

FEBRUARY 1, 2024

TESTIMONY BEFORE THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Hearing on Current and Emerging Technologies in U.S.-China Economic and National Security Competition

Military Artificial Intelligence, the People's Liberation Army, and U.S.-China Strategic Competition

ΒY

Jacob Stokes

Senior Fellow, Indo-Pacific Security Program Center for a New American Security

I. Introduction

Thank you Co-Chair Wessel, Co-Chair Helberg, and the Commissioners for inviting me to provide written and oral testimony on this critical topic.¹ My comments draw on my own research as well as technical insights from my colleagues in CNAS's Artificial Intelligence (AI) Safety and Stability Project (although the policy views are solely mine). It should be noted up front that this field poses special analytical challenges: it is mostly intangible, the technology is complex and evolving rapidly, and China's applications of AI in a military context are still shrouded in secrecy.

My testimony covers China's military applications of AI, as well as the broader geostrategic implications of AI development for U.S.-China major power competition. It starts by examining the role of AI in China's overall military modernization plans. Then, it explores AI implementation to date in China's military, the People's Liberation Army (PLA). Next, my testimony considers obstacles that could block the PLA from reaching its military AI ambitions and explores some of the risks that military AI could pose in the U.S.-China security relationship. Finally, my testimony assesses U.S. responses to date and offers recommendations for American policymakers.

II. The Role of AI in China's Overall Military Modernization

China sees AI playing a central role in advancing its military power. Chinese Communist Party (CCP) General Secretary Xi Jinping has set ambitious goals for the PLA to "basically complete" its modernization by 2035 and transform into a "world-class" military by the middle of the century.² In March 2023, Xi called on the PLA to "raise the presence of combat forces in new domains and of new qualities."³ As part of those goals, Xi wants the PLA to continue to move through stages of military-technological development, from *mechanization* to *informatization* and ultimately *intelligentization*. Broadly, mechanization refers to fielding modern platforms and equipment; informatization refers to linking those systems to networks such as GPS; and intelligentization refers to integrating artificial intelligence, quantum computing, big data, and other emerging technologies into the joint force.⁴ In 2020, China set a new goal to "accelerate the integrated development of mechanization, informatization, and intelligentization" by 2027.⁵ In other words, Beijing aims to make progress on all three stages simultaneously rather than sequentially.

https://www.chinadaily.com.cn/china/19thcpcnationalcongress/2017-11/04/content_34115212.htm.



¹ This testimony is partly adapted from my CNAS report on the topic: Jacob Stokes and Alexander Sullivan with Noah Greene, *U.S.-China Competition and Military AI: How Washington Can Manage Strategic Risks amid Rivalry with Beijing* (Center for a New American Security, July 2023), <u>https://www.cnas.org/publications/reports/u-s-china-competition-and-military-ai</u>.

² Xi Jinping, Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era: Report to the 19th National Congress of the Chinese Communist Party (October 18, 2017), as reposted by China Daily,

³ "China's Xi calls for 'more quickly elevating' armed forces," The Associated Press, March 9, 2023, https://apnews.com/article/china-us-military-taiwan-xi-jinping-14f9c3d8fef26779f017d927aa352eeb.

⁴ Kevin Pollpeter and Amanda Kerrigan, *The PLA and Intelligent Warfare: A Preliminary Analysis* (CNA, October 2021), <u>https://www.cna.org/archive/CNA_Files/pdf/the-pla-and-intelligent-warfare-a-preliminary-analysis.pdf</u>.

⁵ Central Committee of the Communist Party of China, *Communiqué of the Fifth Plenary Session of the 19th Central Committee of the Communist Party of China* (November 17, 2021), as translated by the China Aerospace Studies Institute, https://www.airuniversity.af.edu/CASI/In-Their-Own-Words/Article-Display/Article/2834176/itow-communiqu-of-the-fifthplenary-session-of-the-19th-central-committee-of-th/. For a useful discussion of other semi-authoritative Chinese sources explaining this new goal, see Zichen Wang, "Once-in-a-generation change in PLA guidelines: intelligentization added, mechanization declared 'basically accomplished,''' *Pekingnology* (blog) on Substack, December 8, 2020, https://www.pekingnology.com/p/once-in-a-generation-change-in-pla.

