CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Statement before the
U.S.-China Economic and Security Review Commission

"China's Pursuit of Defense Technologies: implications for U.S. and Multilateral Export Control and Investment Screening Regimes"

A Testimony by:

Gregory C. Allen
Director, Wadhwani Center for AI and Advanced Technologies, CSIS

Thursday, April 13, 2023
419 Dirksen Senate office Building

Chairman Bartholomew, Vice Chairman Wong, and distinguished members of the commission, thank you for inviting me to testify in the proceedings today. My current employer, the Center for Strategic and International Studies (CSIS), does not take institutional policy positions. The views represented in this testimony are my own and should not be taken as representing those of my current or former employers.

I currently serve as the director of the Wadhwani Center for AI and Advanced Technologies at CSIS, where I have the privilege to lead a team conducting policy research at the intersection of technology and geopolitics. Prior to CSIS, I spent three years working at the United States Department of Defense (DoD) Joint Artificial Intelligence (AI) Center, where I most recently served as the director of strategy and policy. Among my diverse duties were to advise senior DoD officials and participate in interagency policymaking processes on policy issues related to China's AI sector. Additionally, during the 2021 Defense Policy Coordination Talks between the DoD and the People's Liberation Army (PLA), I was the DoD's representative in giving a presentation on reducing the risk of unintentional engagement and escalation related to military use of AI.

For my testimony today, I hope to offer a perspective informed by my direct experience working to accelerate DoD AI adoption, as well as my direct experience engaging with Chinese officials and experts on AI. In 2018 and 2019, I traveled to China on five separate trips to attend major diplomatic, military, and private-sector conferences focusing on artificial intelligence (AI). During these trips, I participated in a series of meetings with Chinese officials in China's Ministry of Foreign Affairs, leaders of China's military AI research organizations, Chinese foreign policy and military think tank experts, and corporate executives at Chinese AI companies.

As the United States' principal peer competitor in the field of technology, China has sought to expand in many emerging technology areas, foremost among them is the field of AI. As military competition with China gains increasing salience in our national security policy, U.S. leadership in the realm of military AI is not at all guaranteed. While the United States has important advantages, China may be able to quickly take the lead in government and military adoption of AI capabilities. This is an outcome that the United States should seek to prevent.

My testimony before this commission will attempt to provide an overview of how China perceives AI, how it develops AI, and, crucially, how it integrates AI into its security and military organizations. I will also address the U.S. and allied efforts to use export controls on semiconductor technology as a tool to influence the trajectory of China's AI sector. I will limit my remarks to those that are appropriate for an unclassified setting.

I. China's senior leaders see AI as foundational to the future of economic and military power.

In July 2017, China's State Council issued the New Generation Artificial Intelligence Development Plan (AIDP).[1] This document, as well as the issue of AI more generally, has received significant and sustained attention from the highest levels of China's leadership, including Xi Jinping, the general secretary of the Chinese Communist Party (CCP). Total Chinese national and local government spending on AI to implement this plan is not publicly disclosed, but it is clearly in the equivalent range of tens of billions of dollars. At least two Chinese regional governments have each committed to investing 100 billion yuan (~$14.7 billion in then-year exchange rates).[2] The opening paragraphs of the AIDP exemplify mainstream Chinese views regarding AI:

> AI has become a new focus of international competition. AI is a strategic technology that will lead in the future; the world's major developed countries are taking the development of AI as a major strategy to enhance national competitiveness and protect national security.

More recently, AI was the first technology priority listed in the Chinese government's five-year economic plan for 2021–2026.[3]

In addition to the AIDP and the five-year plan, AI also features prominently in China's most recent defense white paper, which in 2019 argued that,

> International military competition is undergoing historic changes. New and high-tech military technologies based on IT are developing rapidly. There is a prevailing trend to develop long-range precision, intelligent, stealthy or unmanned weaponry and equipment. War is evolving in form towards informationized warfare, and intelligentized warfare is on the horizon.[4]

---

[1] Graham Webster et al., "Full Translation: China's 'New Generation Artifical Intelligence Development Plan' (2017)," New America, August 1, 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

[2] Xinhua, "Shanghai to Set up Multi-Billion-Dollar Fund to Develop AI," *China Daily*, September 18, 2018, http://www.chinadaily.com.cn/a/201809/18/WS5ba0ade9a31033b4f4656be2.html"; and Meng Jing, "This Chinese City Plans a US$16 Billion Fund for AI Development," *South China Morning Post*, May 16, 2018, https://www.scmp.com/tech/innovation/article/2146428/tianjin-city-china-eyes-us16-billion-fund-ai-work-dwarfing-eus-plan."

