Written Testimony Before the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party

Commanding Heights: Ensuring U.S. Leadership in Critical and Emerging Technologies

Wednesday, July 26, 2023 | 7:00 PM EST | 390 CHOB

Lindsay Gorman
Senior Fellow and Head of the Technology and Geopolitics Team, Alliance for Securing Democracy
The German Marshall Fund of the United States

Introduction

Chairman Gallagher, Ranking Member Krishnamoorthi, and distinguished Members of the Select Committee, thank you for the opportunity to testify before you today.

The United States and its democratic partners have woken up to a cold reality that after decades of technological leadership, this position is under severe challenge from an autocratic rival in the People's Republic of China (PRC). At the same time, leadership in critical and emerging technologies is increasingly a dominant mode of national power, through its ability to drive economies, advance militaries, and write the global rules of the road for governance and international standards. The technological competition with the PRC is the contest of our time. This next 'decisive decade' will determine whether the next century of global governance is defined by democracy and freedom, or autocracy and control, and the determinants of that system will be the leaders in critical and emerging technologies. The United States has incredible competitive advantages in this contest – an open innovation system, robust private sector, a successful tradition of state-backed innovation, the world's envy when it comes to attracting global talent, and a strong network of allies and partners around the world. But we need to start playing our cards smarter.

I serve as the head of the Technology and Geopolitics Team at the German Marshall Fund's Alliance for Securing Democracy, where I lead a research initiative studying how democracies can together outcompete autocrats – chiefly the People's Republic of China (PRC) -- in emerging technologies. I come at this question from the perspective of a technologist with academic training in quantum physics and artificial intelligence and first-hand experience researching the technologies we now recognize as critical to U.S. national competitiveness. I recently had the privilege of serving at the White House, where I crafted technology and national security competitiveness strategy across the U.S. government. I also developed initiatives to implement that strategy, including through the US-EU Trade and Technology Council and Quad Critical and Emerging Technology Working Group. Both during my time at the German Marshall Fund and in government, I have had the opportunity and privilege of engaging extensively with officials, policy, and technology communities across the Atlantic on PRC technology matters from 5G and digital infrastructure to AI and international standards setting. Finally, I spent the first part of my career working with start-up companies and venture capital, including founding a firm looking at emerging technologies. The views I express in this testimony and before you are my own and should not be taken as representing those of my current or former employers.

For decades, the United States and its democratic partners have allowed the PRC to execute its global technology dominance strategy largely unimpeded. We naively assumed that PRC economic integration with the world would bring about both economic and political liberalization, ignorant of how that interdependence would be weaponized to propel China to technology leadership. In the face of economic opportunity in China and cheap goods and labor, we looked the other way on intellectual property theft, forced technology transfer, the deliberate effort to replace foreign technology firms with indigenous competitors, and authoritarian consolidation of power.

Today, the PRC leads in some strategic technology areas such as 5G implementation, AI surveillance, and elements of quantum communication applications and remains a fast follower in others. In short, its anti-competitive strategy has been an unmitigated success – to the detriment of democratic values worldwide. Now the United States is in a position where there is a real chance that the innovations of the 21st century and the national, military, and economic power they confer will not be driven by liberal democracies, but an autocratic power. The buck must stop here.

In my testimony I lay out the PRC's ambitions and strategy for technology dominance; discuss competition and risks in key technology areas of AI, quantum information, and biotechnology; offer ideas for how the United States should think about the technology competition; and provide 14 recommendations to Congress for how it can supercharge this effort. The United States cannot afford to rest on its laurels.

The PRC's Aims and Strategy for Critical and Emerging Technology Dominance

The PRC's Made in China 2025 strategy sets out a vision for turning China into a technology exporter in areas such as AI, quantum communications, high-performance computing, 5G mobile networks, biotechnology, and advanced materials and manufacturing. The 14th Five Year Plan emphasizes the PRC's push for technological independence and indigenous innovation. To what extent recent U.S. policy change towards countering China's unfair practices and alarm over its growing technological prowess has accelerated this push for indigenous innovation is hotly debated, but what is clear from CCP strategic documents is that reducing reliance on foreign technology was always the plan. The CCP also is clear-eyed about the competition with the United States. According to Xi, "the United States is the biggest threat to China's development and security."[1]

Of additional concern and relevance to U.S. national security interests is the PRC's long-standing effort to integrate civilian and defense technology sectors through its Military Civil Fusion (MCF) strategy. By sharing talent and resources, the PRC hopes that economic and military modernization can develop side-by-side and in ways that are mutually reinforcing.