Beijing sees progressing through these stages as necessary to keep pace with changes in the technological character of warfare in the 21st century. Chinese scholars speak about the ongoing revolution in military affairs as one of weapons "systems confrontation" requiring "systems destruction warfare" to win.⁶ To compete in this emerging era of conflict, the PLA is developing an overarching concept it calls "multidomain precision warfare."⁷ In layman's terms, this concept posits that the very networking that gives the U.S. military its power creates interdependencies between its forces, which are also vulnerabilities that can be exploited. Thus, rather than needing to destroy U.S. enemy forces directly—ship-to-ship or tank-to-tank—China can attack the weak points linking U.S. systems and domains together and thereby neutralize or overwhelm U.S. advantages. Those weak points can include internet, satellite, or electromagnetic communications links as well as logistical supply systems.

AI is a critical part of this strategy because, in the dynamic environment of an actual conflict, identifying and targeting U.S. vulnerabilities will require sensing, relaying, and processing vast amounts of information at a speed only computers can match. AI is also key for uncrewed autonomous systems. In his speech to the CCP's 20th National Congress in October 2022, Xi called on China to "speed up the development of unmanned, intelligent combat capabilities."⁸ In addition, China's program of Military-Civil Fusion—although its scope remains ambiguous in practice—seeks to appropriate select private technological advancements, including some developed in cooperation with international research partners, to augment the PLA's capabilities.⁹

III. AI Implementation in the PLA

China takes an expansive view of military AI's potential and is engaged in extensive research, development, and experimentation.¹⁰ But so far, open-source information about the PLA fielding specific military AI systems remains sparse. The roles for AI within China's overall program of military modernization are still generally coming into focus. Researchers at the Center for Security and Emerging Technology analyzed 343 PLA equipment contracts and found seven areas of interest for current AI investments: (1) intelligent and autonomous vehicles; (2) intelligence, surveillance, and reconnaissance; (3) predictive maintenance and logistics; (4) information and electronic warfare; (5)



⁶ Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (RAND Corporation, 2018), <u>https://www.rand.org/pubs/research_reports/RR1708.html;</u> Mark Cozad et al., *Gaining Victory in Systems Warfare: China's Perspective on the U.S.-China Military Balance* (RAND Corporation, 2023), <u>https://www.rand.org/pubs/research_reports/RR1535-1.html;</u> and State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (July 2019), as reposted by the China Aerospace Studies Institute, <u>https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2019-</u> <u>07%20PRC%20White%20Paper%20on%20National%20Defense%20in%20the%20New%20Era.pdf?ver=akpbGkO5ogbDP</u> PbflQkb5A%3D%3D.

⁷ U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China* (2022), 39, <u>https://media.defense.gov/2022/Nov/29/2003122279/-1/-1/1/2022-MILITARY-AND-SECURITY-DEVELOPMENTS-</u> INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

⁸ Xi Jinping, Hold High the Great Banner of Socialism with Chinese Characteristics and Strive in Unity to Build a Modern Socialist Country in All Respects: Report to the 20th National Congress of the CCP (October 16, 2022), as reposted by Nikkei Asia, <u>https://asia.nikkei.com/Politics/China-s-party-congress/Transcript-President-Xi-Jinping-s-report-to-China-s-</u> 2022-party-congress.

⁹ Tai Ming Cheung, "The Promise and Peril of Military-Civil Fusion," in *Innovate to Dominate: The Rise of the Chinese Techno-Security State* (Ithaca: Cornell University Press, 2022), 83-141.