[3] "Xi Jinping: 'Strive to Become the World's Primary Center for Science and High Ground for Innovation'," DigiChina, March 18, 2021, translation by Ben Murphy, Rogier Creemers, Elsa Kania, Paul Triolo, and Kevin Neville, edited with an introduction by Graham Webster, https://digichina.stanford.edu/work/xi-jinping-strive-to-become-the-worlds-primary-center-for-science-and-high-ground-for-innovation/.

[4] State Council Information Office, *China's National Defense in the New Era* (Beijing: Foreign Languages Press Co. Ltd, July 2019), English translation available at https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2019-07%20PRC%20White%20Paper%20on%20National%20Defense%20in%20the%20New%20Era.pdf?ver=akpbGkO5ogbDPPbflQkb5A%3d%3d.

China's military leadership believes that the dawn of AI-enabled intelligentized warfare (sometimes translated as "intelligentization") represents a military technology revolution on par with the mechanization and informatization revolutions of the twentieth century.[5]

"Informatization" is as it sounds—the expansion of computers for data analysis and networking, including in the precision-guided munitions revolution of the late twentieth century.

For "intelligentization," the DoD stated in the 2022 China Military Power Report,

> [People's Liberation Army] PLA strategists have stated new technologies will increase the speed and tempo of future warfare, and that operationalization of AI will be necessary to improve the speed and quality of information processing by reducing battlefield uncertainty and providing decision-making advantage over potential adversaries. The PLA is also exploring next-generation operational concepts for intelligentized warfare, such as attrition warfare by intelligent swarms, cross-domain mobile warfare, AI-based space confrontation, and cognitive control operations. The PLA considers unmanned systems to be critical intelligentized technologies, and is pursuing greater autonomy for unmanned aerial, surface, and underwater vehicles to enable manned and unmanned hybrid formations, swarm attacks, optimized logistic support, and disaggregated ISR, among other capabilities.[6]

This long list of AI-related capabilities that the PLA is pursuing is appropriate. It reflects the fact that AI is a general-purpose technology, analogous to electricity or computers. Today there are relatively few military capabilities used by the DoD that do not involve electricity or computers at some stage in their life cycle, whether design, manufacturing, operational use, or maintenance. But in the history of U.S. military technology adoption, some applications incorporated electricity and computers decades before others. A similar, though perhaps faster, story is unfolding in the U.S. and Chinese militaries today with respect to AI.

II. China's most significant national security application of AI is in domestic surveillance.
In recent years, China has initiated a brutal crackdown on residents of its Xinjiang province, predominantly targeting people of the Muslim Uighur minority. The Chinese government has installed an extraordinarily extensive AI-enabled system designed to surveil, censor, and constrain the actions of residents of Xinjiang. The ambition of this program has escalated dramatically over time, and elements of the program are now deployed in regions across China, not just Xinjiang.

This massive, unethical social experimentation has provided a wealth of funding, data, and operational experience for China's surveillance-industrial complex, including many companies at the forefront of Chinese AI development. iFlyTek, a leading Chinese provider of voice recognition and translation software, receives massive subsidies and revenue from the Chinese

[5] Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China* (Washington, DC: Department of Defense, 2021), https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF.
[6] United States Department of Defense.

government.[7] Since 2017, it has collaborated with the government in providing a so-called "voiceprint" system to identify and track residents.[8] SenseTime, a leading Chinese provider of facial recognition software, plays a similar role for facial tracking in surveillance footage.[9]This in-the-field testing provides real-life use cases and training data that allow both companies to advance in their development of and operational experience with AI technology.

The human rights and civil liberties implications of these large-scale AI deployments are enormous. However, they are a separate issue from what the systems signify in terms of the depth and breadth of capability in China's AI sector and the Chinese security establishment's ability to effectively tap that capability. Even if the use case of this AI system is morally horrifying, it is nonetheless technologically and operationally significant. The Chinese state's ability to deploy and scale AI to this extent in a matter of just a few years should give us pause. While the American private sector has made impressive leaps, most recently in the field of generative AI, the Chinese government has demonstrated a dramatic pace of public-sector AI adoption, itself a nontrivial administrative process.

III. China's efforts in domestic surveillance AI offer indirect benefits for military adoption. Although the Chinese Ministry of State Security (MSS) and local government police forces have shown enthusiasm for adopting AI as part of the CCP's domestic security and surveillance operations, it is not guaranteed that this technological success will carry over into the realm of military applications.

Modern machine-learning AI using deep neural networks offers the opportunity for incredible gains in system performance, but that performance depends on having large quantities of training data during development. Moreover, training data needs to closely resemble operational conditions.

In general, it is much easier to get such training data on commercial customers or domestic surveillance targets than from an enemy military, especially if friendly weapons systems and sensors do not often come within range of enemy ones. The most mature U.S. national security AI applications are ones such as AI-enabled analysis of satellite reconnaissance imagery. Even in peacetime, satellites get to take a lot of pictures of Russian and Chinese military forces, and those pictures can be digitally labeled by human experts to turn them into training data. Training data is what machine-learning AI systems learn from. The combination of a learning algorithm and training data is how AI systems learn to recognize what is in an image. But training data is generally application-specific. Training data for satellite image recognition typically only helps build satellite image recognition AI. One cannot magically use labeled satellite image data to train an AI for a missile's guidance computer (at least not with today's technology).

