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

---

[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), https://www.cnas.org/publications/reports/sanctions-by-the-numbers-sdn-cmic-and-entity-list-designations-on-china.

[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, 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/.

[32] Ministry of Foreign Affairs of the People's Republic of China, "Global AI Governance Initiative," Communique, October 20, 2023, https://www.mfa.gov.cn/eng/wjdt_665385/2649_665393/202310/t20231020_11164834.html; United Kingdom, "The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023," January 16, 2024, 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.

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, https://www.defense.gov/News/News-Stories/Article/Article/3597093/us-endorses-responsible-ai-measures-for-global-militaries/.