¹⁰ For a detailed account of these activities, see Elsa Kania, Adjunct Senior Fellow at the Center for a New American Security, "Chinese Military Innovation in Artificial Intelligence," Statement to the U.S.-China Economic and Security Review Commission, June 7, 2019,

https://www.uscc.gov/sites/default/files/June%207%20Hearing_Panel%201_Elsa%20Kania_Chinese%20Military%20Innova tion%20in%20Artificial%20Intelligence_0.pdf.

simulation and training; (6) command and control; and (7) automated target recognition.¹¹ Those categories are illustrative but not necessarily exhaustive. Two areas of special focus are AI in the PLA's weapons systems and AI in the PLA's battlefield functions and support:

AI in the PLA's Weapons Systems (Uncrewed Systems, LAWS). Assessing China's progress in developing and fielding uncrewed autonomous vehicles (i.e., drones) for air, ground, sea surface, and subsea applications is difficult. Beijing clearly has a large and sophisticated drone industry and is the world's largest exporter of military drones.¹² But the fact that those systems can operate without an onboard crew indicates little about the degree to which they can act autonomously; autonomy would be enabled by AI and is therefore highly dependent on the quality of the AI. Uncrewed systems possess varying levels of autonomy. These range from essentially no autonomy in fully remote-controlled systems, to completely autonomous systems that can navigate, choose targets, and even fire without human control, with multiple levels in between.¹³ As DOD's 2023 *China Military Power Report* states, the PLA is "pursuing greater autonomy for unmanned aerial, surface, and underwater vehicles to enable manned and unmanned teaming, swarm attacks, optimized logistic support, and distributed ISR [intelligence, surveillance, and reconnaissance], among other capabilities."¹⁴

China's commercial drone companies have exhibited a world-class ability to operate in AI-dependent swarms, which is likely to be a key capability for military applications.¹⁵ Swarming is an area where capabilities developed in the private sector could be applied to the military sector quickly. Additionally, China is developing a system called the FH-97A, which is similar to the U.S. "loyal wingman" concept, where an autonomous aircraft flies in a team alongside a crewed aircraft.

Separately, China's drone capabilities link directly to the global debate about lethal autonomous weapons systems (LAWS) or, less formally, "killer robots." The PLA possesses plenty of lethal military power, but right now none of it appears to have meaningful levels of autonomy enabled by AI. Beijing's official policy on regulating LAWS is ambiguous, leaving open the possibility that China could develop and field such systems if the technology matures.

AI in the PLA's Battlefield Functions and Support. Tracking implementation of military AI in the categories of battlefield functions and support is even more difficult. That is because those capabilities are primarily software-based and therefore harder to observe through tools such as satellite imagery. That said, the PLA is likely to start using AI for predictive maintenance and logistics systems relatively early given similarity to commercial applications. Further, the PLA likely already uses basic forms of AI for some types of ISR tasks. AI promises to be particularly useful for combing through huge amounts of information from many different types of sensors. ISR is another field where

drones#:~:text=Data%20from%20the%20Stockholm%20International,exporter%20of%20the%20weaponised%20aircraft.



4

¹¹ Ryan Fedasiuk, Jennifer Melot, and Ben Murphy, *Harnessed Lightning: How the Chinese Military Is Adopting Artificial Intelligence* (Center for Security and Emerging Technology, October 2021), 13, <u>https://cset.georgetown.edu/wp-content/uploads/CSET-Harnessed-Lightning.pdf</u>.

¹² Stockholm International Peace Research Institute (SIPRI) data as cited in Zaheena Rasheed, "How China became the world's leading exporter of combat drones," Al Jazeera, January 24, 2023, <u>https://www.aljazeera.com/news/2023/1/24/how-china-became-the-worlds-leading-exporter-of-combat-</u>

¹³ No single universal framework for measuring autonomy in uncrewed systems exists, but one example of a framework can be found at "Breaking Down The Levels of Drone Autonomy," cloudfactory, November 23, 2021, https://blog.cloudfactory.com/levels-of-drone-autonomy.

¹⁴ U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China* (2023), 97, <u>https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.</u>

¹⁵ Emilie Stewart, Survey of PRC Drone Swarm Inventions (China Aerospace Studies Institute, October 9, 2023), <u>https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Other-Topics/2023-10-09%20Survey%20of%20PRC%20Drone%20Swarm%20Inventions.pdf.</u>

China's AI innovations for, and vast training data from, its domestic repression apparatus, including biometrics and image recognition, likely aid progress in the PLA's systems.