---

[7] Henny Sender, "China's IFlytek Raising up to $350m to Invest in AI," *Financial Times*, June 5, 2019, https://www.ft.com/content/d4dbbd18-81a8-11e9-b592-5fe435b57a3b.
[8] Will Knight, "MIT Cuts Ties With a Chinese AI Firm Amid Human Rights Concerns," *Wired*, April 21, 2020, https://www.wired.com/story/mit-cuts-ties-chinese-ai-firm-human-rights/.
[9] Johana Bhuiyan, "US Sanctioned China's Top Facial Recognition Firm over Uyghur Concerns. It Still Raised Millions," *The Guardian*, January 7, 2022, https://www.theguardian.com/world/2022/jan/06/china-sensetime-facial-recognition-uyghur-surveillance-us-sanctions; and Christian Shepherd, "China's SenseTime Sells out of Xinjiang Security Joint Venture," *Financial Times*, April 15, 2019, https://www.ft.com/content/38aa038a-5f4f-11e9-b285-3acd5d43599e.

Getting enough of the right sort of training data to incorporate modern AI into, say, a robotic tank's targeting computer, is a much tougher technical challenge. It is not impossible in principle, but in practice, there are far fewer opportunities to collect the right sort of training data unless your country is currently at war. This is critical to keep in mind in the context of China's widespread use of AI for domestic surveillance. China may have data advantages related to facial recognition for domestic surveillance applications or even commercial applications such as consumer finance, but these data sets have limited relevance for military applications. For some military AI applications, such as precision missile targeting or autonomous drone navigation, China may have no data advantage whatsoever compared with the United States.

Despite this, China's domestic AI deployment has supported military development in lasting, durable ways. For one, an entire generation of Chinese government officials now has experience with the benefits and drawbacks of an AI program and how to effectively administer it at large scale. Private sector corporations, such as iFlyTek and SenseTime, likewise gain experience and connections collaborating with the Chinese government, the CCP, and the Chinese military and national security establishments. Chinese companies such as iFlyTek and SenseTime routinely publish high-quality research and attend prestigious international conferences. Their research operates at or above the level of U.S. companies in the same AI sub-fields. This success—directly related to the massive quantities of data and operational experience that these firms get from participating in domestic surveillance—gives them an advantage in the field of technological development, as well as in access to investment capital, government revenue, and talent.

By contrast, in the United States, major tech firms do not routinely have the same depth of cooperation with our national security organizations in the field of AI. Part of this can be attributed to our commitment to democratic values and our societal choices not to pursue the types of unethical AI applications that are so widespread in China. However, U.S. national security agencies must continue making the needed reforms to deepen cooperation with leading commercial technology companies and accumulate relevant operational experience with AI.

IV. Unclassified information regarding China's research and adoption of military AI has important limitations, but available evidence suggests that China is pursuing development of AI-enabled lethal autonomous weapons.

I previously addressed the differences in developing military versus surveillance AI. Although China has boasted of competency in both, evidence on the extent of Chinese military AI adoption is significantly more limited, particularly at the unclassified level.

Chinese military AI systems are generally developed in secret until they are either sufficiently advanced to serve a deterrence purpose or to be part of military exports. The available sources in the public domain related to Chinese military AI adoption, such as military-affiliated newspapers and academic journals, are worth paying attention to but must be evaluated cautiously. These sources, by their very nature, cannot discuss the full view of China's military advancements and in many cases are individual opinions and speculation rather than official government policy. They may also be exaggerated to carry the Chinese military's desired messages about its own strength.

The best available indications, however, suggest that China's strategy is ambitious, moving beyond any sort of on-the-battlefield human supervision into increasingly autonomous AI-enabled warfare. For example, Zeng Yi, a senior executive at NORINCO, China's third-largest defense company, gave a public speech in 2018 in which he described his company's (and China's) expectations for the future implementation of AI weapons: "In future battlegrounds, there will be no people fighting."[10] Zeng predicted that by 2025 lethal autonomous weapons would be commonplace and said that his company believes ever-increasing military use of AI is "inevitable. . . . We are sure about the direction and that this is the future." I transcribed Zeng's comments (as provided by the simultaneous translators) as I was in attendance at the same conference. However, in the subsequently released transcript of the conference session, all mention of Zeng's presentation and participation was removed, likely indicating that the Chinese government censors had determined it was not in China's interest to have that information in the open.