According to the Defense Department:

> The PRC's MCF development strategy encompasses six interrelated efforts: (1) fusing China's defense industrial base and its civilian technology and industrial base; (2) integrating and leveraging science and technology innovations across

[1]He, Bin (何斌), "Speech at Special Seminar for County-Level Leading Cadre to Study and Implement the 5th Plenum of 19th Central Committee" (在县级领导干部学习贯彻党的十九届五中全会专题研讨班上的发言), Qilian News (祁连新闻), February 25, 2021, http://www.qiliannews.com/system/2021/02/25/013341147.shtml; 2022-report-20th-party-congress.pdf (ucsd.edu)

> military and civilian sectors; (3) cultivating talent and blending military and civilian expertise and knowledge; (4) building military requirements into civilian infrastructure and leveraging civilian construction for military purposes; (5) leveraging civilian service and logistics capabilities for military purposes; and, (6) expanding and deepening China's national defense mobilization system to include all relevant aspects of its society and economy for use in competition and war.[2]

While this deep integration is not a fait accompli by any means, nor is every university or company connected with the military, this strategy has implications for U.S. defensive measures that seek to limit technology flow to the PLA.

Made in China, Exported to the World. Equally important is the PRC's ability and interest in exporting its autocratic values – censorship and control chief among them – to the regions and countries globally that adopt its technology. The case study of Huawei is indicative of how the PRC turned this strategy of state-directed innovation into global control. Through heavy state subsidies, the PRC paved the way for Huawei's rise at a time when democratic investment in telecommunications stalled. As late as the 1990s Lucent and Nortel, both based in North America, cornered the telecommunications market. By 2008, Nortel went bankrupt and Lucent was sold off. Mercantilist policies that fueled the rise of Chinese telecommunications firm Huawei and ZTE in the absence of corresponding investment and recognition of this strategic industry are significantly to blame.[3] Today, Huawei's reach is global as low prices allow it to compete in developing markets and crowd out international competitors. The PRC has leveraged Belt and Road Initiative (BRI) MOU agreements and an outgoing strategy in international standards bodies to gain a leg up on standards essential patents in 5G and transmit training and autocratic capacity-building on surveillance and control. Because internet infrastructure underlies advances in the technologies built atop, facial recognition and "Safe City" technologies made in China have been exported to the world. As of 2019, Huawei supplied AI surveillance technology to at least fifty countries, many of which signed up to China's BRI.[4]

Finally, while many of China's technology strategies are practiced, they are not static. In the face of an era of heightened competition, the CCP seeks to respond, to innovate, and to modernize. The **CCP is currently overhauling its innovation system** to achieve its technological self-reliance goals and close 'chokepoints' in critical areas. In March 2023, the CCP Central Committee and State Council unveiled its Institutional Reform Plan with two major changes to its innovation enterprise: the establishment of a Central Science and Technology Commission to organize and coordinate scientific and technological work more effectively; and a comprehensive restructuring

---

[2] "2022 Report on Military and Security Developments Involving the People's Republic of China", US Department of Defense, November 29, 2022.

[3] Robert D. Atkinson. "Who Lost Lucent?: The Decline of America's Telecom Equipment Industry", *American Affairs* IV, no. 3 (Fall 2020).

[4] Feldstein, Steven, The Global Expansion of AI Surveillance, Vol. 17, Carnegie Endowment for International Peace Washington, DC, 2019.

of the Ministry of Science and Technology (MOST) for leanness and a focus on core innovation strategies. This year represents the third time that MOST has been restructured since 2018.[5]

The United States and its democratic partners have a determined competitor in the PRC that has achieved a remarkable degree of success in a relatively short period of time. It continues to innovate both in technological development and the bureaucratic mechanisms that support its goals. The worst thing the United States can do is loudly signal its intent to compete and fail to follow through on actions to optimize our competitiveness or adopt policies that inadvertently undermine it.

Competition in Critical Technology Areas: AI, Quantum Information, Biotechnology

Assessing the current state of competitiveness in key industries is inherently challenging due to a lack of centralized data and lack of agreement on what metrics determine competitiveness. According to ASPI's Critical Tech Tracker, which draws on open source publication and patent data, China's global lead extends to 37 out of 44 technologies tracked among defense, space, robotics, energy, the environment, biotechnology, AI, advanced materials and key quantum technology areas.[6] Initiatives from the Center for Security and Emerging Technology and MacroPolo come up with different estimates for leadership based on different metrics, but one thing is clear: in nearly all technology areas that the United States, the PRC, and many U.S. allies and partners such as Australia have identified, the competition is close.