Next, China will pursue AI systems for use in command, control, and communications (C3) and decision-making purposes, likely advancing over time through three levels of sophistication. The first level is using AI for counter-C3; that is, to improve China's cyber capabilities with the objective of trying to disrupt the opponent's C3. The use of AI in cyber operations is relatively mature and will likely grow more capable over time. Better offensive cyber capabilities will enable the full range of cyber operations, including "adversarial AI," or trying to disrupt the opponent's AI systems.¹⁶

The second level of military AI for C3 applications is tactical- and operational-level C3 for the PLA's physical weapons systems. The PLA is likely to use AI to control uncrewed systems, either individually or coordinated in a swarm. Improving targeting and allocation of scarce artillery and munitions might be another use. A news report from April 2023 showed the PLA testing an AI system to help with artillery targeting.¹⁷ Further, Beijing is likely to use AI to help develop plans for the tactical and operational level of warfare with the goal of cutting through the fog of war and gaining decision-advantage—a version of what Chinese military experts have called a "command brain."

The third level of sophistication for military AI for C3 purposes would be for strategic- or political-level decisions. In the near- and mid-terms, China will likely hesitate to put in place AI systems for these types of decisions, because the technology will still be immature. Moreover, PRC leaders insist on tight political control, particularly of strategic capabilities such as nuclear weapons.

The future trajectory of military AI in the PLA. While China has ambitious plans for infusing military AI throughout the PLA, the technology's ultimate trajectory is not currently clear. Beijing will have to overcome multiple obstacles to fulfill its objectives, as I will lay out in the next section. At the same time, AI is a general-purpose technology (like electricity or railroads), so analysts cannot yet know all of its potential uses or implications.¹⁸ In the near- and mid-terms, most of the changes AI will usher in will be incremental and narrow. But in the mid- to long-term, some could be revolutionary and general. China provides little transparency on its military modernization efforts, including for AI, which could someday lead to strategic surprise for the United States if Beijing manages to make breakthroughs in secret.

IV. How the PLA Might Fall Short of Its Al Ambitions

Neither articulating lofty goals nor simply throwing money and people at the issue will ensure Beijing fulfills its ambitions for integrating AI into the PLA. China could fall short of, or at least face delays in reaching, its goals due to several obstacles, including:

Technology. The technology itself might prove difficult to master, even with abundant resources. Technology controls imposed by the United States and its allies could hamper Beijing's ability to develop and operate AI-enabled systems at scale. Additionally, China could simply lack the capacity to innovate at the leading edge of military technology. In earlier stages of its military modernization, China could imitate

5



¹⁶ Apostol Vassilev et. al, *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations* (National Institute of Standards and Technology, January 2024), <u>https://csrc.nist.gov/pubs/ai/100/2/e2023/final.</u>

¹⁷ Stephen Chen, "China tests AI-powered long-range artillery that can hit a person 16km away," *South China Morning Post*, April 17, 2023, <u>https://www.scmp.com/news/china/science/article/3217334/china-tests-ai-powered-long-range-artillery-can-hit-person-16km-away</u>.

¹⁸ Jeffrey Ding and Allan Dafoe, "Engines of Power: Electricity, AI, and general-purpose, military transformations," *European Journal of International Security*, 8 no. 2 (February 7, 2023): 1-18, <u>https://doi.org/10.1017/eis.2023.1</u>.

and/or steal technology from the United States, Russia, and other advanced militaries. However, intelligentization requires pioneering totally new military technologies and operational concepts for how to use them—a much more difficult task.