Zeng's comments are consistent with ongoing Chinese autonomous military vehicle development programs and China's current approach to exports of military unmanned systems. China's government is already exporting many of its most advanced military aerial drones to Middle Eastern countries such as Saudi Arabia and the United Arab Emirates. China's government has stated that it also will export its next-generation stealth drones when those are available.[11]

Though many current-generation drones are primarily remotely operated, Chinese officials generally expect drones and military robotics to feature ever more extensive AI and autonomous capabilities in the future. Chinese weapons manufacturers are already selling armed drones that advertise significant amounts of combat autonomy. Ziyan, a Chinese military drone manufacturer, has sold its Blowfish A2 model to the UAE and in November 2019 reportedly was in negotiations with Saudi Arabia and Pakistan for Blowfish A2 sales.[12] Ziyan's website states that the 38-kg Blowfish A2 "autonomously performs more complex combat missions, including fixed-point timing detection, fixed-range reconnaissance, and targeted precision strikes."[13] Depending on customer preferences, Ziyan offers to equip the Blowfish A2 with either missiles or machine guns.

Beyond using AI for autonomous military robotics, China is also interested in AI capabilities for military command decisionmaking. Zeng Yi expressed some remarkable opinions on this subject, stating that today "mechanized equipment is just like the hand of the human body. In future intelligent wars, AI systems will be just like the brain of the human body." Zeng also said that "Intelligence supremacy will be the core of future warfare" and that "AI may completely change the current command structure, which is dominated by humans" to one that is dominated by an "AI cluster." Zeng did not elaborate on his claims, but they are consistent with published

[10] By revenue, NORINCO is the third-largest defense company in China and the ninth-largest worldwide. Gregory C. Allen, *Understanding China's AI Strategy* (Washington, DC: Center for New American Security, February 2019), https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy.
[11] Dake Kang and Christopher Bodeen, "China Unveils Stealth Combat Drone in Development," Associated Press, November 7, 2018, https://www.apnews.com/6b2d2857f73c4fa387379c16b0dc60b9.
[12] Ludovic Ehret, "China Steps up Drone Race with Stealth Aircraft," Phys.Org, November 9, 2018, https://phys.org/news/2018-11-china-drone-stealth-aircraft.html.
[13] Ziyan, "Blowfish A2 Product Overview."

thinking in some Chinese military circles. Several months after AlphaGo's momentous March 2016 victory over Lee Sedol, a publication by China's Central Military Commission Joint Operations Command Center argued that AlphaGo's victory "demonstrated the enormous potential of artificial intelligence in combat command, program deduction, and decisionmaking."[14]

V. The DoD has sought defense policy dialogues with the PLA on military AI risk reduction but has repeatedly been refused.

Machine learning, the technology paradigm at the heart of the modern AI revolution, brings with it not only opportunities for radically improved performance but also new failure modes. When it comes to traditional software, the U.S. military has decades of institutional muscle memory related to preventing technical accidents, but building machine learning systems that are reliable enough to be trusted in safety-critical or use-of-force applications is a newer challenge. To its credit, the DoD has devoted significant resources and attention to the problem: partnering with industry to make commercial AI test and evaluation capabilities more widely available, announcing AI ethics principles and releasing new guidelines and governance processes to ensure their robust implementation, updating longstanding DoD system safety standards to pay extra attention to machine learning failure modes, and funding a host of AI reliability and trustworthiness research efforts through organizations such as the Defense Advanced Research Projects Agency (DARPA).

However, even if the United States were somehow to successfully eliminate the risk of AI accidents in its own military systems—a bold and incredibly challenging goal—it still would not have solved risks to the United States from technical failures in Chinese military AI systems. What if a Chinese AI-enabled early warning system erroneously announces that U.S. forces are launching a surprise attack? The resulting Chinese strike—wrongly believed by China to be a counterattack—could be the opening salvo of a new war.

Substantive diplomacy on this topic is worth pursuing and, if successful, could meaningfully contribute to reducing the risk of a future U.S.-China conflict. There is loud public support in prominent Chinese venues for such a dialogue. However, during my tenure as the director of strategy and policy at the DoD Joint Artificial Intelligence Center, the DoD did just that, twice.[15] Both times the Chinese military refused to allow the topic on the agenda. In the second attempt, the Defense Policy Coordination Talks of 2021, I gave a presentation on U.S. military efforts to reduce AI risks associated with unintentional engagement and escalation. The PLA refused to discuss the issue.

It is important that such risk-reduction dialogues occur bilaterally between the DoD and the PLA, not just via the Chinese Ministry of Foreign Affairs' public proclamations at the United Nations. The Chinese Ministry of Foreign Affairs is not a direct analogue of the U.S. State Department, which complicates its ability to authoritatively speak on behalf of the PLA. In the

[14] Central Military Commission Joint Staff, "Accelerate the Construction of a Joint Operations Command System with Our Nation's Characteristics CMC Joint Operations Command Center," Seeking Truth, August 15, 2016.
[15] Gregory C. Allen, "One Key Challenge for Diplomacy on AI: China's Military Does Not Want to Talk," CSIS, *Commentary*, May 20, 2022, https://www.csis.org/analysis/one-key-challenge-diplomacy-ai-chinas-military-does-not-want-talk.

