From Plan to Action

Operationalizing a U.S. National Technology Strategy

John Costello, Martijn Rasser, and Megan Lamberth

Center for a New American Security

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

Acknowledgments

The authors thank Jessie Liu, James Mulvenon, Eric Sayers, Matt Turpin, and Kevin Wolf for their valuable feedback and suggestions on the report draft. We are grateful to all those who participated in the U.S. National Technology Strategy workshops. Your insights and expertise helped shape the ideas and analysis in this report. The views expressed in this report are those of the authors alone and do not represent those of the workshop participants.

Thank you to CNAS colleagues Maura McCarthy, Melody Cook, Rin Rothback, Emma Swislow, and Anna Pederson for their role in review, production, and design of this report. Finally, thank you to Henry Wu for his valuable research support and assistance in reviewing and finalizing the report. Any errors that remain are the responsibility of the authors alone.

About the Authors

John Costello is an Adjunct Senior Fellow with the Technology and National Security Program at the Center for a New American Security (CNAS). Mr. Costello is the former Deputy Assistant Secretary of Intelligence and Security at the Department of Commerce. Prior to the Department of Commerce, he served as a Senior Director and Lead for Task Force Two at the U.S. Cyberspace Solarium Commission and the Director of Strategy, Policy, and Plans and Senior Advisor to the Director of the Cybersecurity and Infrastructure Security Agency. Mr. Costello is a former U.S. Navy enlisted sailor and is fluent in Chinese Mandarin, having graduated with honors from the Defense Language Institute.

Martijn Rasser is a Senior Fellow and Director of the Technology and National Security Program at CNAS. Mr. Rasser served as a senior intelligence officer and analyst at the Central Intelligence Agency. Upon leaving government service, he was Chief of Staff at Muddy Waters Capital, an investment research firm. More recently, he was Director of Analysis at Kyndi, a venture-backed artificial intelligence startup. Mr. Rasser received his BA in anthropology from Bates College and his MA in security studies from Georgetown University.

Megan Lamberth is a Research Associate for the Technology and National Security Program at the Center for a New American Security (CNAS). Prior to joining CNAS, Ms. Lamberth was a Brent Scowcroft Fellow at the Aspen Strategy Group, where she helped spearhead the planning and execution of the Aspen Strategy Group Summer Workshop and two sessions of the Aspen Ministers Forum. She received her MA in international affairs from the Bush School of Government & Public Service at Texas A&M University, and she graduated from Sam Houston State University with a BA in criminal justice.

About the Report

This report is produced as part of the U.S. National Technology Strategy project at CNAS. The project is developing the intellectual framework for a national technology strategy for the United States that can serve as a road map for successful long-term American innovation and technological leadership. The project focuses on how the government should establish technology policy on key issues such as accelerating American innovation, mitigating risk to U.S. advantages, and contending with the technology strategies of competitors. This report was made possible because of a grant from the U.S. Air Force Office of Commercial and Economic Analysis (OCEA).

This report draws on analysis and insights from prior CNAS reports, including:

"Trust the Process: National Technology Strategy Development, Implementation, and Monitoring and Evaluation," by Loren DeJonge Schulman and Ainikki Riikonen (April 2021)

"Taking the Helm: A National Technology Strategy to Meet the China Challenge," by Martijn Rasser and Megan Lamberth (January 2021)

"Networked: Techno-Democratic Statecraft for Australia and the Quad," by Martijn Rasser (January 2021)

"Democracy by Design: An Affirmative Response to the Illiberal Use of Technology for 2021," by Kara Frederick (December 2020)

"Rethinking Export Controls: Unintended Consequences and the New Technological Landscape," by Martijn Rasser (December 2020)

"Defense Technology Strategy," by Paul Scharre and Ainikki Riikonen (November 2020)

"Common Code: An Alliance Framework for Democratic Technology Policy," by Martijn Rasser, Rebecca Arcesati, Shin Oya, Ainikki Riikonen, and Monika Bochert (October 2020)

"Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific," by Ely Ratner et al. (January 2020)

"The American AI Century: A Blueprint for Action," by Martijn Rasser, Megan Lamberth, Ainikki Riikonen, Chelsea Guo, Michael Horowitz, and Paul Scharre (December 2019)

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

Table of Contents

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

Executive Summary

Ideas abound for actions the United States should take to better position itself for the unfolding global technology competition. Concerning topics as diverse as raw materials to semiconductors to STEM education, a nonstop cavalcade of presidential directives, congressional bills, industry proposals, think tank reports, and pronouncements by big-name luminaries have been issued as measures to address American economic competitiveness and national security challenges. Almost all make their case in the context of dealing with a rising China. Some of these recommendations are excellent and quite a few are good; too many get lost in the noise.