Personnel, bureaucracy, and corruption. Impediments related to personnel, bureaucratic structure, or political control could further constrain the PLA's AI ambitions. These include a lack of skilled personnel needed to operate AI systems and stovepiped military bureaucracies. The PLA's Strategic Support Force (SSF)—a stand-alone military service created in 2015 to focus on space, cyber, and electromagnetic warfare—appears to control the lion's share of AI development resources and authority within the PLA.¹⁹ While the SSF may have been created in part to enable jointness through advanced networking and now AI, it may be loath to relinquish control of its creations to the rest of the PLA, or other services might resist relying on capabilities run by the SSF.²⁰ The PLA's efforts to implement AI across the joint force could also fall prey to corruption, as has reportedly been the case for parts of China's nuclear missile forces.²¹

Political control. The CCP values political control above other aims. The dictum that "the party controls the gun"—first stated by Mao Zedong and reaffirmed by Xi—and the prominent role of political commissars in the PLA reflect that fact.²² Even for expert researchers, today's state-of-the-art AI models present challenges for predictability, "explainability," and transparency. This opacity could make PLA commanders reluctant to trust it for fear that they do not control its actions.²³ Alternatively, however, Chinese leaders might be more willing to place trust in programmable machines over people. Given these contradictory impulses, it is not yet clear to what extent China's military leadership and operational-level commanders will embrace or avoid AI in practice.

Funding. Some obstacles might be material. The PLA officially declared that it achieved full mechanization in 2020, is making rapid progress on informatization, and is pushing to develop cutting-edge capabilities necessary for intelligentization. But as large numbers of once-new ships, aircraft, and other weapons systems age, the cost to operate and maintain them will rise quickly, potentially crowding out investments in next-generation AI-enabled capabilities. Should China's domestic economy face sustained headwinds, fewer resources might be available for advancing AI within the PLA.



¹⁹ John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," in Phillip C. Saunders et al., eds., *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms* (Washington: National Defense University Press, 2019), 437-515, <u>https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1748555/chinas-strategic-support-force-a-force-for-a-new-era/</u>.

²⁰ Amy Nelson and Gerald Epstein, *The PLA's Strategic Support Force and AI Innovation* (The Brookings Institution, December 23, 2022), <u>https://www.brookings.edu/techstream/the-plas-strategic-support-force-and-ai-innovation-china-military-tech/</u>.

²¹ Peter Martin and Jennifer Jacobs, "US Intelligence Shows Flawed China Missiles Led Xi to Purge Army," Bloomberg, January 6, 2024, <u>https://www.bloomberg.com/news/articles/2024-01-06/us-intelligence-shows-flawed-china-missiles-led-xi-jinping-to-purge-military?srnd=undefined</u>.

²² Minnie Chan, "Communist Party 'controls the gun,' PLA top brass reminded," *South China Morning Post*, November 5, 2014, <u>https://www.scmp.com/news/china/article/1632136/communist-party-controls-gun-pla-top-brass-reminded</u>; and Timothy Heath, Senior International Defense Researcher, "The Consolidation of Political Power in China Under Xi Jinping: Implications for the PLA and Domestic Security Forces," Statement to the U.S.-China Economic and Security Review Commission, February 7, 2019, <u>https://www.uscc.gov/sites/default/files/Heath_USCC%20Testimony_FINAL.pdf</u>.

²³ Kelley M. Sayler, *Artificial Intelligence and National Security* (Congressional Research Service, November 10, 2020, update), 30-33, <u>https://crsreports.congress.gov/product/pdf/R/R45178/10</u>.

V. Risks that China's Military Al Poses to the United States

Given the emerging nature of, and sprawling potential applications for, military AI in the PLA, it is too early to know all the risks those capabilities might pose to the United States. It is possible, though, to develop a provisional list, which would include the following:

Shift in the military balance of power. Perhaps the most likely source of strategic risks in the U.S.-China security relationship stemming from military applications of AI will be one that is difficult to measure precisely and cannot be solely attributable to AI: the overall military balance. Many of the most practical uses for military AI in the near term will be for purposes that are relatively mundane but could help the PLA use resources more efficiently and therefore generate more military capabilities per renminbi or dollar spent. These include helping to improve processes for maintenance, logistics, training, and decision-support. Such "back office" functions rarely receive the sustained attention devoted to "tip of the spear" capabilities that appear on the front lines of combat. However, the strength of modern militaries depends as much on their enabling bureaucracies as their frontline troops and weapons.

