Testimony before the U.S.-China Economic and Security Review Commission
Hearing on "China's Pursuit of Defense Technologies: Implications for U.S. and Multilateral Export Control and Investment Screening Regimes"
Panel III: Policy Tools for the United States and Its Allies and Partners

Martijn Rasser
Managing Director, Datenna, Inc.

April 13, 2023

Chairman Bartholomew, Vice-Chairman Wong, and other members of the commission, thank you for the opportunity to appear before you. The views I express today are my own, not of my employer. My views were shaped during my nearly four years as a senior fellow and subsequently as director of the technology and national security program at the Center for a New American Security.

Acknowledgments:
I wish to thank John Costello, Tim Fist, Sam Howell, Hannah Kelley, Emily Kilcrease, Megan Lamberth, Ryan Morhard, Emily Weinstein, and Kevin Wolf, whose insight and ideas are reflected in this document.

Introduction

Technology is at the center of the global strategic competition and a key enabler of economic, political, and military power. On this, leaders in Washington and Beijing agree. Chinese President Xi Jinping has repeatedly made this point in speeches. U.S. President Biden's 2022 National Security Strategy states so explicitly. This tenet is now crystallizing a fundamental shift in how U.S. leaders are conceiving of technology strategy and executing technology policies.

Export controls are a key component of this new strategy. To understand the role of economic statecraft, it is important to first take a step back and view these measures in the broader context.

Promote, Protect, Partner

On September 16, 2022, U.S. national security advisor Jake Sullivan gave a speech outlining a strategy with four pillars to renew and maintain U.S. technological leadership. In essence, this strategy has three thrusts: promote, protect, and partner. The 'promote' agenda comprises two pillars: investing in America's science and technology ecosystem and nurturing top STEM talent. The 'protect' agenda is about safeguarding U.S. technological advantages. The fourth pillar comprises the 'partner' agenda—deepening and integrating U.S. alliances and partnerships. Throughout, the focus is on three families of technologies. Computing-related technologies such as semiconductors and artificial intelligence, biotechnologies and biomanufacturing, and clean energy technologies.

The promote agenda is the most straightforward of the three. It includes investments in R&D, education, and S&T infrastructure, but also changes to immigration processes to attract and retain foreign talent. A new American industrial policy is a cornerstone of this agenda.

The protect agenda relies on longstanding tools to counter unwanted tech acquisitions—export controls most notably—but the prior premise of maintaining relative advantage over China is upended. The most important part of Sullivan's speech was codifying that the new baseline is to maintain as large of a lead as possible in certain technologies, with advanced logic and memory chips served up as the example. Another part of this agenda will be restrictions on outbound investments, expected to be announced in an executive order later this year.

Finally, the partner agenda considers how the United States should collaborate with allies and strategic partners. This is a sensible and pragmatic approach. It doubles down on one of America's great, unmatched strengths: its vast network of friends, which are predominantly tech-leading democracies. It also reflects the reality that the United States rarely has all the pieces of the puzzle for any tech area of consequence, given the global diffusion of technology and requisite knowledge. Tech partnerships are a strategic necessity.

Chipping Away

Semiconductors, or chips, are case in point to show how this new tech-focused geopolitical strategy is taking shape. Chips are a foundational technology essential to the functioning of modern society, being important components in products such as consumer electronics, medical devices, supercomputers, and military systems. Recent legislation and policy action touch on all three agendas.

The marquee item in the promote agenda is the CHIPS and Science Act. The semiconductor-focused portion of the sprawling bill provides $52 billion in manufacturing investment tax credits, research and development, and workforce training. The bulk of the funds, $39 billion, will go toward incentives for new semiconductor fabrication facilities, or fabs, in the United States. U.S. political leaders and national security pundits have fixated on fabs, and for good reason. In 1990, the United States had a 37 percent share of global semiconductor production. By 2022, that share had dropped to 12 percent. The incentives prompted Taiwanese firm TSMC and U.S. firm Intel to announce construction of new fabs in Arizona and Ohio, among a slew of investments by other manufacturers and suppliers.

