Written Testimony Before the Senate Committee on Banking, Housing, and Urban Affairs

Hearing on National Security Challenges:
Outpacing China in Emerging Technology

Thursday, January 18, 2024
10:00 AM EST
Dirksen Senate Office Building 538

Lindsay Gorman

G | M | F Alliance for Securing Democracy

Introduction

Chairman Brown, Ranking Member Scott, and Members of the Committee, thank you for the opportunity to testify before you today.

I lead a research and analysis team at the German Marshall Fund's Alliance for Securing Democracy, studying how democracies can together outcompete autocrats – chiefly the People's Republic of China (PRC) – in emerging technologies. I am also a Venture Scientist with Deep Science Ventures. 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 U.S.-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.

Toward a New Mode of Techno-Economic Statecraft

The United States has spent decades investing in, inventing, and re-inventing new modes of warfare – from the Goldwater-Nichols Act to the first, second, and third offset strategies. And today, inspired in part by rapid capability-fielding in Ukraine, we are undergoing a transformation to enable the Pentagon to draw more effectively on private sector innovation for rapid capability deployment. Each of these offset strategies was aimed at a particular objective and a shift in adversary capability, largely in and around the role of nuclear weapons. Today, the United States's strongest autocratic rival is using tactics in economic, technological, and societal realms that a defense-first national security apparatus was not designed to counter. In the PRC, we face a competitor who wields its own economic power to coerce nations, businesses, and individuals to achieve its technology and national security objectives. This multi-sectoral competition has strained the post-Cold War view of international relations in which more economic engagement implied greater political – even democratic – proximity. The cost of doing business in China is often the hollowing out of technology advantages and IP, described as the greatest transfer of wealth in human history. The CCP also is clear-eyed about competition with the United States. According to Xi, "the United States is the biggest threat to China's development and security."[1]

[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),

So how does the United States best compete with an autocratic rival where that competition is playing out chiefly in non-traditional spheres of battle: technology, economy, and society, in addition to military capability build-ups? Much in the way the Cold War led to a society-wide reworking of our institutions towards great power competition, so too now do we need a rethink of our tools. A key element of this effort is building out a doctrine, toolkit, and alliances for techno-economic statecraft.

We are not starting from whole cloth. Some of these tools already exist, but many were designed for a different era, when the chief concern was preventing the development of Weapons of Mass Destruction (WMD).[2] The remit was far simpler: ensure that technology items with a 'dual-use' capability – i.e., those that could be used for both military and civilian applications – were used for the latter and not the former. Moreover, these dual applications often had clear signatures and relatively long timescales on which a civilian capability could transition to a WMD use. Nuclear energy vs. nuclear weapons is the canonical example, where uranium enriched above a certain threshold becomes weapons-grade and thus a proliferation concern.

These modes are outdated and unfit for our modern challenges for three reasons. First, straightforward distinctions and thresholds between military and civilian applications of emerging technologies in many cases do not exist. Emerging technologies like artificial intelligence, quantum information systems, advanced computing, and biotechnology are *inherently* dual-use. The same quantum computer that could revolutionize chemistry calculations and scientific discovery could break the encryption that secures our communications with submarines. The same synthetic biology and genomic engineering processes that could engineer novel cancer therapies could engineer pandemic pathogens. And the same computing capacity that fuels Large Language Models can fuel drone swarms or societal surveillance. AI is often described as falling into a class of technologies that economists refer to as 'general-purpose technologies' – akin to electricity, the steam engine, or the internal combustion engine.[3] There are no thresholds to set when determining what constitutes a dual use of an internal combustion engine.

Second, the PRC has pursued an explicit strategy of military-civil fusion (MCF) that further blurs the lines of these domains and makes it difficult to have confidence that any civilian use will stay a civilian use. 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:

February 25, 2021, http://www.qiliannews.com/system/2021/02/25/013341147.shtml; 2022-report-20th-party-congress.pdf (ucsd.edu)

[2] *Advancing National Security and Foreign Policy Through Sanctions, Export Controls, and Other Economic Tools, Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs*, 118th Cong. (2023) (statement by Kevin Wolf, Partner at Akin Gump Strauss Hauer & Feld LLP and Senior Fellow at the Center for Security and Emerging Technology)

[3] Erik Brynjolfsson and Andrew McAfee, "The Business of Artificial Intelligence," Harvard Business Review, July 18, 2017, https://hbr.org/2017/07/the-business-of-artificial-intelligence.

