CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Statement before the House of Representatives Committee on the Judiciary Subcommittee on Courts, Intellectual Property, and the Internet

"Protecting Our Edge: Trade Secrets and the Global AI Arms Race"

A Testimony by:

Benjamin Jensen, PhD

Director and Senior Fellow, CSIS Futures Lab

Frank E. Petersen Chair, School of Advanced Warfighting, Marine Corps University

May 7, 2025

Rayburn House Office Building

Chairman Issa, Ranking Member Johnson, and distinguished Members of the Subcommittee, thank you for the opportunity to testify today on a matter of critical importance to the future economic prosperity and national security of the United States: maintaining American leadership in artificial intelligence (AI).

We are entering the era of agentic AI, in which algorithms will manage multiple complex processes in a manner that fundamentally change how we work, live, and govern.[1] Free societies led by the US made this new epoch possible.

While the US has been at the forefront of the theory and engineering that started in the 1950s and grew into the new world we confront today, its position is being challenged by the People's Republic of China (PRC). In short, the race to dominate the agentic era is now a central feature of 21st century great power competition. In this confrontation, failing to protect American innovators risks ceding the century to the Chinese Communist Party.

At the same time, with new technology comes new legal and economic questions. The strength of an open, free society is that the circulation of ideas helps its citizens imagine and build the future. Yet, authoritarian regimes like the CCP exploit this openness to steal a march illicitly acquiring U.S. intellectual property (IP), trade secrets, technological know-how, and sensitive data. As a result, the fundamental question before this committee is how to protect American innovation without sacrificing the very openness and creativity that makes it possible.

To address this challenge, I want to highlight three areas:

1) Disrupting Methods the PRC uses to Hijack U.S. AI models
2) Deterring Cyber Espionage in the Era of Agentic AI
3) The Futility of Export Restrictions

These challenges eclipse the tool kits currently used to protect American innovators and citizens. New methods, from laws to better aligning federal executive agencies, are needed to meet the challenge head on. Three standout:

1) Modernizing Intellectual Property Protections for the AI Era
2) Strengthen Cybersecurity and Treat AI Companies as Critical Infrastructure
3) Escalate to Active Defense and Offensive Operations Against Systemic IP Theft

Challenge 1: Disrupting Methods the PRC uses to Hijack U.S. AI models

[1] Mark Purdy "What is Agentic AI and How Will It Change Work?" *Harvard Business Review* December 12, 2024, online: <<https://hbr.org/2024/12/what-is-agentic-ai-and-how-will-it-change-work>>; Alex Wang on Why China Can't Be Allowed to Dominate AI-Based Warfare" *The Economist* March 4, 2025 << https://www.economist.com/by-invitation/2025/03/04/alex-wang-on-why-china-cant-be-allowed-to-dominate-ai-based-warfare>>; Benjamin Jensen, Dan Tadross, and Matthew Strohmeyer "Agentic Warfare is Here. Will America Be the First Mover?" *War on the Rocks* April 23, 2025 <<https://warontherocks.com/2025/04/agentic-warfare-is-here-will-america-be-the-first-mover/>>.

An emerging threat to American AI leadership involves the replication of advanced AI models through methods such as "distillation". This technique allows a competitor to train a new, often smaller and more efficient, AI model (the "student") by feeding it vast amounts of output generated by a more powerful, pre-existing model (the "teacher"). Access to the teacher model's outputs is frequently obtained via its Application Programming Interface (API), potentially in violation of the provider's terms of service. The recent controversy involving U.S.-based OpenAI and the Chinese AI firm DeepSeek starkly illustrates this challenge. OpenAI has publicly accused DeepSeek of improperly using its API to exfiltrate large volumes of data. OpenAI alleges this data, generated by its proprietary models like ChatGPT, was then used via distillation to train DeepSeek's competing R1 reasoning model. Such actions would likely violate OpenAI's terms of service, which explicitly prohibit using API outputs to develop competing AI models. Supporting these allegations, Microsoft security researchers reportedly detected significant, anomalous data extraction patterns originating from OpenAI developer accounts believed to be affiliated with DeepSeek in late 2024. OpenAI subsequently blocked these accounts.

