PUBLIC COMMENT: FOUNDATION FOR DEFENSE OF DEMOCRACIES

Department of Commerce
Bureau of Industry and Security

Framework for Artificial Intelligence Diffusion FR Parts 732, 734, 740, 742, 744, 748, 750, 762, 772, and 774

[Docket No. 250107-0007]
RIN 0694-AJ90

AUTHORS

Craig Singleton
Senior Director, FDD's China Program

Jack Burnham
Research Analyst, FDD's China Program

Leah Siskind
AI Research Fellow, FDD's Center on Cyber and Technology Innovation

Johanna Yang
Research and Editorial Associate, FDD's Center on Cyber and Technology Innovation

Washington, DC
May 15, 2025

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

America's strategic rivalry with China will increasingly hinge on each country's success in translating scientific and technological innovation into military and economic supremacy — a race which now firmly centers on artificial intelligence (AI).

In a bid to displace Washington as the leading global power, Beijing has poured resources into developing and deploying AI across all facets of Chinese society — all with the aim of strengthening its military prowess and economic potency. Having perceived AI as a crucial future technology, the Chinese Communist Party (CCP) has constructed a series of national champions across its entire domestic AI industry, seeking both to dominate upstream inputs and to spur global proliferation.[1]

Beijing has paired these efforts with a growth strategy aimed at aggressively capturing global market share. Chinese national champions promote open-source AI as a foundation for foreign developers seeking low-cost access to advanced models, while the CCP has embraced the "democratization" of AI in multilateral fora.[2]

These efforts directly serve Beijing's geopolitical ambitions by bolstering its military strength and enhancing its push for industrial self-reliance. The People's Liberation Army (PLA) has raced to integrate AI into its military platforms, command and control systems, and training programs.[3] Chinese firms, often backed by state subsidies, have increasingly used AI both to retool traditional industries, such as heavy manufacturing, and to build new engines of economic growth, such as biotechnology and autonomous robotics.[4]

---

[1] Stephen Ezell, "How Innovative Is China in Semiconductors?" *Information Technology and Innovation Foundation*, August 19, 2024. (https://itif.org/publications/2024/08/19/how-innovative-is-china-in-semiconductors); Jessica Dawson, Tarah Wheeler, "How To Tackle The Data Collection Behind China's AI Ambitions," *Brookings Institution*, April 29, 2022. (https://www.brookings.edu/articles/how-to-tackle-the-data-collection-behind-chinas-ai-ambitions); Zeyi Yang, "Here's How DeepSeek Censorship Actually Works—and How to Get Around It," *Wired*, January 31, 2025. (https://www.wired.com/story/deepseek-censorship)

[2] Catherine Thorbecke, "China's Embrace of Open-Source AI Will Tip the Scales," *Bloomberg*, March 6, 2025. (https://www.bloomberg.com/opinion/articles/2025-03-06/china-s-embrace-of-open-source-ai-will-tip-the-scales); Fiona Alexander, "UN Attempts AI Power Grab. The West is Unhappy," *Center for European Policy Analysis*, July 24, 2024. (https://cepa.org/article/un-attempts-ai-power-grab-the-west-is-unhappy)

[3] Jacob Stokes, "Military Artificial Intelligence, the People's Liberation Army, and U.S.-China Strategic Competition," *Center for a New American Security*, February 1, 2024. (https://www.cnas.org/publications/congressional-testimony/military-artificial-intelligence-the-peoples-liberation-army-and-u-s-china-strategic-competition); Koichiro Takagi, "Is the PLA Overestimating the Potential of Artificial Intelligence?" *National Defense University*, January 27, 2025. (https://www.ndu.edu/News/Article-View/Article/4116123/is-the-pla-overestimating-the-potential-of-artificial-intelligence); Elsa B. Kania and Ian Burns McCaslin, "Learning Warfare From The Laboratory—China's Progression In Wargaming And Opposing Force Training," *Institute for the Study of War*, September 2021. (https://www.understandingwar.org/report/learning-warfare-laboratory-china%E2%80%99s-progression-wargaming-and-opposing-force-training)

[4] Alex He, "In Developing AI, China Takes the Industrial Route," *Centre for International Governance Innovation*, August 12, 2024. (https://www.cigionline.org/articles/in-developing-ai-china-takes-the-industrial-route); Craig Singleton, "Biotech Battlefield: Weaponizing Innovation in the Age of Genomics," *Foundation for Defense of Democracies*, January 15, 2025. (https://www.fdd.org/analysis/2025/01/15/biotech-battlefield); Katrina Northrop and Lyric Li, "China Wants To Lead The World In Robots — From Dogs To Dancers," *The Washington Post*, March 29, 2025. (https://www.washingtonpost.com/world/2025/03/29/china-unitree-ai-robotics-revolution); Jack Burnham

These trends pose a distinct risk to U.S. national security, threatening the future prosperity of the American economy and undermining the country's military strength. To prevent American innovation from falling into the hands of an adversary, the Bureau of Industry and Security (BIS) should institute stringent criteria to screen foreign customers seeking to purchase computing power. These criteria would simultaneously tighten export controls on countries that pose a heightened diversion risk while relaxing purchasing restrictions for U.S. allies and partners working to counter Chinese economic statecraft.