It's not just the sheer volume that presents a challenge to identifying and executing the most promising recommendations. The U.S. government lacks a strategic construct to merge these ideas—for research and development spending, public-private partnerships, tax policy and subsidies, immigration reform, and education—into a coherent whole. The goal of CNAS' National Technology Strategy project is to create the framework for a comprehensive, whole-of-nation approach for the United States to navigate the global technology competition.

The first report in this initiative, "Taking the Helm," makes the case for a national technology strategy and lays out what such a modern-day strategy should be.[1] Its chief argument is that the United States is in a long-term, multifaceted geostrategic competition with China, one that has technology at its core. Technological leadership is more important than ever, yet current U.S. government policies fall well short of what is needed to maintain it. Crafting an affirmative technology policy agenda is not just about competing with China; it comprises the guiding principles for the nation's technology policy goals and priorities to pursue economic prosperity, protect national security interests and democratic values, and advance society.

How the U.S. government should structure itself organizationally and bureaucratically to execute such a strategy is the focus of the second report, "Trust the Process."[2] Today, key institutions such as the National Security Council, National Economic Council, and Office of Science and Technology Policy are not optimized to craft, run, and maintain this effort. "Trust the Process" explains what talent, resources, infrastructure, and processes are needed for strategy development, implementation, and monitoring and evaluation.

This third report in the series focuses on concrete and pragmatic measures that U.S. policymakers should take to operationalize a national technology strategy. There are four premises to the security and technology competition that guide these findings: the utility of industrial policies, the convergence of national and economic security, gaps in knowledge, and the need for international partnerships. The report offers recommendations for specific changes to U.S. government departmental and agency authorities, regulatory updates, policy initiatives, and diplomatic efforts that will bolster the U.S. government's ability to craft, execute, and maintain this strategy.

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

SUMMARY OF RECOMMENDATIONS

"However beautiful the strategy, you should occasionally look at the results."
- Sir Winston Churchill

Strategies can be eloquent and inspiring. How successful they are rests in addressing gritty details outside the spotlight. This report lays out concrete steps needed to ensure that the vision, framework, and processes necessary to successfully execute a national technology strategy are established.

Bolster the Department of Commerce

The Department of Commerce will be one of the most important entities in the U.S. government for planning, implementing, and monitoring and evaluating a national technology strategy. While its leaders bear responsibility for a range of issues at the intersection of economic security and national security, the department is not well positioned to execute its expanding mission. Several actions by Congress and the executive branch are necessary:

- *Expand the mission of the Bureau of Industry and Security (BIS).* BIS should take on the authority to regulate and protect U.S. technology supply chains and reorganize itself on the model of the Department of Treasury's Office of Terrorism and Financial Intelligence to execute its increased duties.

- *Designate the Department of Commerce as a U.S. Intelligence Community member.* A formal role for the department on intelligence matters will improve the government's ability to conduct analysis of economic, trade, and technology developments required for executing a national technology strategy. This should be done while preserving and avoiding any disruption to the department's science and technology, statistics, and economic mission.

- *Establish an information fusion center, headquartered in the International Trade Administration's Office of Industry & Analysis.* A new information center would enable the Department of Commerce to better understand foreign and domestic industrial and technological trends by collecting and integrating a myriad of open-source and proprietary information.

- *Expand the use of existing industrial survey authorities.* Regular surveys of specific industries will provide policymakers with better and up-to-date information on topics such as research and development (R&D) trends, manufacturing capacity, and supply chain risks.

- *Establish a Defense Production Act "Title III" Office under the Department of Commerce.* The goal of the new office would be to oversee non-military projects related to economic or technological competitiveness. Doing so would accommodate the broadened conception of "national defense" under a revised Defense Production Act (DPA) and reduce the strain on the existing office at the Department of Defense.

- *Address Department of Commerce resource constraints.* Congress should ensure that it apportions adequate fiscal and human resources to the Department of Commerce commensurate to its expanded mission.

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

Mitigate Supply Chain and Technology Transfer Risk

Updated legislation and regulations are needed for the U.S. government to address new supply chain and technology transfer risks. Congress and the executive branch should take the following steps:

- *Codify and tailor the information and communications technology and services Executive Order 13873.* The law should authorize the secretary of commerce to review, grant, or block licenses for foreign entities to sell information and communications technologies and services in the United States.

- *Update the International Emergency Economic Powers Act (IEEPA) Berman Amendment.* The amendment, which pertains to informational materials, is out of sync with the scope and scale of commoditized data generation, dissemination, and exploitation in 2021. A revised amendment would provide current and future administrations with enough leeway to address data privacy and espionage threats.

- *Establish minimum cyber and personnel security standards and requirements for recipients of federal R&D funding.* U.S. policymakers and government officials are renewing efforts to protect America's R&D infrastructure from intellectual property theft. The White House Office of Science and Technology Policy, in conjunction with the Department of Justice, should establish cyber and personnel security standards and requirements for recipients of federal R&D funding.