This case underscores the vulnerability of cutting-edge AI models to unauthorized replication through novel techniques that challenge existing legal frameworks. Current intellectual property laws, including copyright, patent, and trade secrets, were not designed to address the unique complexities of AI, such as the ownership of AI-generated outputs or the legality of model distillation. For instance, U.S. copyright law generally requires human authorship for protection, making it difficult to assert copyright over the outputs of an AI model used in distillation. Furthermore, distillation replicates the functionality and knowledge embedded in a model's outputs, rather than directly copying the underlying code or patented processes, making traditional infringement claims challenging beyond a breach of contract (Terms of Service). The alleged mechanism of API abuse also highlights that this is not merely an IP issue, but a significant cybersecurity challenge. It points to vulnerabilities in API security protocols, inadequate access controls, and insufficient monitoring for anomalous data exfiltration, potentially exposing AI firms to unbounded consumption attacks, in which manipulated input data allows an attacker to exceed data restrictions when using an AI model API.[2]

New technology creates new legal and regulatory quandaries that have significant economic implications. Take AI distillation. Is using a teacher model of a known market competitor to teach a student model illegal? DeepSeek used chatbots to bombard OpenAI's ChatGPT with questions and used the resulting answers to train its model and reduce the underlying computational costs associated with training its R1 as little as $6 million.[3] To put that in perspective, there are reports that ChatGPT 5 cost more than $2 billion dollars to develop, 400 times the cost of ChatGPT 3 and 17 times the cost of ChatGPT 4. The cost to develop new

[2] Master Spring Ter "Consumption and How to Secure Your Spring Boot2.x APIs" *Medium* November 10, 2024 << https://master-spring-ter.medium.com/owasp-api-security-top-4-unrestricted-resource-consumption-and-how-to-secure-your-spring-boot-3-x-42d2e506b39a>>

[3] Adiya Soni and Zaheer Kachwala „DeepSeek's Low-cost AI Spotlights Billions Spent by US Tech" *Reuters* January 29, 2025 <<https://www.reuters.com/technology/artificial-intelligence/big-tech-faces-heat-chinas-deepseek-sows-doubts-billion-dollar-spending-2025-01-27/ >>

models has tended to grow by 2.4 times per year, but likely will increase baring a new method as seen in the ballooning costs of ChatGPT 5.[4]

Yet, is distillation IP theft? There is a difference of opinion this committee must address. According to the White House and OpenAI, distillation is a new form of IP theft.[5] According to a study by the US patent office there are divergent views of whether AI generated content can be copyrighted protected.[6] When distillation takes advantage of techniques like unbounded consumption attacks, it almost certainly violates the terms of service.

Regardless in an agentic era the central question is whether AI output counts as "creative content." Do lines of code have agency to produce original content? The legal community is split. AI models are trained with scrapped data - massive amounts of data that increases with each new version - which is why groups have sued copies like OpenAI claiming copyright infringement by multiple organizations including the *New York Times*.[7]

Challenge 2: Deterring Cyber Espionage in the Era of Agentic AI

Beyond legal questions about distillation techniques, there are major concerns about the depth of Chinese APT groups penetration into the modern IT infrastructure and cloud service providers alongside old fashion IP theft.[8] China's demonstrated track record of cyber espionage could further increase its ability to collect the mass amounts of data it needs to train new AI models even when firms seek to deny access.[9] Take the case of SilkTyphoon.[10] Since 2024, this group has used stolen API keys and other credentials to collect data of interest to the Chinese government. Accessing privileged data could allow Chinese researchers the ability to tailor generative AI models.

Here there is less legally gray area. Rampant cyber espionage, especially when it is linked to advancing narrow commercial interests, is illegal including under the Computer Fraud and Abuse Act (CFAA). The challenge is enforcement. How can the US make it more difficult to

---

[4] Ben Cottier et al "How Much Does It Cost to Train Frontier AI Models?" *EpochAI* June 3, 2024 <<https://epoch.ai/blog/how-much-does-it-cost-to-train-frontier-ai-models>>

[5] aura Italiano and Natalie Musucemi "OpenAI has Little Legal Recourse Against DeepSeek Tech Law Experts Say" Yahoo News January 31, 2025 <<https://www.yahoo.com/news/openai-little-legal-recourse-against-150858401.html?guce_referrer=aHR0cHM6Ly93d3cud2luc3Rvbi5jb20v&guce_referrer_sig=AQAAAArXZc5imJWVNSHJ_92vh3Cvxiyr89PZUWLeOhPKcDaW6uO1YPI_wGC-GADRHUbZStcRS8RKlIABBgYth54UWMX5fqueIV86YSBPgOlMvkVpDYXMJgIo5xaszIM8M72u7uyk_P8VvEjrKZsUe4eRU5WaVN2ydtoZTtWJNnH3BZBo>>

[6] United States Copyright Office. *Copyright and Artificial Intelligence Part 2: Copyrightability* January 2025 <<https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-2-Copyrightability-Report.pdf>>

[7] "Judge Allows Newspaper Copyright Lawsuit against OpenAI to Proceed" *AP* March 26, 2025 <<https://apnews.com/article/nyt-openai-copyright-lawsuit-chatgpt-cc19ef2cf3f23343738e892b60d6d7a6 >>

[8] Billy Perrigo "Every AI Datacenter is Vulnerbale to Chinese Espionage" *Time* April 22, 2025 << https://time.com/7279123/ai-datacenter-superintelligence-china-trump-report/>>

[9] Brandon Valeriano, Benjamin Jensen, Ryan Maness. *Cyber Strategy: the Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018).