BIS should define the criteria required to prevent the diversion of advanced technologies. These criteria should aim to cover all aspects of countries' respective AI and science and technology ecosystems, including cybersecurity measures, foreign investment screening, export controls, and academic research security. This approach would ensure clarity for U.S. allies and partners seeking to gain access to greater quantities of computing power. It would also strengthen measures to prevent the diversion of cutting-edge innovation to China.

BIS should define the requirements necessary to demonstrate a commitment to upholding U.S. foreign policy interests. These requirements should focus on furthering U.S. national interests, with an emphasis on contributing to the national security of the United States via technological cooperation and providing a free and open global marketplace for AI innovation.

This public comment will provide further detail into the threat China's AI industry poses to U.S. national security. It will also offer detailed recommendations to strengthen the current Framework for AI Diffusion.

Overview of the Threat from the People's Republic of China

Seeking to supplant the United States as a leading global power, China has poured substantial financial and technical resources into AI research and development with the aim of leveraging its innovations against its adversaries.

Beijing has released a flurry of plans to integrate AI into all facets of its military and economy. Over the past several years, the PLA has steadily released military doctrines predicated on the operational concept of "intelligentized warfare," which envisions the PLA using AI to coordinate and launch precision strikes against a near-peer adversary's command-and-control infrastructure, rapidly blunting the enemy's capacity to deploy forces.[5] This concept has informed the PLA's efforts to integrate AI into its major weapons platforms and combat capabilities as well as non-combat operations such as sustaining military hospitals and improving logistical planning.[6]

---

and Johanna Yang, "U.S. at Risk of Falling Behind China in Biotechnology," *Foundation for Defense of Democracies*, April 15, 2025. (https://www.fdd.org/analysis/policy_briefs/2025/04/15/u-s-at-risk-of-falling-behind-china-in-biotechnology)

[5] U.S. Department of Defense, "Military and Security Developments Involving the People's Republic of China, 2024," December 18, 2024. (https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF); Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, "People's Liberation Army Operational Concepts," *RAND*, September 29, 2020. (https://www.rand.org/pubs/research_reports/RRA394-1.html)

[6] Jacob Stokes, "Military Artificial Intelligence, the People's Liberation Army, and U.S.-China Strategic Competition," *Center for a New American Security*, February 1, 2024. (https://www.cnas.org/publications/congressional-testimony/military-artificial-intelligence-the-peoples-liberation-

Recognizing its lack of combat experience, the PLA has also integrated AI into its training regimes, allowing officers to simulate the experience of battlefield command.[7]

Confronting a domestic economy mired in structural malaise, the CCP views AI as a potential growth multiplier, transforming its overburdened manufacturing sector and bolstering pre-existing investments in emerging sectors. Under the slogan of "New Quality Productive Forces," Beijing has raced to integrate AI into a host of designated future industries that the CCP deems critical to ensuring China's continued economic growth.[8] Following this directive and looking to move up global value chains, Chinese factories have integrated AI to rapidly upgrade their technical capabilities, while other industries seek to enhance productivity and gain an advantage within hypercompetitive domestic markets.[9] These efforts have also been integrated into longer-standing economic programs, such as biotechnology, quantum computing, material sciences, and energy production.

These trends pose an acute threat to U.S. national security by threatening to accelerate Beijing's military modernization program while enhancing its economic prowess. Having engaged in the fastest military build-up of any nation since the Second World War, the PLA seeks to use AI to fully transform into a modern military. Rather than rely on its overwhelming quantitative edge in fleet tonnage, magazine depth, and manpower to deter and defeat its adversaries, the PLA may further its emerging qualitative edge in precision strikes, drones, and space-based assets to gain a decisive advantage over a near-peer competitor.[10] In addition to direct technology integration,

---

army-and-u-s-china-strategic-competition); Jack Burnham, "China's Military Reportedly Deploys DeepSeek AI for Non-Combat Duties," *Foundation for Defense of Democracies*, March 27, 2025. (https://www.fdd.org/analysis/policy_briefs/2025/03/27/chinas-military-reportedly-deploys-deepseek-ai-for-non-combat-duties)