> 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 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**.[4] [emphasis added]

And third, not all the national security risks associated with PRC emerging technology acquisition and dominance fall into the military domain. Human rights abuses, the promotion of autocratic values and standards baked into emerging technologies, and strategic economic and technological dependence of critical supply chains fall outside the scope of structures aimed at the traditional conception of dual use.[5]

Today, a growing list of 'defensive technology measures' for techno-economic statecraft include:

- Export controls
- Sanctions
- Supply Chain Due Diligence
- Investment Screening
    - Inbound investment
    - Outbound investment
- Anti-dumping measures
- Research security
- Prosecution of IP theft
- Tariffs on high-tech industries

A new doctrine for techno-economic statecraft must survey and leverage U.S. and allied advantages (and realistically assess willingness to fuse these ecosystems), deepen capabilities, and define short-, medium-, and long-term objectives for technology competition. It must be supported by a robust analytical and intelligence apparatus and resourced appropriately. And it must blend proactive ('promote') tools with defensive ('protect') technology measures. On the

[4] U.S. Department of Defense, "2022 Report on Military and Security Developments Involving the People's Republic of China2022 Report on Military and Security Developments Involving the People's Republic of China", US Department of Defense, November 29, 2022,

[5] Lindsay Gorman, "The U.S. Needs to Get in the Standards Game – With Like-Minded Democracies," Lawfare, April 2, 2020, https://www.lawfaremedia.org/article/us-needs-get-standards-game%E2%80%94-minded-democracies; Cyberspace Solarium Commission Report (United States Cyberspace Solarium Commission, 2020), https://www.solarium.gov/report; Paul Mozur and Don Clark, "China's Surveillance State Sucks Up Data. U.S. Tech is Key to Sorting It.," New York Times, November 22, 2020, https://www.nytimes.com/2020/11/22/technology/china-intel-nvidia-xinjiang.html.

latter, outpacing China no longer simply means outrunning the PRC but also impeding its capabilities in select game-changer and 'force-multiplier' technologies. The stated goal of National Security Advisor Jake Sullivan in the context of foundational semiconductors "to maintain as large of a lead as possible" will require the United States and its allies to **control capabilities, not only technologies**.

Emerging Technologies' Inputs: Considerations for Control

Critical to a strategy for techno-economic statecraft is the selection of objectives in critical technology areas that drive considerations for how their transfer may be controlled. I discuss several such considerations in the cases of AI, biotechnology, and quantum information technologies. All three can be thought of in terms of their data, software, and 'hardware' (or 'bio-ware') inputs. Hardware is the most straightforward to control, but new advances may render that focus insufficient.

Artificial Intelligence: Inputs to AI include data to train models on, algorithms to build those models and perform the training, and computing power to process this development.[6] Pioneering controls on the PRC's AI capabilities issued on October 7, 2022 focused on hardware – exploiting a chokepoint to stifle the flow of ultra high-end semiconductor technology, specialized manufacturing tools, and manufacturing capacity to China. With complex controls including end user applications of the Entity List and Foreign Direct Product Rule, end use controls, PRC-wide controls, and restrictions on U.S. persons, they demonstrate a holistic approach to controlling capabilities. Netherlands and Japan enacted similar controls, though Germany, whose Zeiss and Trumpf laser and optoelectronics firms supply the Dutch ASML for lithography equipment, has not. Moreover, Chinese developers are already finding workarounds, and smuggling networks risk blunting the controls' effects. One glaring loophole is the ability to access equivalent processing power using cloud computing infrastructure. With the advent of frontier models, whether to restrict their application in specific end uses including military and human right abuses will need to be considered as well. Indeed, the most fraught elements of the Treasury Department's Advanced Notice of Proposed Rulemaking on outbound investment included the breadth of AI and the ability to circumvent military end-uses dependent on exclusive or primary use.[7]

Biotechnology: Inputs to biotechnology advances include: genetic material (DNA, RNA, genomes); data (such as genetic data); bioinformatics tools and advanced computing (such as software and algorithms for analyzing biological data); specialized biological components

[6] Export Control Reform Implementation: Outside Perspectives, Hearing Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, 115th Cong. (2019) (statement of Ben Buchanan, Assistant Teaching Professor, School of Foreign Service, Senior Faculty Fellow, Center for Security and Emerging Technology, Georgetown University).

[7] "Outbound Investment Program," U.S. Department of the Treasury, https://home.treasury.gov/policy-issues/international/outbound-investment-program; Department of the Treasury, "Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern," Federal Register Vol. 88 no. 155 (August 14, 2023): https://www.govinfo.gov/content/pkg/FR-2023-08-14/pdf/2023-17164.pdf.