The United States and its democratic partners need a systematic way of assessing both the state of competition but also the national security, supply chain, and human rights risks of this state in critical technology areas. I outline several in AI, biotechnology, and quantum information here, but rigorous analytical assessments – informed by expertise from the United States government and private sector -- across these areas and more are sorely needed.

Artificial Intelligence: In AI, a primary driver for the PRC has been state security. At times, state-directed industrial policy, PRC security needs, and technological advancement have been mutually reinforcing. The PRC surveillance industry is a case in point. A desire to suppress dissent and quell unrest drove local state governments to seed the security and surveillance industry through government contracts for security services. Companies like SenseTime and iFlyTek reaped economic and commercial benefits through the ability to tap into this data to improve AI and facial recognition systems.

---

[5] Zhang Tianqui. "Why China is Restructuring its Science and Tech Ministry", Caixin Global, March 9, 2023.
[6] Jamie Gaida, Jennifer Wong-Leung, Stephan Robin, and Danielle Cave. "ASPI's Critical Technology Tracker: The Global Race for Future Power", Australian Strategic Policy Institute, 2023.

The PRC's approach to AI regulation also includes a heavy emphasis on security and control. With the rise of generative AI, such control means limiting Chinese citizens' own ability to use generative AI tools like ChatGPT or DALL-E and Midjourney to undermine state power. In short, the CCP is worried about its ability to control the proliferation of information – text, images, and videos that could spread politically liberal ideas or undermine the Communist Party leadership. In April, the Cyberspace Administration of China released draft rules for generative AI that insist companies adhere to Chinese censorship rules with AI systems that "reflect socialist core values." Under the rules, generative AI providers would be required to apply to the CAC for a security assessment and are also responsible for content produced by their systems.[7] Whether these rules will succeed in steering innovation to support CCP objectives or create burdensome compliance requirements and an environment that stifles innovation is a central question for PRC's competitiveness in Large Language Models (LLMs) and the applications built on top of them.

One risk that policymakers must guard against is that PRC norms of censorship and surveillance get baked into global standards on AI out of a continuing desire for market access. AI image generator Midjourney CEO David Holz has already laid his cards on the table. He is quoted as saying on Discord that the company's objectives are to "minimize drama." "Political satire in china is pretty not-okay…the ability for people in China to use this tech is more important than your ability to generate satire." Midjourney blocked images of Xi Jinping, despite allowing satire of other political leaders, though in its initial release was fairly easy to evade.[8] Amidst significant attention to concern around deepfakes, algorithmic harms, and the threat of AI-driven extinction, these geopolitical questions concerning freedom of expression should not receive a pass in TTC or G7 processes on AI. Free expression is what is at stake in the quest for technological dominance.

Biotechnology: In biotechnology, the PRC is amassing global bio data, taking advantage of partnerships with BGI, Huawei and firms like WuXi App Tech, which has been associated with popular genetics company 23andMe. As is the case in many strategic industries, concerning pieces of China's biotechnology industry can be tied directly to U.S. partnerships. In 2012, Chinese biotech giant BGI received CFIUS clearance to acquire California-based Complete Genomics.[9] Today, multiple BGI affiliates, including BGI Research and BGI Tech Solutions, have been placed on the U.S. Entity List for their collection and analysis of genetic data that risks contributing to PRC surveillance and monitoring, as well as the risk of diversion to military programs. As innovators globally incorporate AI into biotechnology, these concerns will grow. Despite being flagged by CFIUS over a decade ago, the rise of BGI demonstrates a complete failure of imagination to envision the drivers of national power and the risks of autocratic biotechnology competitiveness. Few guardrails today apply.

---

[7] Seaton Huang, Helen Toner, Zac Haluza, Rogier Creemers, and Graham Webster, "Translation: Measures for the Management of Generative Artificial Intelligence Services (Draft for Comment)", DigiChina, Stanford University, April 2023

[8] Isaac Stanley-Becker, and Drew Harwell, "How a tiny company with few rules is making fake images go mainstream", The Washington Post, March 30, 2023.

[9] "BGI-Shenzhen and Complete Genomics, Inc. Receive CFIUS Clearance for BGI-Shenzhen's Proposed Acquisition of Complete Genomics, Inc.", Securities and Exchange Commission, December 28, 2012.