[7] Elsa B. Kania and Ian Burns McCaslin, "Learning Warfare from The Laboratory—China's Progression in Wargaming and Opposing Force Training," *Institute for the Study of War*, September 2021. (https://www.understandingwar.org/report/learning-warfare-laboratory-china%E2%80%99s-progression-wargaming-and-opposing-force-training); Dennis J. Blasko, "The Chinese Military Speaks to Itself, Revealing Doubts," *War on the Rocks*, February 18, 2019. (https://warontherocks.com/2019/02/the-chinese-military-speaks-to-itself-revealing-doubts)

[8] Arthur Kroeber, "Unleashing 'New Quality Productive Forces': China's Strategy for Technology-Led Growth," *Brookings Institution*, June 4, 2024. (https://www.brookings.edu/articles/unleashing-new-quality-productive-forces-chinas-strategy-for-technology-led-growth); Craig Singleton and Amaya Marion, "Safeguarding U.S. Interests in the Face of China's 'New Productive Forces' Strategy," *Foundation for Defense of Democracies*, May 2, 2024. (https://www.fdd.org/analysis/2024/05/02/safeguarding-u-s-interests-in-the-face-of-chinas-new-productive-forces-strategy)

[9] Hodan Omaar, "How Innovative Is China in AI?" *Information Technology and Innovation Foundation,* August 26, 2024. (https://itif.org/publications/2024/08/26/how-innovative-is-china-in-ai); Hanna Dohmen, "Assessing China's AI Development And Forecasting Its Future Tech Priorities," *Atlantic Council*, September 18, 2024. (https://www.atlanticcouncil.org/content-series/strategic-insights-memos/assessing-chinas-ai-development-and-forecasting-its-future-tech-priorities); Wendy Chang and Antonia Hmaidi, "China's EVs Are AI-On-Wheels, While European Cars Are Still Trying To Get Smart," *Mercator Institute for China Studies*, August 1, 2024. (https://merics.org/en/comment/chinas-evs-are-ai-wheels-while-european-cars-are-still-trying-get-smart)

[10] Ryan Brobst and Bradley Bowman, "Arsenal of Democracy: Arming Taiwan, Ukraine, and Israel While Strengthening the U.S. Industrial Base," *Foundation for Defense of Democracies*, April 7, 2025. (https://www.fdd.org/analysis/2025/04/07/arsenal-of-democracy); Michèle Flournoy and Gabrielle Chefitz, "Sharpening the U.S. Military's Edge: Critical Steps for the Next Administration," *Center for a New American Security*, July 13, 2020. (https://www.cnas.org/publications/commentary/sharpening-the-u-s-militarys-edge-critical-steps-for-the-next-administration); U.S. Department of Defense, "Military and Security Developments Involving the People's Republic of China, 2024," December 18, 2024. (https://media.defense.gov/2024/Dec/18/2003615520/-1/-

Beijing's program of military-civil fusion (MCF) will ensure the rapid weaponization of any private-sector innovation.[11] Combined with Beijing's persistent pursuit of non-market practices, the mass adoption of advanced AI may allow Chinese firms to gain an even greater asymmetrical advantage over their American competitors, weakening the U.S. economy.

Evaluation of the Risk Posed by Chinese Efforts to Circumvent Current U.S. AI Export Controls

To fuel its AI industry, China has worked tirelessly to circumvent previous U.S. export controls on advanced AI components via a combination of licit and illicit means. Having benefited from state investments in the country's science and technology base and sponsored repressive data-collection efforts, Chinese firms have continuously improved their capacity to produce key AI inputs, including advanced graphic processing units (GPUs), hyperscalers, and large language models (LLMs).[12] This investment has surged in the wake of DeepSeek's release, which contributed to a dramatic increase in Chinese technology stock valuations and has prompted a rash of data center construction among leading Chinese AI firms.[13]

Beijing's reliance on open-source models to drive AI innovation also offers an avenue to circumvent current U.S. export controls. Unlike closed-source models, which are typically more powerful but cannot be easily modified by outside users, open-source models can be readily adopted by a broad range of clients and cheaply integrated into other applications.[14] Both Chinese national champions and smaller developers have released a series of ever-more advanced open-source models, led by DeepSeek, which released an open-source LLM and reasoning model that performed on par with major Western closed-sourced models.[15] Along with allowing Chinese firms to install their products as key nodes within the global AI stack, this

---

1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF)