(molecules and materials harvested organically or synthetically produced); and specialized equipment (such as DNA sequencers or bioreactors). However, China's biomanufacturing ecosystem is highly developed, leading to strategic dependencies for the United States in advanced pharmaceutical ingredients and making prospects for technology controls difficult.[8]

The story of Beijing's genetic data rise is also one of failed defensive technology measures ill-adapted to a new reality. 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 the popular genetics company 23andMe. 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.[10] However, BGI maintains a network of over 200 global subsidiaries, most of whom are not on the Entity List, allowing it access to genomic data from around the globe.[11] 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 – a mistake the United States cannot afford to repeat and must attempt to better forecast.[12]

Quantum Computing and Information Technologies: In quantum information, the PRC has led in large-scale applications of quantum communications. These technologies aim to encrypt information using quantum key distribution (QKD) that may be theoretically more tamper-proof. In 2016, China launched the world's first quantum satellite (Micius) – enabled in part by German

---

[8] Jeffrey Algazy, et al., Vision 2028: How China could impact the global biopharma industry (McKinsey & Company, 2022), https://www.mckinsey.com/~/media/mckinsey/industries/life%20sciences/our%20insights/vision%202028%20how%20china%20could%20impact%20the%20global%20biopharma%20industry/vision-2028-how-china-could-impact-the-global-biopharma-industry.pdf

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

[10] Countering China: Advancing U.S. National Security, Economic Security, and Foreign Policy, Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, 118th Cong. (2023) (statement of Thea D. Rosman Kendler, Assistant Secretary of Commerce for Export Administration).

[11] Advancing Growth, Knowledge, and Innovation through Higher Education, Before the U.S.-China Economic and Security Review Commission hearing on
"China's Challenges and Capabilities in Educating and Training the Next Generation
Workforce," 118th Cong. (2023) (statement of Anna B. Puglisi, Director of Biotechnology Programs at Center for Security and Emerging Technology, Georgetown University).

[12] Commanding Heights: Ensuring U.S. Leadership in Critical and Emerging Technologies, Before the House Select Committee on the Competition Between the United States and the Chinese Communist Party, 118th Cong. (2023) (statement of Lindsay Gorman, Senior Fellow and Head of the Technology and Geopolitics Team, Alliance for Securing Democracy, The German Marshall Fund of the United States).

and EU funding.[13] 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. Quantum communications is also an increasing area of Sino-Russian collaboration, as the no-limits partnership blossoms in the technology and information arena. In December 2023, Chinese and Russian scientists demonstrated the encrypted communication using quantum key distribution of images between ground stations in Urumqi, Xinjiang and outside Moscow, by way of China's quantum satellite.[14]

However, the real competition in quantum computing is the race to a universal fault-tolerant quantum computer, which carries the ability to break the classical encryption services that modern secure systems from our intelligence apparatus to our nuclear deterrent 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. 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. And some post-quantum cryptography algorithms are subject to BIS export licenses. Proposed outbound investment controls would prohibit covered investments into quantum computers and components (such as cooling systems), quantum sensors, quantum networking and communication systems, as well as low-temperature semiconductors operating under 4.5 Kelvin used for quantum chips.[15] Here, technology forecasting and tracking will be essential to defensive measures, as preferred approaches are still evolving with scientific research.[16]

Building and Resourcing the Defensive Technology Measures Toolkit

Just as we have spent decades resourcing the U.S. military for strategic advantage, so too we must resource the tools of techno-economic statecraft. At the heart of this effort is the Commerce Department and specifically its Bureau of Industry and Security, charged with implementing and enforcing export controls on critical and emerging technologies and helping to secure the nation's supply chains.

Here, I offer three categories of recommendations:

---

[13] Sandra Petersmann and Esther Felden, "China's quantum leap – Made in Germany," *Deutsche Welle*, June 16, 2023, https://www.dw.com/en/chinas-quantum-leap-made-in-germany/a-65890662.

[14] Xu Ning, "How important is it for China and Russia to cooperate in testing quantum satellite communications? Who is stronger in the United States and China?" *VOA News*, January 11, 2024, https://www.voachinese.com/a/us-china-russia-quantum-communication-20240110/7434011.html.

[15] "Outbound Investment Program," U.S. Department of the Treasury, https://home.treasury.gov/policy-issues/international/outbound-investment-program; ANPRMDepartment of the Treasury, "Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern," Federal Register Vol. 8 no. 155 (August 14, 2023): https://www.govinfo.gov/content/pkg/FR-2023-08-14/pdf/2023-17164.pdf.