The other big salvo in the technology competition was in the protect agenda. On October 7, 2022, the Biden administration imposed wide-ranging semiconductor-related export controls on China. These measures captured what Sullivan had said the Biden administration would do a few weeks earlier: an effort to halt China's ability to develop and use specific AI applications by prohibiting sales of specific advanced chips, limit its ability to develop supercomputers for China's military by prohibiting the shipment of technology and software, and thwart Beijing's ambitions to develop an advanced indigenous semiconductor industry by restricting U.S. firms from shipping certain types of production equipment and barring U.S. persons from providing services such as maintenance and upgrades to equipment already in China without a license.

On the 'partner' front, the Biden administration has been active. The United States is pursuing chip-related efforts in the Quad (with Australia, India, Japan), in the U.S.-EU Trade and Technology Council, via a fledgling grouping dubbed the 'Chip 4' (with Japan, South Korea, Taiwan), and bilaterally with India, Japan, and South Korea, among others. And administration officials have convinced their Dutch and Japanese counterparts to follow suit on export controls on chip production equipment, although the details have yet to be announced.

A Protect Agenda for the Times

What Sullivan signaled in his speech, and what the Biden administration implemented with its October 7 rule, is, in the words of export control expert Kevin Wolf, a transformational shift in the use of export controls from one tied to narrow non-proliferation objectives to "a strategic tool". The scope and timing of these actions should be considered in this framing. Specifically, the purpose of the controls is to restrict China's ability "to produce advanced military systems including weapons of mass destruction; improve the speed and accuracy of its military decision making, planning, and logistics, as well as of its autonomous military systems; and commit human rights abuses." The near-term impact will be significant. How effective these actions will be over the longer term is less clear, however. A major factor will be to what extent the Dutch and Japanese governments follow suit in imposing controls on semiconductor manufacturing equipment.

That the United States acted unilaterally in imposing these export controls is an overriding critique. In this instance, the Biden administration may well succeed in securing the desired buy-in from partners. Obtaining *post facto* support is not a sustainable way of operating, however. The U.S. government should craft a better way forward by building on the precedent of the plurilateral export controls and sanctions levied on Russia in response to its renewed invasion of Ukraine.

The first step is emphasizing that the existing four multilateral export control regimes—the Nuclear Suppliers Group, the Australia Group, the Wassenaar Arrangement, and the Missile Technology Control Regime—are not designed for strategic technology competition and that their approach to 'dual use' items are outdated. Another complicating factor is that Russia is a member of three of these groupings. Moscow is likely to thwart meaningful work in these forums, which require consensus among its members.

The goal then should be to initiate a new multilateral export controls regime. One purpose should be to address nonproliferation concerns that the existing regimes won't be able to address if Moscow disrupts their functioning. The overriding objective, though, should be to codify the measures needed to deal with the reality that the concept of 'dual-use' is largely obsolete and that technological leadership is a defining feature of strategic competition. Several concepts for such a regime have already been proposed.

Getting to Yes: Addressing the China Challenge

The fundamental hurdle to crafting more aligned and effective export control policies among the leading techno-democracies remains diverging views on the nature of the China challenge. Unless and until the governments of U.S. allies and key partner countries are more aligned with the United States on assessments of the scope and scale of the security challenges posed by the Chinese Communist Party's laws, policies, and actions, coordinated policies to address those challenges will be sporadic and difficult to achieve.

The overarching priority for U.S. policymakers should be to foster greater convergence. Administration officials and members of Congress must focus on explaining the analysis and rationale underpinning America's technology policies toward China. Signs that perspectives on the China challenge are beginning to converge are encouragingly increasingly common. For example, European Commission President Ursula von der Leyen gave a clear-eyed and practical speech on March 30, calling for a new European strategy towards China. Japan updated its National Security Strategy to label China an unprecedented strategic challenge and to boost defense spending. This comes on the heels of its Economic Security Law to protect Japan's economy from hostile actors.