[11] Emily de La Bruyère and Nathan Picarsic, "Defusing Military-Civil Fusion: The Need to Identify and Respond to Chinese Military Companies," *Foundation for Defense of Democracies*, May 27, 2021. (https://www.fdd.org/analysis/2021/05/26/defusing-military-civil-fusion)

[12] "China Steps Up Support for Tech Sector as AI Enthusiasm Soars," *Bloomberg*, March 6, 2025. (https://www.bloomberg.com/news/articles/2025-03-06/china-steps-up-support-for-tech-sector-as-ai-enthusiasm-soars); Stephen Ezell, "How Innovative Is China in Semiconductors?" *Information Technology and Innovation Foundation*, August 19, 2024. (https://itif.org/publications/2024/08/19/how-innovative-is-china-in-semiconductors); Emily de La Bruyère and Nathan Picarsic, "China's Quest For Asymmetric Dominance In Data Centers," *Foundation for Defense of Democracies*, June 25, 2024. (https://www.fdd.org/analysis/op_eds/2024/06/25/chinas-quest-for-asymmetric-dominance-in-data-centers); Jessica Dawson, Tarah Wheeler, "How To Tackle The Data Collection Behind China's AI Ambitions," *Brookings Institution*, April 29, 2022. (https://www.brookings.edu/articles/how-to-tackle-the-data-collection-behind-chinas-ai-ambitions)

[13] Evelyn Cheng, "DeepSeek AI cranks open the spigots on Chinese venture capital," *CNBC*, March 11, 2025. (https://www.cnbc.com/2025/03/12/deepseek-ai-cranks-open-the-spigots-on-chinese-venture-capital.html); Jack Burnham, "China's Military Reportedly Deploys DeepSeek AI for Non-Combat Duties," *Foundation for Defense of Democracies*, March 27, 2025. (https://www.fdd.org/analysis/policy_briefs/2025/03/27/chinas-military-reportedly-deploys-deepseek-ai-for-non-combat-duties)

[14] Catherine Thorbecke, "China's Embrace of Open-Source AI Will Tip the Scales," *Bloomberg*, March 6, 2025. (https://www.bloomberg.com/opinion/articles/2025-03-06/china-s-embrace-of-open-source-ai-will-tip-the-scales)

[15] Elizabeth Gibney, "China's Cheap, Open AI Model DeepSeek Thrills Scientists," *Nature*, January 23, 2025. (https://www.nature.com/articles/d41586-025-00229-6); Evelyn Cheng, "DeepSeek AI Cranks Open the Spigots on Chinese Venture Capital," *CNBC*, March 11, 2025. (https://www.cnbc.com/2025/03/12/deepseek-ai-cranks-open-the-spigots-on-chinese-venture-capital.html)

trend has ensured that Chinese firms can benefit from global AI development efforts, particularly outside the West.

These efforts complement Beijing's aim to spur the development of its own AI industry by preemptively circumventing potential Western chokepoints. Through a range of strategic investments, particularly within the Gulf region, China has gained access to other countries' AI ecosystems, from university laboratories to data centers to restricted AI components.[16] These investments, coupled with Chinese national security laws such as the 2017 National Intelligence Law, which mandates that private Chinese firms under Chinese jurisdiction cooperate with authorities, allow Beijing to gain influence over the proliferation of emerging technologies.[17] This strategic outreach has also allowed Chinese firms to maintain steady access to Western capital and knowledge, accelerating the pace of domestic innovation.

Likewise, Beijing continues to support the "democratization" of AI within international multilateral fora, offering financial and technical support to interested partners while accusing the West of monopolizing access to emerging technologies.[18] These efforts complement Beijing's ongoing drive to influence global technical standards and decision-making bodies to underpin its technological rise, allowing China to maintain access to critical components by circumventing U.S. export controls.

Along with leveraging these connections, Chinese firms have benefited from a range of sophisticated smuggling networks run through neighboring countries. Relying on front companies and cooperative foreign nationals, Chinese firms have gained access to components designated for authorized Nvidia regional customers, including servers containing hundreds of thousands of advanced chips.[19] These smuggling networks, along with allegations that Chinese models distill leading closed-source Western models, demonstrate the CCP's willingness to use extrajudicial means to further its technical prowess.[20]

---

[16] "China Tech Giants Eye Middle East for Growth Amid Rising Demand for Digital Infrastructure," *Middle East Monitor*, September 25, 2024. (https://www.middleeastmonitor.com/20240925-china-tech-giants-eye-middle-east-for-growth-amid-rising-demand-for-digital-infrastructure); Johanna Yang and Jack Burnham, "To Beat China, America Must Balance AI Innovation with National Security," *The Cipher Brief*, April 10, 2025. (https://www.thecipherbrief.com/column_article/to-beat-china-america-must-balance-ai-innovation-with-national-security)