[16] Edward Parker, *Promoting Strong International Collaboration in Quantum Technology Research and Development* (RAND Corporation, 2023), https://www.rand.org/pubs/perspectives/PEA1874-1.html; Edward Parker, et al., *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology* (RAND Corporation, 2022), https://www.rand.org/pubs/research_reports/RRA869-1.html.

1. **Significantly expand U.S. and allied analytical capacity**. In order to make informed decisions on which levers of the techno-economic toolkit to pull, the United States needs a significant analytical capability that can forecast technology areas and needs, analyze the effects of techno-economic measures, assess U.S. leadership potential and China's indigenization prospects in critical technology areas, and wargame techno-economic actions and responses. As Daleep Singh told this Committee, economic wargames should model the extensive wargaming the Pentagon conducts for military affairs.[17]

   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. It should also include input from the intelligence community on areas of PRC IP theft, the state of technology transfer, and identification and tracking of chokepoints. This center could be housed at the Commerce Department and report to the Secretary's Office with a dotted line reporting structure to the ODNI. It should include a wargaming cell dedicated to conducting red-blue team exercises in the techno-economic sphere.

2. **Increase funding for personnel, but also technology tools**. BIS's overall budget has not kept paced with its growing responsibilities. In the Commerce Department's FY 2023 budget request, BIS identified more than $53 million in unfunded requirements.[18] These included ICTS supply chain security, additional Special Agents and Enforcement analysts to keep pace with the rise cases related to China and Russia, industry survey studies, the use of data to assess the effectiveness of licensing systems, and expanding a partnership with Canada on securing supply chains.[19] In FY2024, that number was $14 million, including elements of developing a modern Data Science and Impact Analysis Capability.[20] The FY 2024 budget requests a $31 million increase in BIS budget from FY 2023.

   Congress should at minimum fully fund this request, $16.866 million of which accounts for inflationary adjustments, and increase BIS's FY 2024 budget to fund its $14 million in unfunded priorities.

---

[17] *Advancing National Security and Foreign Policy Through Sanctions, Export Controls, and Other Economic Tools, Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs*, 118th Cong. (2023) (statement by Daleep Singh, former Deputy National Security Advisor for International Economic and Deputy Director of the National Economic Council).

[18] Gregory C. Allen, Emily Benson, and William Alan Reinsch, *Improved Export Controls Enforcement Technology Needed for U.S. National Security* (Center for Strategic and International Studies, 2022), https://www.csis.org/analysis/improved-export-controls-enforcement-technology-needed-us-national-security.

[19] U.S. Department of Commerce, Bureau of Industry and Security, *Fiscal Year 2023 President's Budget Request*, 2023, https://www.commerce.gov/sites/default/files/2022-03/FY2023-BIS-Congressional-Budget-Submission.pdf.

[20] U.S. Department of Commerce, Bureau of Industry and Security, *Fiscal Year 2024 President's Budget Request*, 2024, https://www.commerce.gov/sites/default/files/2023-03/BIS-FY2024-Congressional-Budget-Submission.pdf.

Moreover, U.S. techno-economic competition should be resourced with cutting-edge tools, including leveraging technologies like AI and data science to track smuggling networks that help evade controls, and keep pace with the proliferation of subsidiaries and shell companies that regularly spin up from companies on the Entity List. Automatic systems could flag new entities that may be owned in whole or in part by listed entities. Knowledge graphs or link-analysis tools could modernize BIS's ability to trace smuggling networks, track shell companies, and fuse data from Chinese-language technology and financial sources to discern whether and how controls were being violated. The U.S. Army, for example, uses such software to manage a 3 TB database to forecast logistical needs for replacement parts, calculate mean time for failure rates, perform multi-dimensional cost comparisons, and inform budget requirements – slashing needed employee hours by 88%.[21] MITRE's Cygraph analyzes large loads of isolated data and optimizes pattern recognition to find and stop cyber-attacks.[22] Tools like expanded versions of the Australian Strategic Policy Institute's China Defence Universities Tracker can help analysts discover and prevent export controls evasion by elucidating the complex linkages among PRC actors with military-industrial ties. The datasets relevant to export enforcement are likely harder to come by, but no less critical. Finally, controlled hardware parts could embed geolocation tagging so that export enforcement analysts could track their movement globally.[23]

To address concerns around data security and influence stemming from autocratic ICTS platforms, Congress should:

a. 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 Americans than ever getting their news from a platform whose parent company answers to the CCP, there is true urgency.

b. 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.