Chinese Lenninist system, the Chinese military is a part of the CCP, not the Chinese government, which controls the Chinese Ministry of Foreign Affairs. Though both organizations ultimately have the same leader—Xi Jinping is both the president of the People's Republic of China and chairman of the CCP—experience has shown that there is no substitute for direct DoD-PLA dialogue on military issues.

VI. The U.S. edge in advanced AI research does not necessarily translate to skill in adoption.

The United States is unquestionably the leader in developing the foundational science of AI. We have deeper reserves of institutional talent and knowledge. However, historically, it is not always true that the inventor of a cutting-edge technology or maker of a scientific discovery is its primary beneficiary.

Consider the case of stealth aircraft. Several of the key underlying scientific breakthroughs that enabled stealth technology originated in 1962 in the Soviet Union with research by Petr Ufimtsev, a physicist at the Moscow Institute for Radio Engineering. English translations of Ufimtsev's work were not available until 1971.[16] Despite having a nine-year head start, and later making an aggressive effort to replicate U.S. advances, the Soviet Union never successfully fielded stealth aircraft, while the United States did so in 1981.[17] If the U.S. aerospace research community had never come across Ufimtsev's breakthrough work, it is possible that the initial invention of stealth aircraft might not have occurred until decades later.

In the case of AI, we cannot allow the United States to play the role of the Soviet Union in the stealth story. Our leadership in AI technology research does not inherently mean that the United States will lead in the effective military adoption of AI.

VII. As a strong but still developing global military, China has advantages in AI adoption.

Some leaders in China's government see AI as a promising military "leapfrog development" opportunity, meaning that it offers military advantages over the United States and could be easier to implement in China than in the United States.[18]

The term "leapfrog development" describes a technology for which laggard countries can skip a development stage, or one for which being behind on the current generation of technology actually offers an advantage in adopting the next generation. A commonly cited example is the rapid and widespread adoption of cellular phone technology in countries that had only minimal landline phone adoption. Kai-Fu Lee, one of the leading venture capitalists in China's AI sector, argues that the absence of many developed-economy capabilities, such as easy credit checks, have led to a flood of Chinese entrepreneurs making innovative use of AI capabilities to fill those

[16] Petr Ya Ufimtsev, "DTIC Translation - Method of Edge Waves in the Physical Theory of Diffraction," Defense Technical Information Center, September 07, 1971, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=AD0733203.
[17] Director of Intelligence, "US Stealth Programs and Technology: Soviet Exploitation of the Western Press," Central Intelligence Agency, August 1, 1988, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB443/docs/area51_44.PDF.
[18] Webster et al., "Full Translation: China's 'New Generation Artifical Intelligence Development Plan' (2017)."

gaps.[19] Plastic credit cards are nearly nonexistent in China, but mobile phone payments secured by facial recognition are ubiquitous.

China's emphasis on AI as a leapfrog technology enabler extends to national security applications. China's 2017 National AI Development Plan identifies AI as a "historic opportunity" for national security leapfrog technologies.[20] Chinese defense executive Zeng Yi echoed that claim, saying that AI will "bring about a leapfrog development" in military technology and presents a critical opportunity for China.

If this strain in Chinese thinking is correct, that AI presents a leapfrog opportunity, it would mean that China is better positioned to adopt military AI than the United States. In this theory, the United States' current advantages in stealth aircraft, aircraft carriers, and precision munitions actually would be long-term disadvantages because the entrenched business and political interests that support military dominance today will hamper the United States in transitioning to an AI-enabled military technology paradigm in the future.[21] As one Chinese think tank scholar explained to me, he believes that the United States is likely to spend too much to maintain and upgrade mature systems and underinvest in disruptive new systems that make America's existing sources of advantage vulnerable and obsolete. China's military also faces perverse incentives to protect legacy systems, but to a far lesser extent: Chinese military spending tripled from 2007 to 2017, technology is a top priority, and there is a general understanding that many of its current platforms and approaches are obsolete and must be replaced regardless.[22]

Just one of many examples of China's AI leapfrog strategy is its prioritized investment and technology espionage for low-cost, long-range autonomous and unmanned submarines.[23] China believes these systems will be a cheap and effective means of threatening U.S. aircraft carrier battlegroups and an alternative path to projecting Chinese power at range. In some cases, Chinese thinkers see military AI research and development as a cheaper and easier path to threatening America's sources of military power than developing Chinese equivalents of American systems.

The United States still outspends China on defense, but much of that spending is tied up in legacy programs. The concern with regard to AI adoption is two-fold. First, the existence of

---

[19] Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order* (Boston: Houghton Mifflin Harcourt Trade & Reference Publishers, 2018).