Regarding export controls, the task at hand is for U.S. officials to secure broader buy-in from allies for the use of export controls as a strategic tool designed to constrain technology development, technology indigenization, and specific end uses such as training certain AI models and human rights abuses. Here too, there are encouraging signs that a workable consensus is budding. In a March 17 interview with Japanese news outlet Nikkei Asia, Dutch trade minister Liesje Schreinemacher noted that "when it comes to national security and to restricting certain technology coming into the wrong hands, we [democracies] really have to cooperate. I want to have as many countries and specifically democratic countries on board when it comes to these export restrictions." Such pronouncements bode well for building a comprehensive collaborative approach by the techno-democracies.

Toward a Tech Alliance

The 'partner' agenda is where the boldest action is still needed. A new export control regime will require deep coordination on tech policies where it does not yet exist. Collaboration is also needed in a broad range of areas including standard setting, defining and promoting norms for technology use, energy security, and supply chain resilience. A new grouping—an 'alliance' of tech-leading democracies—is needed to foster agreements and coordinate action among governments, with input from leaders in industry and civil society.

Existing groupings such as the G-7, OECD, or NATO cannot readily be adapted—they either don't have all the right members, are too large, or their original purpose doesn't fit the purview of coordinating tech policy at the highest level of statecraft. Nor do Washington's bounty of minilateral and bilateral efforts fit the bill. Semiconductor-related policies are a good example of how current engagements fall short.

The main issue is the highly globalized nature of the semiconductor value chain. Simply put, current dialogues don't have all the relevant players at the table at the same time. This is inefficient, and potentially counterproductive. Take the example of the proposed 'Chip 4' alliance of Japan, South Korea, Taiwan, and the United States. Can such a grouping make meaningful progress on supply chain resilience without key European countries taking part?

Another challenge is one of capacity. The proliferation of dialogues and initiatives mentioned above focused on semiconductors alone are a challenge to manage and institutionalize for a bureaucracy as large as the U.S. government, let alone those of partners with less resources. Consolidation will be necessary to avoid having these well-intended efforts fade into irrelevance through inertia.

Creating a tech alliance would be challenging yet is eminently feasible. The foremost condition—recognition of the need for coordinated multi-nation approaches to technology policy—is there. And the building blocks for such a grouping are already in place, with the United States alone already engaged in a multitude of efforts. Concrete proposals exist for what a larger tech steering committee should look like and what its agenda should be, with work taking place behind the scenes to refine these concepts further.

Navigating Complex Tech Matters Together

Coordination and collaboration among the tech-leading democracies will be essential to ensuring that the promote and protect agendas of modern technology statecraft are effective. Technological capabilities and requisite know-how are diffused and oftentimes there is no clear technology leader and multiple viable technology acquisition pathways exist. Furthermore, protective measures—export controls, inbound and outbound investment reviews, and research security practices—will differ in scope, scale, and feasibility depending on what technology area or scientific discipline is addressed. Clear points of leverage, such as a complete reliance for key inputs on a single or small number of foreign sources—China's dependence on a handful of American, Dutch, and Japanese companies for semiconductor manufacturing equipment, for example—are rare.

Even a cursory overview of key technology areas—artificial intelligence, quantum information science, and biotechnology, technologies that the Commission inquired after—underscores the challenge in crafting effective economic statecraft policies. At present, the feasibility of controls beyond specific AI-relevant hardware is limited. There is potential to place limits on providing compute-as-a-service, such as provided by cloud service providers, blocking the proliferation of datasets needed for certain narrow AI applications, and placing parameters on what datasets can be made publicly available in the future. Compute governance measures in the future could include building hardware security features into the chips themselves, such as a 'kill-switch' that renders them unusable if unauthorized usage occurs. While preliminary research on the latter is underway, much work remains to be done for this to be a viable option.

Chinese entities are already using cloud computing infrastructure to train AI models with Nvidia A100 chips that are subject to the October 7 rule, according to reporting by the Financial Times. As a first step, Congress should work with the White House and industry representatives to stipulate stronger 'know-your-customer' regulations to mitigate the risk of foreign actors of concern skirting export controls by accessing compute through other means.

Quantum information science—comprising the subfields quantum sensing, quantum computing, and quantum communications—presents other challenges to designing and implementing export controls. Only quantum sensing, advanced sensors that detect changes in motion, and electronic and magnetic fields, are currently subject to some export controls. The capabilities in this subfield are most mature and the national security risks, such as the potential to negate stealth technologies and improve navigation and timing capabilities, are better understood.