[10] Jai Vijayan "China's Silk Typhoon APT Shifts to IT Supply Chain Attacks" *Darkreading* March 5, 2025 <https://www.darkreading.com/remote-workforce/china-silk-typhoon-it-supply-chain-attacks>

steal US data? To date, and despite monumental past efforts by Congress to include the U.S. Cyberspace Solarium Commission, America has yet to find the right suite of mechanisms to deter mass cyber espionage.[11]

Second, the semiconductor industry provides the essential hardware foundation upon which the entire AI ecosystem is built. Consequently, intellectual property related to semiconductor design and manufacturing is a prime target for theft, particularly by nations seeking to rapidly advance their domestic capabilities. The case involving ASML, the world-leading Dutch producer of photolithography equipment crucial for advanced chipmaking, and entities linked to China, illustrates this threat vividly. ASML sued Xtal Inc., a Silicon Valley startup founded by former ASML engineer Zongchang Yu, for stealing trade secrets and won over $800 million.[12] Sadly, the settlement came after individuals linked to XTAL had already stolen over 2 million lines of code.[13] The stolen IP was directly linked to DJEL, who the Chinese government gave approval to under a program known as "little giants."[14] As a result, ASML – a maker of advanced extreme ultraviolet lithography systems key to cutting-edge chips – asked customers not to do business with DJEL.

This case reveals several critical vulnerabilities. First, it highlights the targeting of extremely specialized and foundational technology – computational lithography optimization software – the compromise of which can have cascading effects throughout the technology ecosystem by enabling the production of more advanced semiconductors essential for AI. Second, the alleged use of parallel corporate entities in different jurisdictions (Xtal in the US, DJEL in China) points to a sophisticated method for circumventing legal accountability and facilitating cross-border IP transfer. Third, the apparent state endorsement of DJEL through "little giant" status and investment *after* its affiliate was found liable for massive IP theft severely undermines the deterrent effect of civil litigation and monetary damages alone. It suggests that such activities might be viewed as contributing to national technological goals, thereby insulating perpetrators from consequences within their home jurisdiction. Fourth, ASML's reported difficulties in investigating DJEL directly in China and its recourse to warning customers underscore the practical challenges of international IP enforcement, particularly against entities potentially shielded by foreign governments, necessitating stronger government-to-government mechanisms.

Last, there is growing evidence that state-linked entities in China are trying to exploit AI foundation models associated with U.S. firms for malicious purposes. Google has published

---

[11] Montgomery, M., B. Jensen, E. D. Borghard, J. Costello, V. Cornfeld, C. Simpson, and B. Valeriano. 2020. Cyberspace Solarium Commission Report. Washington, DC. https://www.solarium.gov/report; Brandon Valeriano and Benjamin Jensen "Building a National Cyber Strategy: The Process and Implications of the Cyberspace Solarium Commission Report" *IEEE 13th International Conference*, 2021 <<https://ieeexplore.ieee.org/document/9467806>>

[12] "ASML Says Ex-Employeeds in China Stole Chip Data" Bloomberg February 15, 2023 << ASML Says Ex-Employee in China Stole Chip Data - Bloomberg>>

[13] "Engineer Who Fled Charges of Stealing Chip Technology in US Now Thrives in China" CSET June 6, 2022 < Engineer Who Fled Charges of Stealing Chip Technology in US Now Thrives in China | Center for Security and Emerging Technology>>

[14] "ASML Warns Chinese Rival May Be Infringing Its Trade Secrets" Data Center Knowledge February 10, 2022 << ASML Warns Chinese Rival May Be Infringing Its Trade Secrets>>

evidence of state-based actors in China seeking to exploit its Gemini model to refine propaganda as well as enhance its cyber capabilities, including using generative AI to obtain deeper access to target networks through privilege escalation, data exfiltration, and detection evasion.[15]

Challenge 3: The Futility of Export Restrictions

Recent reports have demonstrated the futility of existing export controls to limit AI advances in China.[16] Despite U.S. restrictions, China has continued to access high-end export controlled chips.[17] These shadow market includes using third-party firms.[18] When combined with domestic investments as part of the PRC's civil-military fusion policy, this illicit activity ensures that the CCP has access to the computational power and IP required to build new generative AI models like DeepSeek.[19]