[21] Neo4j, "Neo4j Keeps the Army Running by Tracking Equipment Maintenance," accessed January 17, 2024, https://neo4j.com/case-studies/us-army/.
[22] Neo4j, "Graph Technology Powers Cybersecurity Situational Awareness That's More Scalable, Flexible & Comprehensive," accessed January 17, 2024, https://neo4j.com/case-studies/mitre/.
[23] Chris Miller and Jordan Schneider, "How to Stop Our High-Tech Equipment From Arming Russia and China," *New York Times*, December 29, 2023, https://www.nytimes.com/2023/12/29/opinion/chips-semiconductor-china-russia-military.html.

3. **Build capacity among U.S. allies and partners on novel techno-economic statecraft tools and approaches.** As business groups from the Semiconductor Industry Association to the National Foreign Trade Council have exhorted, unilateral controls harm U.S. businesses relative to allied foreign competitors, as these competitors simply backfill the void created by U.S. exits in the context of remaining market demand.[24] The extent and timescale over which this backfilling is possible depends on the degree to which U.S. industry corners the market, but unilateral controls do risk the United States shooting itself in the foot, especially if such controls end up being insufficient to meaningfully limit PRC capabilities at issue due to allied backfilling. For these reasons, multilateral action is a necessity. The challenge is that democratic nations are experimenting with new tools, new authorities, new uses, and new modes of statecraft themselves, at the same time as there is a need to implement these measures jointly.

   On export controls and outbound investment screening, FIRRMA's expansion of CFIUS for inbound investment screening provides a strong model for international cooperation. FIRRMA included three provisions to aid U.S. allies and partners in strengthening their own investment screening mechanisms[25]:

   - ***A formal process for information transfer*** to allow for shared understanding of national security rationales for investment screening among U.S. allies and partners.
   - ***Outreach and technical support***. Treasury conducted international outreach and offered technical support and capacity-building for countries interested in constructing investment review mechanisms.
   - ***Incentives to strengthen screening mechanisms***. At the same time, FIRRMA's implementing regulations created a category of "excepted foreign states, whose covered investments into the United States could be subject to less rigorous review, provided these states had developed robust enough investment screening mechanisms in their own right."

While incomplete, this process has been a resounding success. In 2019, the European Commission announced guidelines to encourage member states to stand-up formal investment review procedures. As of October 2023, 21 EU member states had screening mechanisms (up from 11 in 2017), and several others are in the process of adopting an investment review regime.

---

[24] Semiconductor Industry Association, "Comments of the Semiconductor Industry Association on Advanced Notice of Proposed Rulemaking regarding Review of Controls for Certain Emerging Technologies" (public comment, 2019), https://www.regulations.gov/document/BIS-2018-0024-0130; National Foreign Trade Council, "Comment on Advanced Notice of Proposed Rulemaking Regarding Review of Controls for Certain Emerging Technologies" (public comment, 2019), https://www.regulations.gov/document/BIS-2018-0024-0081.

[25] John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115*th* Cong. (2018).

This international technical assistance capacity should be expanded in the context of outbound investment screening and replicated at the Commerce Department in the context of export controls.[26]

Complementary to this effort, the United States should:

a. 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, a more permanent commitment, and the eventual involvement of Five Eyes partners. The US-EU Trade and Technology Council's work on investment security can be a natural jumping off point for this cooperation in the transatlantic context, where the United States should seek to build capacity and shared understanding at the European Commission, even as many measures will be implemented at the Member State level.

b. Invest in the U.S.-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 five-to-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.

c. 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.[27] 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.

d. Coordinate targeted outbound investment screening with allies and partners, including information sharing mechanisms. While discussions on outbound investment screening are further ahead in the U.S., aligning approaches and critical technology sectors with Europe can help drive allied competitiveness. At a minimum, screening tools should include restrictions on private investment to entities on the Entity List and Treasury's NS-CMIC. The U.S. must ensure

[26] European Commission, "EU foreign investment screening and export controls help underpin European security," October 19, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5125.

[27] Lindsay Gorman, *A Future Internet for Democracies: Contesting China's Push for Dominance in 5G, 6G, and the Internet of Everything* (The Alliance for Securing Democracy, 2020), https://securingdemocracy.gmfus.org/future-internet/; Bryce Barros, Nathan Kohlenberg, and Etienne Soula, *China and the Digital Information Stack in the Global South* (The Alliance for Securing Democracy, 2022), https://securingdemocracy.gmfus.org/china-digital-stack/.

coordination amongst these lists and use sector-specific outbound investment screening to close loopholes in export controls aimed at exploiting chokepoints.

e. 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.

U.S. allies and partners have an extremely strong hand to play if they act thoughtfully, decisively, and multilaterally in building out the doctrine and tools of techno-economic statecraft. I look forward to your questions.