Quantum computing is nascent and an area where premature export controls could thwart technological development. Scientists are pursuing 12 known modalities, or methods, to produce qubits, the basic unit of information in quantum computing. While the so-called superconducting qubit and trapped ion modalities are the most common and appear most promising now, it is unclear which method will prove most effective or even if it is preferable to promote just one method. Placing limits too early could thus cut off promising research.

For now, researchers such as Sam Howell of the Center for a New American Security and Edward Parker of RAND Corporation posit that the most promising areas for further controls are to expand existing end user controls. Targeting specific applications of quantum computing and quantum communications, and eventually integrated quantum systems such as quantum computers and communication networks could become feasible once quantum technology generally is sufficiently matured.

The most important geopolitical implications of advancements of biotechnology will relate to how things are produced. Bio-manufacturing enables the production of chemicals, materials, food, and other inputs into the economy without relying on fossil fuels. A world reliant on bio-based manufacturing is one with potential for dramatically different inter-dependencies, with several implications for economic and national security.

Misuse of advanced biotechnology is also a major concern. Constraining dangerous developments in biotechnology could prove to be vexing. Advancements in the field are such that the barriers to entry are low. The required equipment is inexpensive and widely available, while the needed knowledge can be attained at many universities around the world. Breakthroughs in generative AI, algorithms that can create novel content from training data, could be used to design biological and toxin weapons quickly and cheaply.

The opportunities to craft useful export controls in biotechnology are limited. As the bioeconomy expands, it will be critical that biosecurity and biosafety is a top consideration, and that steps are taken to regulate and gain visibility at the right junctures. Additionally, many of the capabilities that the United States has relied on to navigate COVID-19 will be essential to mitigating risk and impact of misuse of biotechnology, including biosurveillance

One of the most valuable resources in biotechnology development is also the most difficult to control: data. Genetic data, from both humans and non-humans, has significant implications for national security, health, and innovation. In the health domain, personal genetic data, both in isolation and in aggregate, has contributed to life-saving treatments, but also raises important privacy concerns. Already, around the world, there are databases containing genetic data from tens of millions of people. Likewise, non-human data is essential to unlocking advancements in the bioeconomy, including to leverage bio-manufacturing to produce products essential for defense, economic security, and to fight climate change.

The Chinese government seeks to develop the world's largest bio-database and Chinese firms are buying and collecting genetic data around the globe. The United States, in partnership with the techno-democracies, need to counter this effort in three ways. First, U.S. lawmakers should restrict the sale of genetic data of U.S. persons going forward. Second, Congress should incentivize the creation of robust sources of non-human biological data, especially in the genetic sequencing of microbes and plants, which drive innovation in the bioeconomy. Third, U.S. policymakers can implement export controls on the suite of technologies that will enable the use of biological data, including in AI, quantum computing, and semiconductors most prominently.

The risk of adverse impacts to the respective national security and national interest of the techno-democracies due to developments in these emerging technologies is significant. China in particular is devoting outsized resources to breakthroughs in each of these areas. The risk of bad outcomes will be higher still if the United States and its allies do not work together to craft a viable 'protect' strategy in these technological and scientific disciplines.

Needed Change at Home

Policymakers must bolster and adjust elements of the U.S. government to craft and execute its overall national technology strategy and the 'protect' agenda. The executive and legislative branches each have important actions to take. First and foremost, the President should articulate the need and objectives for a comprehensive strategy for technology competition. Without this framing, it is challenging to stimulate effective legislation, prioritize resources, and rally society. Second, the President should appoint a deputy national security advisor for technology competition to lead the process for developing the strategy and stand up new policy and analytic teams to manage strategy implementation.

Congress should increase funding for relevant departments and agencies and initiate a partial reorganization of the federal government to improve its ability to marshal the country for technology competition. Government offices central to implementing the protect agenda, such as the Department of Commerce Bureau of Industry and Security, are under-resourced and would benefit from expanded authorities. And Congress can take action to improve the government's capacity to engage with its allies and partners on matters of technology policy.