Quantum Information: In quantum information, the PRC has led in large-scale applications of quantum communications. In 2016, it launched the world's first quantum satellite (Micius) – enabled in part by German and EU funding.[10] It continues to test technologies through its Quantum Experimentation at Space Scale (QUESS) quantum-enabled communications satellite, including sending quantum keys for use in quantum cryptography between Austrian and Chinese ground stations. Concerns over military applications in counter-stealth and counter-submarine technologies as well as the potential to break classical encryption drove Entity List additions of PRC quantum technology entities including QuantumCTek. Unlike some of the other strategic technology areas discussed, competition in quantum computing is truly a race to a universal fault-tolerant quantum computer, which carries the ability to break the classical encryption services that modern secure systems rely on. There is a case, therefore, to be made for taking steps to put the United States in a significant leadership position towards this goal, akin to new U.S. posture outlined by National Security Advisor Jake Sullivan on foundational semiconductors to seek "as large of a lead as possible."

These are but 3 of the key areas in which the PRC is midway through its aims to supplant U.S. technology leadership, including via direct technology acquisition. As the Defense Department has assessed, "China also excels at high-speed railways, electric vehicles, and numerous aspects of the digital ecosystem, such as big data analytics and cloud computing." [11] The overarching takeaway is that China is "at or near the frontier" in numerous CET areas, in part due to decades of U.S. inattention.

U.S. Technology Competitiveness: Leveraging Our Strengths and Playing Defense

I offer a few points to consider in the formulation of U.S. competitiveness strategy and considerations around derisking or decoupling:

- First, our strategy needs to **capitalize on our own sizeable competitive advantages** – a robust open innovation ecosystem, human capital at home and from abroad, and a strong network of allies and partners – in this fight.
- Modern industrial policy should recognize that the history and success of U.S. innovation has not occurred in spite of the state or due to an unregulated free market environment, but because of it. Much of the PRC's MCF strategy seeks to emulate the success of the U.S. Defense Department in seeding private sector technologies from GPS to autonomous vehicles. As Mariana Mazzucato points out in her seminal work "The Entrepreneurial State," the major technical components of the iPhone from its GPU to its LCD were

[10] China's quantum leap — Made in Germany, Deutsche Welle (DW), Sandra Petersmann and Esther Felden. June 13, 2023.
[11] Department of Defense. "Military and Security Developments Involving the People's Republic of China". A Report to Congress. Pursuant to the National Defense Authorization Act of 2000. Washington: Government Printing Office, 3 November 2021.

derisked and made possible by strategic investment by the U.S. government to overcome technical and market barriers that the private sector would not take on.[12]

- Even as it studies the CCP's strategies, the United States must not seek to emulate China, or take actions that would undermine our own competitiveness. Similarly, however, allowing the PRC to execute its technology dominance strategy unobstructed is not an option. To ensure US – and I would added allied – leadership to CET, we must specifically tease out and counter elements of that strategy from intellectual property theft and forced technology transfers to gathering global genetic data.
- In the face of the PRC's ambitions, it is tempting to paint Xi and the CCP as 10 feet tall. In fact, many core elements of the PRC's technology dominance strategy are born out of a fear that China will not be able to indigenize quickly enough. Its talent programs were set up in response to 'brain drain' to the United States; and many efforts to beg, borrow, and steal critical technologies are attempts to remove dependencies and chokepoints from foreign suppliers. The United States needs to recognize and leverage its strategic advantages across supply chains, talent, and the attractive power of free societies.
- The approach we need draws on **both de-risking** supply chains for resilience as well as a **targeted strategic decoupling** from the PRC military and its human rights abuses. Simply put, U.S. investors should not be directly aiding and abetting these efforts with homegrown U.S. innovation and capital.

Policy Recommendations for Congress

Expand U.S. and Allied Analytical and Policy Capacity on Technology Competition

These questions of de-risking, decoupling, and economic and technological engagement with the world's second largest economy cannot be made in a data vacuum. Expanding our defensive measures as well as knowing which CET areas to prioritize year over year and how requires robust data and analysis.

1) Establish a National Technology Competitiveness Analysis Center (NTCAC) modelled after National Counterterrorism Center or National Counterintelligence Center, to conduct red-blue team analyses on critical and emerging technology ecosystems. This center should draw on expertise across the federal government, such as in the national labs and DOD, in addition to industry analysis, and include input from the intelligence community on

[12] Mariana Mazzucato. "The Entrepreneurial State: Debunking Public vs. Private Sector Myths".

areas of PRC IP theft, the state of technology transfer, and identification and tracking of chokepoints.

2) Build out joint competitive analytic capacity with key allies and partners. The Quad Critical and Emerging Technology effort on Horizon Scanning is a first step, but this effort needs deeper resourcing, including involving Five Eyes partners.

3) Guided de-risking: Adopt a framework with key allies and partners to measure the PRC's technological control in a given country or region. My team at GMF has developed a proof of concept of this analysis on China's Digital Technology Stack. Building a true allied understanding of China's penetration in global technology ecosystems is the first step towards robust allied competitiveness and a common operating picture of the threat. Such analysis can also guide G7 and multilateral development efforts.