While export controls remain an important tool to slow adversary access to sensitive technologies, they have proven increasingly ineffective in the AI competition with China. The Biden administration's AI Diffusion Policy, introduced in 2025 to regulate the global spread of advanced AI systems, exemplifies both the necessity and the limits of this approach.[20] By categorizing countries into tiers, the policy aims to prevent adversaries like China from acquiring advanced chips, model weights, and critical software. Yet Beijing's playbook is not reliant on fair-market purchases alone. Chinese firms routinely evade restrictions through intermediaries, global subsidiaries, and gray market channels. They optimize AI workloads on restricted chips, leverage vast pools of open-source AI research, and accelerate indigenous semiconductor development subsidized by the state. These realities mean that while the AI Diffusion Policy may impose temporary friction, it does little to fundamentally constrain China's long-term trajectory. In a race defined by rapid innovation cycles and aggressive state backing, speed bumps are not barriers. For this reason, President Trump is right to explore significant changes to the policy.[21]

Moreover, policies like AI Diffusion risk harming U.S. technology leadership more than degrading China's ambitions. Export restrictions deny American companies access to lucrative

---

[15] Google Threat Intelligence Group. Adversial Misuse of Generative AI. January 29, 2025 << https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai>>

[16] Ritwik Gupta, Leah Walker, and Andrew Reddie" Whack-a-Chip: The Futility of Hardware-Centric Export Controls" arXiv 2411. <<https://arxiv.org/pdf/2411.14425>>

[17] Josh Ye, David Kirton, and Chen Li "Inside China's Underground Market for High-end NVIDIA AI Chips" *Reuters* June 20, 2023 << https://www.reuters.com/technology/inside-chinas-underground-market-high-end-nvidia-ai-chips-2023-06-19/>>

[18] Jack Burnham "Seeking Decisive Edge, China Uses Third-Party Countries to Circumvent U.S. AI Export Controls" *Foundation for Defense of Democracy,* March 4, 2025 << https://www.fdd.org/analysis/policy_briefs/2025/03/04/seeking-decisive-edge-china-uses-third-party-countries-to-circumvent-u-s-ai-export-controls/>>

[19] Kenneth Ong "China's Defiant Chip Strategy" FPRI June 28, 2024 << https://www.fpri.org/article/2024/06/chinas-defiant-chip-strategy/>>

[20] Matt Bracken "Biden Administration Unveils Export Controls on AI Models, Chips" *Fedscoop* January 13, 2025 << https://fedscoop.com/commerce-ai-diffusion-rule-biden-admin-industry-security/>>

[21] Karen Freifeld "Trump officials eye changes to Biden's AI chip export rule, sources say" *Reuters* April 29, 2025 << https://www.reuters.com/world/china/trump-officials-eye-changes-bidens-ai-chip-export-rule-sources-say-2025-04-29/>>

markets, particularly in fast-growing AI sectors, while foreign competitors — less burdened by restrictions — fill the vacuum. Revenue losses erode the resources U.S. firms reinvest into frontier R&D, weakening long-term global competitiveness. Leading voices in the AI hardware ecosystem, such as NVIDIA**,** have strongly criticized the Biden Administration's AI Diffusion rule as regulatory overreach that risks derailing innovation and ceding U.S. technological advantage. As NVIDIA argued, for decades, America's strength has come from fostering open and competitive computing and software ecosystems — not dictating design, sales, and global market access.[22] The company warns that the new rule, drafted with minimal transparency, seeks to impose sweeping government control over how semiconductors, computers, and software are marketed worldwide — restricting even mainstream technologies widely used in gaming PCs and consumer devices. Cloaked in national security language, such restrictions, they argue, will do little to stop China while directly undercutting U.S. global competitiveness and stifling the innovation that fuels economic growth and American influence.

Simply put, defensive measures like AI Diffusion, when deployed in isolation, can backfire: they limit U.S. firms, strain alliances, and slow innovation without stopping China's systemic theft and replication efforts. To be effective, export controls must be paired with offensive measures — targeting theft, disrupting circumvention, and degrading stolen IP. Without this shift, current policies risk becoming self-imposed constraints while Beijing accelerates unchecked.

Taken together these challenges suggest three broad categories of action Congress can help set in motion to ensure the US retains the commanding heights in the coming agentic era.