In addition, some emerging military AI applications will improve the PLA's combat capabilities. Initially, those improvements are likely to be *evolutionary* rather than *revolutionary*. Consider the air domain, to name just one of many examples. "Loyal wingman"-type systems where uncrewed aircraft fly with crewed aircraft could improve on what human pilots could do on their own.²⁴ But uncrewed and fully autonomous air systems—capable of greater persistence, maneuverability, and other attributes due to their lack of human bodily limitations—will likely be necessary for a complete paradigm shift in air combat operations. A similar story is playing out across nearly every aspect of military affairs. If the totality of improvements in military AI across every area tip the U.S.-China military balance in Beijing's favor, then the risks of conflict could rise.

Decision-making. Military AI tools could increase strategic risks emanating from the decision-making and information domain in three main ways: by compressing the time policymakers have to make high-stakes decisions, by generating bad inputs to decision-making processes, and by tempting actors to try to undermine states' deliberations through large-scale information operations. (My co-panelist will cover China's "cognitive domain operations," so I am skipping over them despite their clear relevance in this area.)

Autonomous uncrewed systems. Autonomous uncrewed systems could lead to deliberate escalation in a crisis if leaders see them as less dangerous to deploy, either because of lower expected human casualties or merely because the systems are more capable. Drones could also cause inadvertent escalation if either state takes an action using an autonomous system that the other state sees as provocative and escalatory. Finally, autonomous uncrewed systems could lead to an accident due to error or malfunction.

Intelligence, surveillance, and reconnaissance (ISR). AI is likely to be particularly effective for ISR applications given its ability to identify patterns in massive amounts of data. Additionally, it could enable new ISR capabilities, such as some surveillance balloons, in areas where norms are non-existent or weak.



²⁴ Liu Xuanzun, Cao Siqi, and Fan Wei, "Exclusive: China's new loyal wingman drone to greatly change air combat: designer," *Global Times*, November 7, 2022, <u>https://www.globaltimes.cn/page/202211/1278930.shtml</u>; Tom Ward, "The US Air Force Is Moving Fast on AI-Piloted Fighter Jets," *Wired*, March 8, 2023, <u>https://www.wired.com/story/us-air-force-skyborg-vista-ai-fighter-jets/</u>.

Command, control, and communication (C3). AI could empower better PLA C3 as China pursues multi-domain precision warfare, its analog to the U.S. Joint All-Domain Command and Control (JADC2) concept. Conversely, AI could empower attacks against U.S. or allied C3 systems. AI-assisted C3 and counter-C3 together have the potential to create "use or lose" pressures on decisionmakers in both countries during a crisis or contingency that could drive escalation.

Nuclear weapons. In the nuclear arena, AI systems could enable large-scale processing of data from various sensors to track mobile missile systems on land and even submarines at sea, especially if combined with other emerging technologies, such as quantum sensors.²⁵ Those applications are still only theoretical but could be feasible in the medium term.²⁶ If they come to pass, they could create transparency with destabilizing effects by undermining the *survivability*—the property of a military system that makes it hard for adversary forces to find and destroy—of components of two legs of the nuclear triad by enabling adversary tracking and targeting of those assets for counterforce strikes.

Additionally, PRC experts have expressed concerns that these same capabilities, if fielded by the United States, could undermine China's nuclear deterrent.²⁷ Those experts also worry that uncrewed autonomous systems could create new nuclear counterforce options. Such concerns could be one among several reasons China is expanding its nuclear arsenal.

VI. Assessing U.S. Policy Toward China's Military AI Activities

How the United States and its allies and partners respond to China's military AI ambitions will be an important factor shaping the balance of military AI capabilities specifically and military power generally. Washington's approach to date can be assessed along three lines of effort: improving U.S. and allied military AI capabilities, taking steps to hinder China's progress on developing military AI, and diplomacy with China related to military AI. This section will cover each in turn.