Recommendations for Congressional Action Pertaining to Export Controls
Congress has ample opportunity to gird U.S. capabilities in strategic technology competition to maximize the odds that the interests of the United States and of those of its allies and trusted partners are promoted and protected. The Department of Commerce, with its role in enforcing export control laws and cooperating with and supporting other countries on export control issues, should be the highest priority for action.

The United States Congress should:

- **Expand the mission of the Bureau of Industry and Security (BIS).** The Department of Commerce needs structural and organizational reform. BIS focuses largely on export controls. It should, however, play a much larger role in taking on the national security equities related to regulation and protection of U.S. technology supply chains. By centralizing these authorities in a single office, the U.S. government can more effectively execute economic statecraft. The Department of the Treasury's Office of Terrorism and Financial Intelligence could serve as a useful model for such a reorganization, given how it straddles the economic and national security arenas and is designed to tackle nontraditional national security threats.
- **Designate the Department of Commerce as a U.S. Intelligence Community member.** While department officials have regular access to classified information to inform their decision making, the department lacks a full-fledged intelligence analysis component. This office should not only support internal missions that require national security information but become a hub for economic and technology intelligence analysis within the U.S. government. One of its main mission areas should be to study the long-term economic implications of export controls. To lead the new analytic office, Congress should create the position of assistant secretary for intelligence.
- **Address Department of Commerce resource constraints.** The department's current resources, fiscal and human, do not reflect its growing importance in protecting U.S. technology advantages, addressing supply chain vulnerabilities, and ensuring long-term economic competitiveness. Throughout modern U.S. history, Congress has created, funded, adapted, and restructured department to deal with challenges and threats the country faced, such as the National Security Act of 1947 and the creation of the Department of Homeland Security. Stepping up to support the Department of Commerce won't be as dramatic, yet the impact may be as consequential.

Congress has an important role to play in forging alignment among the techno-democracies on cooperative and beneficial technology policies ranging from research partnerships to supply chain resilience initiatives to export controls. There is substantial opportunity to strengthen the U.S. government's capacity for multilateral collaboration on these issues.

The United States Congress should:

- **Establish a cadre of tech diplomats.** These officials would be the vanguard for implementing the international aspects of U.S. technology policies, including cooperative research agreements, human capital exchanges, infrastructure development, and export controls. Some of the building blocks for a large corps of technologically savvy diplomats are already in place: the Department of State's office of the special envoy for critical and emerging technology and its regional technology officer program, and the Department of Commerce's digital attaché program.
- **Establish the position of a special envoy for export controls.** The remit of the special envoy should be to enhance international cooperation on export controls. This function will be essential to cementing the long-term collaboration required to maintaining and updating export controls. The special envoy could reside in the Department of Commerce or the Department of State.
- **Promote the creation of a technology alliance.** Technological leadership will be the cornerstone for a country's ability to safeguard its interests and to compete on the global stage. In an era of increasingly diffused technological prowess and globalized supply chains, executing U.S. technology strategy will require closer collaboration with other tech-leading democracies. A steering committee of the world's tech-leading democracies—Australia, Canada, Finland, France, Germany, India, Israel, Italy, Japan, Netherlands, South Korea, Sweden, United Kingdom, and United States, for example—could cooperate in areas including research and development, supply chain resilience, countering economic coercion, harmonizing export controls, and coordinating industrial policies. Actionable concepts for institutionalization and detailing an agenda already exist.

Conclusion

Questions of technology have never mattered more in geopolitics. How countries conduct technology policy will have outsized impact on how they fare in global strategic competition. Political leaders have long recognized that technological prowess harnesses advantages in economic competitiveness and impacts international security. But now for the United States technological leadership in areas such as computing and biology is a national security imperative and export controls will play an essential role in securing that leadership.

The strategy to gain and maintain that leadership will touch every level of American society, with investments in people, research, and infrastructure that can transform the U.S. economy. It will also color U.S. relations with countries around the world, friend and foe alike. How the strategy is executed matters tremendously. At stake is America's capacity to empower its people, compete economically, and secure its national interests.