[20] Specifically, the report says that China should "firmly seize the major historic opportunity for the development of AI . . . and support national security, promoting the overall elevation of the nation's competitiveness and leapfrog development."

[21] See, for example, Leo Blanken, Jason Lepore, and Stephen Rodriguez, "America's Military Is Choking on Old Technology," *Foreign Policy*, January 29, 2018, https://foreignpolicy.com/2018/01/29/americas-military-is-choking-on-old-technology.

[22] In nominal RMB terms. Source: Nan Tian et al., "Trends in World Military Expenditure, 2017," Stockholm International Peacre Research Institute, May 2018, https://www.sipri.org/publications/2018/sipri-fact-sheets/trends-world-military-expenditure-2017.

[23] Stephen Chen, "China Developing Robotic Subs to Launch a New Era of Sea Power," *South China Morning Post*, July 23, 2018, https://www.scmp.com/news/china/society/article/2156361/china-developing-unmanned-ai-submarines-launch-new-era-sea-power; and James Eng, "Woods Hole Oceanographic Institution Says Hack Linked to China," NBC News, October 16, 2016, https://www.nbcnews.com/tech/security/woods-hole-oceanographic-institution-says-hack-linked-china-n446226.

legacy programs provides a strong economic disincentive against investing in new approaches that are built from the ground up. This creates a painful division of funds in which the lion's share of research is invested in maintaining and improving existing systems and integrating them with AI, and only a minority is dedicated to programs designed with AI from square one.

Second, there is a deeper cultural and organizational issue. Many DoD organizational structures face a bias toward more expensive and sophisticated "exquisite" technologies. However, it may be that the most promising near-term use cases for AI will be inferior to the systems and processes that they replace in terms of traditional performance metrics but superior in terms of cost, availability, or expendability. The DoD should not let philosophical attachment or organizational inertia allow it to fall behind in the field of new and disruptive AI innovations.

VIII. Many of the obstacles to China's adoption of military AI are similar to those of the United States.

The main ingredients to developing AI are straightforward, if not easily procurable: (1) a model needs large quantities of data matching its expected operational use case to train; (2) skilled AI researchers and engineers must be recruited and retained, at either public or private research institutions; and (3) AI labs need a consistent funding stream to support their computational infrastructure and staff. These three ingredients are the key raw materials which in a productive environment can be channeled into the development of military AI. However, on all these fronts, neither China nor the United States has the quantities desired.

Data is always at a premium, especially for the niche use cases that relate to military functionality. While surveillance data, both from the internet and from Xinjiang, is plentiful for the Chinese government, how they might source sufficient data for autonomous targeting or underwater navigation remains to be seen. Likewise, American tech companies have no shortage of information on online social media activity or consumer spending habits, but this cannot be applied to military uses.

Likewise, engineers, and particularly researchers, are a limiting resource. The United States and China both draw from a finite field of talent in which demand far outstrips supply.

Finally, and most plainly, AI labs and companies, whether public or private, require consistent funding in order to thrive. While AI is a fundamentally transformational technology, the immediate benefits to customers may not immediately be apparent. AI is highly theoretical—until it is not. OpenAI was founded in 2015 but took seven years to dazzle the world with ChatGPT. In the intervening time, it was supported by a $1 billion investment from Microsoft—something not every AI startup is fortunate enough to have.[24] In China, flagship companies such as iFlyTek and SenseTime operate with a heavy input of data and a large revenue stream from the Chinese government. The principal limiting ingredients of China's AI are, like ours, questions of data, money, and personnel, and we should not underestimate the value of staying ahead of China in these basic ways.

[24] Grace Kay, "The History of ChatGPT Creator OpenAI, Which Elon Musk Helped Found before Parting Ways and Criticizing," *Business Insider*, February 1, 2023, https://www.businessinsider.com/history-of-openai-company-chatgpt-elon-musk-founded-2022-12.

IX. Recent U.S. export controls on semiconductor technology are designed to limit the future advancement of China's military AI sector.

The AI development stack is not merely an issue of software. All AI software has to run on semiconductor hardware somewhere, and many aspects of that hardware ecosystem are controlled by the United States and allied countries. For example, almost all AI models are trained on graphics processing units (GPUs)—sophisticated, parallel chips originally designed for gaming but often designed and optimized today for training sophisticated AI models. As of September 2022, Nvidia and AMD, two American GPU providers, were responsible for 95 percent of China's domestic GPU market. Nvidia, and its proprietary CUDA software architecture, are the foundation that AI researchers use to develop and train their models. CUDA makes it much easier for programmers to write massively parallelized software (as all modern AI software is) and ensures backward and forward compatibility so that older chips can still run newer software and vice versa.[25] Any customer who seeks to stop using Nvidia chips has to leave the CUDA ecosystem, which requires solving a lot of incredibly hard software problems for which CUDA already provides free answers. Those free answers reflect billions of dollars of investment in the CUDA platform by both Nvidia and its customers. As a result, China has high barriers to establishing a domestic competitor in the space of the next-generation chips that are necessary for AI.