Improving U.S. and allied military AI capabilities. The U.S. Department of Defense has prioritized developing and fielding cutting-edge AI for military applications, including unilaterally through the Chief Digital and Artificial Intelligence Office (CDAO), the Replicator Initiative, and the first-ever National Defense Industrial Strategy. Washington is also working with allies on military AI through the advanced capabilities (pillar 2) of the Australia-United Kingdom-United States (AUKUS) partnership and the creation of an AI Strategy for NATO.²⁸ American defense officials recognize the possible ramifications of maturing AI technologies for the international security environment. That said, any revolution in military affairs that AI might create is still in its infancy, if it happens at all. There is a long road ahead where the United States

8



²⁵ Paul Bracken, *The Hunt for Mobile Missiles: Nuclear Weapons, AI, and the New Arms Race* (Foreign Policy Research Institute, September 21, 2020), <u>https://www.fpri.org/article/2020/09/the-hunt-for-mobile-missiles-nuclear-weapons-ai-and-the-new-arms-race/</u>; and Edward Geist and Andrew Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War* (RAND Corporation, 2018), <u>https://www.rand.org/pubs/perspectives/PE296.html</u>.

²⁶ Kelley M. Sayler, *Defense Primer: Quantum Technology* (Congressional Research Service, November 15, 2022, update), <u>https://crsreports.congress.gov/product/pdf/IF/IF11836</u>; and Edward Parker, *Commercial and Military Applications and Timelines for Quantum Technology* (RAND Corporation, 2021), <u>https://www.rand.org/pubs/research_reports/RRA1482-4.html</u>.

²⁷ Chen Qi and Zhu Rongsheng, Uncertainties: Why Are We Concerned about the Impact of AI on International Security?

⁽Center for International Security and Strategy at Tsinghua University, 2019), 5, <u>https://ciss.tsinghua.edu.cn/info/eyjdt/1363</u>. ²⁸ Patrick Parrish and Luke Nicastro, *AUKUS Pillar 2: Background and Issues for Congress* (Congressional Research Service, June 20, 2023), 5-6, <u>https://crsreports.congress.gov/product/pdf/R/R47599</u>.

could be held back by an R&D and acquisition system that is still too often stuck in the 20th century, military service cultures sometimes reluctant to embrace major changes, and fierce resource competition. More broadly, in competition with China over military AI, U.S. officials will have to pursue competitive policies across all the constituent parts of AI: chips for "compute" power, data, algorithms as well as the talent and institutions to develop and scale them.²⁹

Slowing down China's progress on developing military AI. Washington has also taken significant steps to slow down Beijing's acquisition of advanced AI, particularly for military applications. These include aggressive semiconductor controls; restrictions on outbound and inbound investment into the sector; and placing entities with ties to the PLA on various sanctions lists.³⁰ Those are all smart actions, but they will have to be updated over time as China continually develops workarounds. Most of the enforcement action so far has focused on chips, but U.S. policymakers will have to monitor action on all the constituent parts of AI mentioned earlier.

Specifically, protecting algorithms and data controlled by U.S. and allied organizations from PRC espionage will be critical. Taking steps to improve the physical and cyber security of key U.S. and allied firms that possess or make inputs for AI will be a logical imperative in this context. And while there have not been any blatantly obvious copies of U.S. AI technology like those seen in the advanced fighter aircraft field, it is reasonable to surmise that major data sets stolen by China—such as the 2015 theft of data from the U.S. Office of Personnel Management—could be used to train AI models.

Engaging China on stability and norms related to military AI. Washington has also sought to engage Beijing on developing norms for military AI and potentially even arms control measures in the future. The U.S. readout of President Biden's November 2023 meeting with General Secretary Xi said the two leaders "affirmed the need to address the risks of advanced AI systems and improve AI safety through U.S.-China government talks."³¹ Beijing seeks to shape the agenda for both civilian and military AI governance globally. China proposed the Global AI Governance Initiative in October 2023, although details of what that initiative entails are sparse, and attended the November 2023 AI Safety Summit in the United Kingdom and signed the resulting Bletchley Declaration.³² The United States has similarly been active in putting forward principles for governing AI domestically and internationally, notably through the "Political Declaration on

Bold. Innovative. Bipartisan.



