked (Apr. 2025), <https://perma.cc/2BDE-EE3U>. For more on distillation, see Issue Brief: Adversarial Distillation, Frontier Model Forum (Feb. 23, 2026), <https://www.frontiermodelforum.org/issue-briefs/issue-brief-adversarial-distillation/>.

⁵¹ *Id.*

⁵² Updating restrictions of sales to unsupported regions, Anthropic (Sep. 4, 2025), <https://www.anthropic.com/news/updating-restrictions-of-sales-to-unsupported-regions>; Supported countries & regions, Anthropic (accessed on Apr. 8, 2026), <https://www.anthropic.com/supported-countries>; Supported countries and territories, OpenAI (accessed on Apr. 8, 2026), <https://developers.openai.com/api/docs/supported-countries>; Available regions for Google AI Studio and Gemini API, Gemini (accessed on Apr. 8, 2026), <https://ai.google.dev/gemini-api/docs/available-regions>.

⁵³ OpenAI, Memo to the U.S. House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party on "Updated Stakes for American-Led, Democratic AI" (Feb. 12, 2026), https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/rRmqL_jjCxb4/v0.

⁵⁴ Detecting and preventing distillation attacks, Anthropic (Feb. 23, 2026), <https://www.anthropic.com/news/detecting-and-preventing-distillation-attacks>.

⁵⁵ GTIG AI Threat Tracker: Distillation, Experimentation, and (Continued) Integration of AI for Adversarial Use, Google Threat Intelligence Group (Feb. 12, 2026), <https://cloud.google.com/blog/topics/threat-intelligence/distillation-experimentation-integration-ai-adversarial-use>.

⁵⁶ songquanpeng, One API, GitHub, <https://github.com/songquanpeng/one-api> (accessed on Apr. 8, 2026); QuantumNous, New API, GitHub, <https://github.com/QuantumNous/new-api> (accessed on Apr. 8, 2026). Of note, the Committee has not confirmed whether the model providers identified in this report were aware of, or had specifically attributed abuse to, each individual service or

repository discussed here. These examples are included to illustrate the broader relay and access infrastructure supporting unauthorized use of U.S. frontier AI models.

⁵⁷ *Id.*

⁵⁸ Homepage, CloseAI, <https://perma.cc/RXJ3-N5KW> (accessed on Mar. 30, 2026).

⁵⁹ Most notably, CloseAI's business model is architecturally designed to absorb account termination losses. Its pricing page includes "ban cost" as an explicit line item in its fee structure—priced right alongside standard operational expenses like Stripe transaction fees, currency exchange fees, and bandwidth costs, *see Id.*

⁶⁰ BianXie's homepage states that it is "backed by multiple PhD students studying in the United States" (背靠多位留美博士生). In context, "backed" (背靠) is best read to mean operational support, suggesting that U.S.-based PhD students help run or supply the platform, rather than referring to its customer base. That reading is consistent with account-creation records published on the affiliated chatgptboke.com blog, which show OpenAI accounts registered through Yale University (ASN 29) and Columbia University (ASN 14) network infrastructure, *see* Portable AI Aggregator API [便携AI聚合API], Bianxie (Feb. 20, 2026), <https://perma.cc/QN8K-JEPF>; ChatGPT Account Purchase and ChatGPT Proxy Registration Services [ChatGPT账号购买与ChatGPT代注册服务], ChatGPT Blog (Nov. 3, 2025), <https://perma.cc/8M3S-DM8P>; ChatGPT Knowledge Planet: Hundreds of tutorials to help you go from beginner to proficient with ChatGPT [ChatGPT知识星球: 上百篇ChatGPT教程带你从0到1玩转ChatGPT], Bianxie (July 15, 2023), <https://perma.cc/74TX-G77J>; ChatGPT account purchase and ChatGPT registration service [ChatGPT账号购买与ChatGPT代注册服务] (Nov. 3, 2025), <https://perma.cc/U5NV-YE58>.

⁶¹ Homepage, ChatfireAPI, <https://perma.cc/RT8T-BQXG> (accessed on Mar. 30, 2026).

⁶² Lily Ottinger et al., How to Use Banned US Models in China, ChinaTalk (June 5, 2025), <https://www.chinatalk.media/p/the-grey-market-for-american-llms>.