In 2018, a Chinese government-run newspaper, *Science and Technology Daily*, published a list of 35 "chokepoint" technologies where Chinese domestic production significantly lags the international standard. Each of these technologies is an area in which Chinese leaders are concerned that the United States and its allies could choke off China's access, making them a national security concern. Among the 35 technologies, seven concern computer chips or chip manufacturing, sectors that are currently dominated by a group of companies across Taiwan, South Korea, the Netherlands, Japan, Germany, and the United States.[26]

The Biden administration's October 7 export controls lay out a unified theory of pressure that seeks to make access to American chips extremely difficult. The controls have five interlocking elements[27]:

1. Strangle the Chinese AI and supercomputing industries by choking off access to high-end chips.

2. Block China from designing AI chips domestically by choking off its access to U.S.-made chip design software and U.S.-built semiconductor manufacturing equipment.

3. Block China from manufacturing advanced chips by choking off access to U.S.-built semiconductor manufacturing equipment.

[25] Ben Thompson, "Shopify vs. Buy With Prime, Instagram Shopping, CUDA and China," Stratechery, September 7, 2022, https://stratechery.com/2022/shopify-vs-buy-with-prime-instagram-shopping-cuda-and-china/.
[26] These seven include photolithography machines, chips, high-end capacitors and resistors, core industrial software, photoresists, and ultra-precision polishing techniques. "35 Key 'Stranglehold' Technologies," PRC Ministry of Education, edited by Ben Murphy, translated by Etcetera Language Group, Inc, May 13, 2021, https://cset.georgetown.edu/publication/35-key-stranglehold-technologies/.
[27] Gregory C. Allen, "Choking off China's Access to the Future of AI," CSIS, October 11, 2022, https://www.csis.org/analysis/choking-chinas-access-future-ai.

4. Block China from developing its own semiconductor manufacturing equipment by choking off access to U.S.-built components.

5. Ensure that China does not replace lost access to U.S. semiconductor technology by partnering with U.S. allies.[28]

In theory, these four policies should definitively hamper China's march toward AI technology. However, China's export control evasion activities are significant and growing. My primary recommendation is that Congress focus on concrete strategies to tighten this enforcement and shore up remaining gaps that risk allowing China to close the AI gap.

X. The Department of Commerce's Bureau of Industry and Security must be technologically modernized to combat China's evasion of export controls.

The five chokepoints mentioned above are not all alike in the case of enforcement. Chipmaking equipment, which is large and expensive and requires significant post-sale support, is easiest to enforce. However, from China's perspective, the most direct path to continued AI progress is continuing to use U.S. chips. It is at this first and crucial chokepoint that China most flagrantly attempts to evade our export controls, and too often succeeds.

I and colleagues at CSIS recently conducted an in-depth analysis on U.S. export controls enforcement capacity.[29] Our findings were concerning.

The Bureau of Industry and Security (BIS) at the Department of Commerce oversees most export controls. Unfortunately, BIS is increasingly challenged by worldwide smuggling and export control evasion networks, especially those that are supported by Russia and China. For example, investigators have examined the wreckage of downed Russian weapons systems in Ukraine and found that they contain U.S. and allied components, including semiconductor electronics that were manufactured years after the implementation of the 2014 Russia export controls.[30]

As our geopolitical rivals pursue increasingly aggressive and better-resourced means of obtaining critical technology, BIS must use every tool available to increase capacity and productivity for effective enforcement. The need for robust U.S. export controls is more strategically critical than at any time since the end of the Cold War, but BIS's enabling technology is in a dreadful state. The cause is simple: decades of underinvestment. Current and former BIS staff told me in a series of interviews that the major government databases that they

[28] Gregory C. Allen and Emily Benson, "Clues to the U.S.-Dutch-Japanese Semiconductor Export Controls Deal Are Hiding in Plain Sight," CSIS, March 1, 2023, https://www.csis.org/analysis/clues-us-dutch-japanese-semiconductor-export-controls-deal-are-hiding-plain-sight; and Gregory C. Allen, Emily Benson, and Margot Putnam, "Japan and the Netherlands Announce Plans for New Export Controls on Semiconductor Equipment," CSIS, *Commentary*, April 10, 2023, https://www.csis.org/analysis/japan-and-netherlands-announce-plans-new-export-controls-semiconductor-equipment.

[29] Gregory C. Allen, Emily Benson, and William Alan Reinsch, "Improved Export Controls Enforcement Technology Needed for U.S. National Security," CSIS, November 30, 2022, https://www.csis.org/analysis/improved-export-controls-enforcement-technology-needed-us-national-security.