4) Increase information sharing on IP theft.

Invest in U.S. Enduring Advantages

Iteratively, continuously, and for a sustained period over at least the next decade, the United States needs to leverage its key competitive advantages: innovation ecosystem, human capital at home and from abroad, network of allies and partners. It should also consider what true allied competitiveness would look like.

5) Pass legislation to build a iterative structure for technology investment planning. The White House Office of Science and Technology Policy has issued a list of priority areas for Critical and Emerging Technologies, but these advances are not static. With the advent of superior Large Language Models, today's list would likely even look a bit different from the one guiding technology resource planning now. The CHIPS and Science Act is an excellent start in reversing the chronic public underfunding of U.S. R&D. Congress should build in an iterative process that takes inputs from the NTCAC and drives budgetary planning in R&D, workforce initiatives, and defensive measures such as export controls, CFIUS, and outbound investment screening.

6) Invest in the US-EU Trade and Technology Council and Quad for semi-permanence*:* Congress should build a line-item into the State and Foreign Operations budget to support the TTC over a 5-10 year timescale. Connective tissue is important, and bureaucratic mechanisms take time and effort to stand up and to build trust. Congress can help insulate this mechanism from changing political winds in the United States, while providing the means for its strategic evolution and adaptation over time.

7) Double down on allied competitiveness through innovation initiatives in AI, Biotechnology, and 6G. A Human-Genome-style effort to build next generation bio data for democracies should be part of this list. I offer this report, A Future Internet for

Democracies: Contesting China's Push for Dominance in 5G, 6G, and the Internet of Everything, for further specific recommendations for joint competitiveness initiatives on AI and 6G.[13]

8) Invest in Responsible AI and Write the Rules of the Road with Allies and Partners. Privacy-preserving and explainable AI are areas that advance democratic values but need government investment to de-risk and make viable. Content authenticity architectures can protect the democratic information environment from manipulation and prioritize credible information in an era of exploding deepfakes and AI-generated media. Finally, as the US builds out its own AI regulatory efforts, it should identify areas where a common allied approach can provide a distinct, high-standards democratic offering to third countries.

9) Reform immigration to prioritize the retention of top tech talent. Measures include expansions of the H1B and OPT via programs to capitalize on the US ability to attract and retain top talent.

10) Fund workforce initiatives in biodata and biomanufacturing to strengthen the U.S. bioeconomy.

Counter the PRC's Technology Indigenization Strategy via Defensive Measures

A laissez-faire approach to competition is no longer sufficient. The Untied States, along with its key allies and partners, must unwind the ways that innovations and capital from democracies inadvertently undermine democratic values through the prism of the CCP's technology dominance strategy.

11) Develop a new multilateral export control regime for critical and emerging technologies that includes a strong consideration of human rights abuses. Existing, Cold War-era regimes such as the Wassenaar Arrangement are inadequate to address the explosion of dual-use technology across all segments of society as well as their democracy and human rights implications. Many allied export control regimes lack or are just developing the capacity to implement end-user controls. Few are structured to account for human rights abuses. Yet multilateralizing U.S. defensive policies is essential to their success.

12) Pursue targeted outbound investment screening and coordinate with allies and partners: While discussions on outbound investment screening are further ahead in the US, aligning approaches and critical technology sectors with Europe can help drive allied competitiveness. At a minimum, screening tools should include restrictions on private

[13] Lindsay Gorman. "A Future Internet for Democracies: Contesting China's Push for Dominance in 5G, 6G, and the Internet of Everything", Alliance for Securing Democracy at the German Marshall Fund, October 27, 2020.

investment to entities on the Entity List and Treasury's NS-CMIC. Ensure coordination amongst these lists and use sector-specific outbound investment screening to close loopholes in export controls aimed at exploiting chokepoints.

13) Pass legislation on a risk-based framework for assessing ICTS platforms operating in the United States and lead by example on autocratic apps. Develop an international coalition a comprehensive, risk-based framework for autocratic internet apps -- democratic allies and partners to develop a comprehensive framework for addressing the threats posed by authoritarian internet apps and critical information infrastructure. TikTok and Huawei are not one-offs. We cannot treat them as such. As we head into the 2024 election season with more American than ever getting their news from a platform whose parent company answers to the CCP, there is true urgency.

14) Pass Federal Data Privacy and Data Security Legislation. We cannot solve technology espionage through data privacy alone, but we can close loopholes and punish excess abuses.

Above all, the United States holds an incredibly strong hand in this competition. We must start playing our cards and well.