⁶³ *Id.*

⁶⁴ Platform Introduction, CloseAI, <https://doc.closeai-asia.com/tutorial/introduction.html> (accessed on Mar. 30, 2026); Portable AI Aggregator API [便携AI聚合API], Bianxie (Feb. 20, 2026), <https://perma.cc/QN8K-JEPF>; Types of China IP transit, Bandwagon Host, <https://perma.cc/CET6-4RQ5> (accessed on Mar. 30, 2026); Types of China IP transit, Bandwagon Host, <https://perma.cc/9Y3P-K9FJ> (accessed on Mar. 30, 2026); Homepage, GigsGigs Cloud, <https://perma.cc/BB5Y-JKX8> (accessed on Mar. 30, 2026); Homepage, ChatfireAPI, <https://perma.cc/RT8T-BQXG> (accessed on Mar. 30, 2026).

⁶⁵ FCC Revokes and Terminates China Telecom America's Authority to Provide Telecom Services in America, Fed. Comm'ns Comm'n, FCC 21-114, at para. 2 (Oct. 26, 2021), <https://perma.cc/RS4H-QUS4>.

⁶⁶ FCC Revokes China Unicom Americas' Authority to Provide Telecom Services in America, Fed. Comm'ns Comm'n, FCC 22-9, at para. 2 (Jan. 27, 2022), <https://perma.cc/WU66-6QZB>.

⁶⁷ In March 2025, the Committee sent both firms a bipartisan request for information and, after they refused to respond, subpoenaed them in April, *see* Press Release, House Committee Subpoenas Chinese Telecom Giants After Refusal to Disclose CCP and Military Links, H. Select Comm. on China (Apr. 24, 2025), <https://perma.cc/6QHY-8XCG>. Also, *see* PRC National Security Laws, Ctr. for Naval Analyses, (2023), <https://perma.cc/KCJ8-RDX8>.

⁶⁸ For more examples of how Chinese AI models like DeepSeek are being used to advance China's military and intelligence goals, *see* Sunny Cheung & Kai-shing Lau, DeepSeek Use in PRC Military and Public Security Systems, The Jamestown Foundation (Oct. 27, 2025), <https://jamestown.org/deepseek-use-in-prc-military-and-public-security-systems/>.

⁶⁹ Addition of Entities to and Revision of Entry on the Entity List, 90 Fed. Reg. 4,617 (Jan. 16, 2025), <https://www.federalregister.gov/documents/2025/01/16/2025-00704/addition-of-entities-to-and-revision-of-entry-on-the-entity-list>.

⁷⁰ Winning the Race: America's AI Action Plan, The White House (July 2025) at 18, <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>. In February 2026, the executive assistant director for cybersecurity at the Cybersecurity and Infrastructure Security Agency revealed that there was no timeline for establishing AI-ISAC, *see* Eric Geller, AI-ISAC inches forward under Trump administration, Cybersecurity Dive (Feb. 3, 2026), <https://www.cybersecuritydive.com/news/ai-isac-us-government-update-cisa/811281/>.

⁷¹ Press Release, Cadence Design Systems Agrees to Plead Guilty and Pay Over \$140 Million for Unlawfully Exporting Semiconductor Design Tools to a Restricted PRC Military University, U.S. Dep't of Justice (July 28, 2025), <https://www.justice.gov/opa/pr/cadence-design-systems-agrees-plead-guilty-and-pay-over-140-million-unlawfully-exporting>.

⁷² Press Release, Superseding Indictment Charges Chinese National In Relation To Alleged Plan To Steal Proprietary AI Technology, U.S. Dep't of Justice (Feb. 4, 2025), https://www.justice.gov/usao-ndca/pr/superseding-indictment-charges-chinese-national-relation-alleged-plan-steal?utm_medium=email&utm; Press Release, Former Google Engineer Found Guilty of Economic Espionage and Theft of Confidential AI Technology, U.S. Dep't of Justice (Jan. 30, 2026), https://www.justice.gov/usao-ndca/pr/chinese-national-residing-california-arrested-theft-artificial-intelligence-related?utm_medium=email&utm; Press Release, Former Google Engineer Found Guilty of Economic Espionage and Theft of Confidential AI Technology, U.S. Dep't of Justice (Jan. 30, 2026), <https://www.justice.gov/opa/pr/former-google-engineer-found-guilty-economic-espionage-and-theft-confidential-ai-technology>.