[17] Craig Singleton and Mark Montgomery, "Laser Focus: Countering China's LiDAR Threat to U.S. Critical Infrastructure and Military Systems," *Foundation for Defense of Democracies*, December 2, 2024. (https://www.fdd.org/analysis/2024/12/02/laser-focus-countering-chinas-lidar-threat-to-u-s-critical-infrastructure-and-military-systems)

[18] Fiona Alexander, "UN Attempts AI Power Grab. The West is Unhappy," *Center for European Policy Analysis*, July 24, 2024. (https://cepa.org/article/un-attempts-ai-power-grab-the-west-is-unhappy)

[19] Jack Burnham, "Seeking Decisive Edge, China Uses Third-Party Countries to Circumvent U.S. AI Export Controls," *Foundation for Defense of Democracies*, 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)

[20] Mark Sweney, Dan Milmo, "OpenAI 'reviewing' allegations that its AI models were used to make DeepSeek," *The Guardian*, January 29, 2025. (https://www.theguardian.com/technology/2025/jan/29/openai-chatgpt-deepseek-china-us-ai-models)

Recommendations to Strengthen the Framework for AI Diffusion

To counter China's burgeoning AI sector, BIS should tighten export controls on critical components, including advanced GPUs and closed AI model weights that contain American technology or engineering, while ensuring that U.S. allies and partners that comply with stringent security restrictions can gain access to the necessary resources to develop their AI industries.

1. **The cybersecurity standards required for National Validated End User (NVEU)/Universal Validated End User (UVEU) certification should apply both to data centers and to their adjacent infrastructure.** This adjacent infrastructure includes systems used by third-party contractors, critical communications, and relevant edge devices, all of which Beijing's has targeted with malicious cyber operations. Moreover, these standards, which the National Security Agency sets, should be subject to periodic reviews and revisions in response to the threat landscape.

2. **BIS should offer priority access to countries based upon their foreign-investment screening mechanisms.** While recognizing regulatory divergences due to relevant international treaties, the Commerce Department should offer priority to interested countries that have a strong track record of adhering to U.S. economic security practices. Commerce should review the capacity of interested countries to monitor investments both upstream and downstream of AI development, such as research, manufacturing, and technology transfers. Moreover, to prevent adversarial states from using investments as a backdoor for espionage and sabotage, these reviews should extend to AI deployment, particularly in projects related to critical infrastructure, healthcare, and military-adjacent industries, all of which Chinese cyber intrusions have repeatedly targeted.

3. **BIS should offer priority access to countries based upon export control harmonization with the United States.** While supply chain management plans are currently required for Validated End User (VEU) accreditation, BIS should expand this standard to encompass secondary components, particularly those installed within close physical proximity of data centers, research laboratories, and other related settings.

4. **BIS should offer priority access to countries based upon their research security policies.** This issue has become more pressing as China continues to fund AI research and development programs at universities across the Gulf region, raising significant diversion risks due to the broader availability of cutting-edge Western technologies and deep capital markets. In response, licensing decisions should be predicated on recipients' research funding regulations, screening guidelines for international student visas, and capacity to maintain strict on-campus security measures to prevent unauthorized access to ongoing AI-related research programs.

5. **BIS should offer priority access to countries based upon their alignment with the foreign policy interests of the United States.** As demonstrated by both Israel and Ukraine, U.S. allies and partners can positively contribute to the Department of Defense's AI strategy, from improving intelligence, surveillance, and reconnaissance during counterinsurgency and conventional operations to deploying AI-enhanced unmanned aerial systems. With the United States now confronting a series of authoritarian powers

whose military capabilities have expanded rapidly over the past decade, tapping partners' innovations will improve the U.S. military's lethality and significantly contribute to its warfighting potential.

6. **BIS should offer priority access to countries based upon their commitment to a free and open marketplace for AI innovation.** While maintaining a focus on preventing diversion, BIS should modify these regulations to prioritize countries whose regulatory standards align with those of the United States, particularly regarding AI deployment. Along with providing an incentive to prevent discrimination against American firms, this approach will also prevent greater Chinese penetration into the global AI market by allowing Washington to capitalize on its current lead.

Conclusion

The CCP's efforts to develop advanced AI pose an acute threat to U.S. national security. BIS's initiatives to prevent AI diversion by tightening export controls while allowing U.S. allies and partners to gain access to advanced GPUs to build their indigenous capabilities are appropriate and critical to protect the United States.

Thank you for considering our comment, and we look forward to seeing how our input is incorporated into the final rule.