[30] Jeanne Whalen, "U.S. Probing How American Electronics Wound up in Russian Military Gear," *Washington Post*, June 15, 2022, https://www.washingtonpost.com/world/2022/06/15/us-computer-chips-russian-military/.

use to monitor trade flows and identify suspicious activity can perform only a fraction of the needed functionality and crash routinely. Instead of knowledge graph databases and machine learning—capabilities that have revolutionized both the private sector and other federal agencies with similar missions—BIS analysts perform their work primarily using Google searches and Microsoft Excel.

Modern, data-driven digital technologies utilizing AI and machine learning can and should play an integral role in enhancing BIS export control enforcement capabilities. Relatively modest investments could lead to 5 to 10 times greater analyst productivity. Despite the increasingly pressing need to invest in these new enforcement capabilities, the budget of BIS has not increased commensurate with the increased number of export-controlled items, the evolving threat landscape, and the growing pressure from an increasingly sophisticated evasion regime.

A changed geopolitical landscape demands reinvigorated U.S. government export controls capacity, and this cannot be done without additional resources. CSIS analysis of relevant comparable data-driven digital technology modernization efforts by other U.S. government agencies with similar mission requirements suggests that this could be accomplished with an additional appropriation for technology modernization at BIS of roughly $25 million annually for five years. This funding would allow BIS to better ingest, connect, and analyze hundreds of billions of records from both government and open-source data. By applying modern data science and machine learning techniques, BIS could increase productivity across all its processes. For example, it could automatically detect that a purported Eastern European “tractor manufacturer” has the same phone number as a supplier of engines to the Russian military. This figure accounts for opportunities at BIS to improve collaboration with other U.S. government agencies and the need to prevent unnecessary duplication of effort.

However, a more productive enforcement analysis community will identify more entities as likely shell companies engaging in illicit transactions. This will in turn increase the need for enforcement agents to conduct site inspections or criminal investigations of these identified entities. Despite the severe current technological limitations on the efficacy of the analytic community, its work is already identifying enough candidate entities for inspection to more than fully consume the capacity of the current staff. Therefore, in addition to the $25 million annual increase for five years to support new technology and staff for BIS analytical capabilities, BIS will also require an additional $18.4 million and 48 positions annually for the Export Enforcement organization as well as another $1.2 million for additional classified facility space for these individuals to support the classified aspects of their work. Thus, the total size of the additional BIS budget appropriation that I and my CSIS colleagues recommended is $44.6 million annually.

In terms of return on investment, this $44.6 million annual increase in BIS’s budget is likely to be one of the best opportunities available anywhere in U.S. national security. The U.S. government is currently spending tens of billions to assist Ukraine in destroying the weapons of Russia’s military, which too often are powered by U.S. technology. Providing a few tens of millions of dollars annually to BIS to modernize the technology that enables export controls enforcement would go a long way toward ensuring that far fewer Russian and Chinese weapons using U.S. technology are built in the future.

As every street corner narcotics dealer knows, there is a major difference between a business transaction being illegal and it being impossible. The U.S. export licensing and administration process determines whether or not an international sale by a U.S. entity is permissible, but the efficacy of enforcement of the controls determines whether or not such sales will succeed when they are attempted and whether the terms of the license are honored subsequent to export. There are a variety of tactics that illicit actors can use to gain access to U.S. technology in defiance of export controls, ranging from outright theft and smuggling to the use of shell companies that hide the identity of an unlawful end user behind a front company falsely purporting to be purchasing the item legally. Former Department of Commerce and U.S. intelligence community officials interviewed for our CSIS project said that it can sometimes take the Russian and Chinese military mere days to successfully set up a shell company for purchasing U.S. technology, while the current process for uncovering a shell company's illegal activity may take years, if it is uncovered at all.

XI. Conclusion

The United States and the People's Republic of China are peer competitors in the key field of AI. But although the two sides are roughly equally matched, the advantages and disadvantages of each are not the same. The United States has deep industry, scientific, and institutional knowledge in the sciences of machine learning and exercises significant control over the physical supply chain of chips that are the cornerstone of AI development. However, we have not matched China's level of government adoption for security applications, as well as public-private cooperation.

The United States government has tools for influencing both the trajectory of U.S. military AI adoption as well as China's AI trajectory. On the latter issue, I feel that the main focus of the conversation in Washington, D.C., is incomplete. There is a great deal of focus on which technologies to apply export controls and to which countries. But there is a missing discussion about U.S. export controls capacity. The export controls policy that the United States has enacted on China's AI and semiconductor sectors is a direct challenge to two of China's top technological priorities for both their economy and national security. It is clear that China will devote extraordinary resources to circumventing those controls, and they are already doing so. The United States government should be willing to devote significant additional focus and funding toward ensuring that China does not succeed.

Thank you for the opportunity to testify today, and I look forward to your questions.