1. Modernize Intellectual Property Protections for the AI Era

The first priority must be addressing the legal and regulatory blind spots surrounding intellectual property in an agentic economy. As this subcommittee's important prior work on digital copyright and platform regulation has shown, emerging technologies often challenge legacy legal frameworks. Techniques like model distillation and unbounded consumption attacks—where API outputs are systematically harvested to train rival AI models—undermine the fundamental economics of AI innovation. These attacks are not only breaches of contract but strike at the intellectual core of American firms investing billions in foundation models. Congress should expand existing IP protections to clarify the legal status of AI-generated outputs, develop new statutory tools to criminalize intentional distillation that violates terms of service, and empower firms to take action against bad actors. Further, to avoid driving these activities offshore, the subcommittee should coordinate with counterparts in Commerce and Foreign Affairs to pursue international agreements that criminalize unauthorized model replication, creating unified global standards against this growing threat.

[22] Ned Finkle "NVIDA Statement on the Biden Administration's Misguided AI Diffusion Rule" *NVIDA* January 13, 2025 << https://blogs.nvidia.com/blog/ai-policy/>>

2. Strengthen Cybersecurity and Treat AI Companies as Critical Infrastructure

Second, cybersecurity must become a central pillar in defending U.S. AI leadership. While distillation attacks exploit legal gaps, Chinese espionage campaigns exploit technical vulnerabilities, including stolen API keys, cloud service intrusions, and access to development pipelines. This is not simply a civil issue — it is a national security threat. Congress should consider tax credits and other market-based incentives to encourage AI firms to increase their cyber defenses, invest in anomaly detection, and enhance user verification systems. The subcommittee should also work with counterparts on Homeland Security to ensure that AI firms are formally recognized as part of U.S. critical infrastructure under CISA's framework. Doing so would unlock a broader range of federal support, including enhanced threat intelligence sharing, voluntary cybersecurity performance goals, and rapid incident response assistance. Given the evidence of state-backed actors targeting these firms to advance Chinese industrial policy, AI companies must be treated not just as technology providers, but as pillars of national resilience.

3. Escalate to Active Defense and Offensive Operations Against Systemic IP Theft

Finally, the United States must move from passive protection to active disruption. Defensive tools alone will not deter a nation like China, which uses a coordinated state-backed strategy combining espionage, legal loopholes, and market coercion. As a first step, Congress should ensure that the Intelligence Community and law enforcement prioritize collection on PRC IP theft campaigns, with a mandate to declassify evidence where possible. Providing DOJ and allied nations' legal authorities with clear, court-admissible intelligence on state-directed theft will allow for more aggressive prosecution strategies and multilateral lawfare efforts. Diplomacy and technical standards-setting must also become offensive tools — rallying allies to adopt higher standards, coordinate enforcement, and close legal loopholes that allow Chinese firms to exploit jurisdictional arbitrage. In the most extreme cases, covert action should not be off the table. Just as the U.S. used software sabotage and misinformation programs in the 1980s to slow Soviet industrial espionage, tailored offensive cyber operations, data poisoning, and supply chain disruption efforts should be considered to degrade and delay the use of stolen U.S. intellectual property. In short, America cannot win this contest through defense alone. Restoring deterrence requires imposing real costs on state-backed IP thieves and making the economic and political risks of this strategy unbearable for Beijing and its proxies.

Why We Must Win the Agentic AI Race

At its core, this is not just a debate about intellectual property or cybersecurity. It is about strategic competition — and whether free societies will define the AI century or cede it to authoritarian regimes that view knowledge as power and power as control.

AI is no longer just a tool. We are entering the era of agentic AI — systems capable of generating new knowledge, accelerating scientific discovery, and shaping human decision-making at scale. Whoever leads in this domain will write the rules of the emerging international order. Beijing understands this. That is why China is not merely stealing technology opportunistically — it is waging a systematic campaign to siphon intellectual property, circumvent export controls, and exploit legal and technical gaps to build competitive AI ecosystems.

If China wins this race, AI will not become a catalyst for human flourishing. It will become a mechanism for surveillance, coercion, and influence. But if the United States and its allies prevail — if we defend IP, secure our digital frontiers, and go on offense against theft — AI can unlock new frontiers of growth, creativity, and global problem-solving. Free societies will innovate faster and more responsibly. Markets will remain open. Science will advance unshackled by censorship or central control.

That is why the stakes could not be higher. This is about more than defending the bottom line of U.S. firms — it is about defending a model of governance built on liberty and openness. History will not remember the lawsuits or regulations that defined the margins of this fight. It will remember whether we acted boldly enough to keep the commanding heights of the AI revolution in the hands of those who believe knowledge should empower, not oppress.

We cannot afford to lose the AI century to regimes that see agentic AI as the ultimate instrument of authoritarian control. The time to act — and to compete — is now.