²⁹ My colleague Paul Scharre has called computing power, data, talent, and institutions the "four battlegrounds" of global AI competition. Paul Scharre, *Four Battlegrounds: Power in the Age of Artificial Intelligence* (New York: W.W. Norton & Company, 2023).

³⁰ Emily Kilcrease and Michael Frazer, *Sanctions by the Numbers: SDN, CMIC, and Entity List Designations on China* (Center for a New American Security, March 2, 2023), <u>https://www.cnas.org/publications/reports/sanctions-by-the-numbers-sdn-cmic-and-entity-list-designations-on-china</u>.

³¹ White House, "Readout of President Joe Biden's Meeting with President Xi Jinping of the People's Republic of China," press release, November 15, 2023, <u>https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/15/readout-of-president-joe-bidens-meeting-with-president-xi-jinping-of-the-peoples-republic-of-china-2/.</u>

³² Ministry of Foreign Affairs of the People's Republic of China, "Global AI Governance Initiative," Communique, October 20, 2023, <u>https://www.mfa.gov.cn/eng/wjdt_665385/2649_665393/202310/t20231020_11164834.html</u>; United Kingdom,

[&]quot;The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023," January 16, 2024, <u>https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023.</u>

Responsible Military Use of Artificial Intelligence and Autonomy" that has been endorsed by 47 states.³³ Ultimately, U.S.-China dialogue on these issues is important but just one pillar of a comprehensive strategy to govern AI, including for military applications.

VII. Recommendations for Policymakers

1. Take bold action to constrain China's progress in AI for military and repressive purposes, but do so in a narrow way that avoids self-defeating steps. Washington should continue to take aggressive steps to constrain China's progress in these areas. But U.S. leaders must also ensure those efforts are coordinated with allies and close partners, and that they account for technical and market dynamics given that the primary source of innovation in AI is in the commercial rather than the government sector.

2. Build U.S. military AI capabilities to stay on the cutting edge. AI could define the future of military power. Washington will need to move quickly to stay on the cutting edge. This will require pushing forward reforms to the Pentagon's acquisition process and, in some cases, prioritizing funding for future capabilities over buying and operating already-mature capabilities. Deterring China today should be balanced with what will be necessary for deterrence 5-15 years down the road.

3. Continue to shape global rules, norms, and institutions around the deployment and use of military AI. Congress should support U.S. efforts to build consensus around rules, norms, and institutions to govern the use of military AI. U.S. foreign policy's core objective is upholding a rules-based global order. Unlike in many other areas, though, there are no legacy rules and norms for military AI. Instead, they are being written in real time. It is therefore important to develop and promulgate norms in this emerging area and build a coalition of states in support them. Moreover, such norms should address links to other key strategic areas like nuclear weapons, cyber, and space.

4. Engage with China in a clear-eyed way on military AI risks. Talks with Beijing about the risks of AI and how to bolster safety and stability are worthwhile and should move forward. The key, however, will be keeping expectations modest for what those talks can achieve. Early topics could include working toward a risk hierarchy for military AI applications; exchanging select information about test, evaluation, validation & verification (TEVV) processes; and implementation of the principle of always keeping humans in the loop for actions related to nuclear weapons.

5. Prioritize intelligence-gathering and analysis on, and net assessment of, China's military AI capabilities. China has ambitious plans for military AI and is pursuing them at a rapid pace. But whether the PLA can develop and field military AI capabilities for real-world use at scale remains to be seen. U.S. officials should allocate additional resources to tracking Beijing's progress (or lack thereof) across the full range of military AI applications. As part of that effort, U.S. intelligence should assess China's access to important data sets—for example, data Russia has gleaned from Moscow's combat systems operating in Ukraine and Syria—and algorithms that could help train AI systems for combat applications.



³³ U.S. Department of Defense, "U.S. Endorses Responsible AI Measures for Global Militaries," press release, November 13, 2023, <u>https://www.defense.gov/News/News-Stories/Article/Article/3597093/us-endorses-responsible-ai-measures-for-global-militaries/</u>.