- *Enact a national data protection and privacy law.* A federal law would address current hurdles in identifying and mitigating national security and supply chain risks associated with foreign companies operating and investing in the United States. The law also would eliminate the growing patchwork of state and local laws that burden private industry and stifle innovation.

Streamline Technology Policy Coordination and Implementation

Responsibility for technology policy decisionmaking is diffused across an array of government departments and agencies. Congress and the White House need to collaborate to ensure that effective interagency mechanisms are in place to coordinate and implement technology policy. Concrete measures legislators and administration officials should take are to:

- *Establish a Technology Security Coordination Group (TSCG).* The group should be an interagency effort to coordinate technology and supply chain–related regulatory and policy actions. This grouping will be necessary to ensure a unified and consistent approach to technology strategy execution.

- *Craft a government-wide definition for "critical technology" and create a framework and mechanism for making prioritization decisions.* The U.S. government lacks a universal definition for what constitutes a critical technology. Crafting such a definition is an integral step in articulating a strategic vision for technology policy and required to be able to set priorities.

- *Codify and designate the Department of Commerce International Trade Administration's Office of Industry & Analysis as the federal government center for foreign company risk information.* There exists no interagency mechanism to compile or share due diligence or risk information on foreign companies obtained through reviews and investigations. Creating a central repository that specializes in open-source and proprietary intelligence on industrial and technology analysis would facilitate establishing a common risk profile on specific entities and reduce inefficiencies and duplicative work.

- *Establish a National Economic and Technology Security Intelligence Center (NETSIC) housed in the Office of the Director of National Intelligence*. NETSIC's key functions should include centralizing and aggregating intelligence related to vulnerabilities in the industrial base of foreign countries, tracking foreign emerging technology developments, and establishing a "map" of foreign supply chain and economic dependencies.

Increase Capacity to Pursue International Technology Partnerships

The U.S. government needs greater capacity to initiate, maintain, and expand collaborative technology relationships with allies and other like-minded countries. The United States increasingly will have to work with partners to successfully tackle the most vexing tech policy issues. The U.S. government needs a dedicated organizational and bureaucratic infrastructure to unify and formalize nascent initiatives. The best way to do so is for Congress and the White House to:

- *Create a Technology Partnership Office at the Department of State*. Headed by an assistant secretary for technology, this office would be the lead U.S. government entity to manage America's technology partnerships around the world. A formal office will be necessary to provide the needed organization and permanence to sustain such relationships.

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

Key Premises of U.S. Technology Security and Competition

Formulating policies under the rubric of an overarching national technology strategy requires understanding the broader context in which these decisions take place. The nature of the China challenge and economic and political realities require changes to long-standing assumptions and desired end states that dominate American political discourse. There are four fundamental suppositions that will shape U.S. technology policy. The first is the understanding that greater engagement by the U.S. government on technology policy is needed to ensure that the foundation for long-term economic and technological competitiveness is strong. The laissez-faire approach to industrial policy since the Reagan years is inadequate for countering China's techno-mercantilism.

Second is the need to broaden the concept of national security. Economic security and national security are effectively one and the same. Third is the fact that the U.S. government has too many blind spots for effective technology policymaking. There are necessary actions that would improve the situational awareness of U.S. leaders. Finally, there is the reality that greater self-sufficiency will be expensive and difficult to achieve. There are pitfalls in the autarkic tendencies of the strategic visions of American leaders, whether it's America First or Build Back Better. Collaborative solutions formulated in concert with like-minded partners—done bilaterally, plurilaterally, and multilaterally—should be a central feature of strategic technological statecraft.

Industrial Policy Can Restore Free and Fair Competition

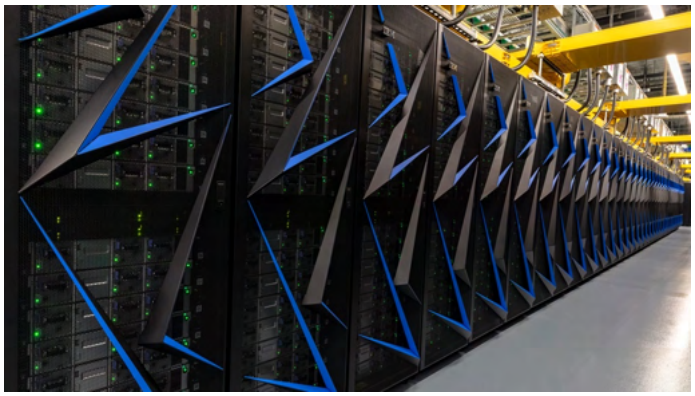
The term "industrial policy" elicits a range of strong reactions from policymakers and industry leaders.[3] In recent years, it has had a negative connotation—perceived by critics as misguided government overreach or an attempt to pick winners and losers. Broad-based industrial policy that is burdensome, inefficient, or runs the risk of undermining the free market is justifiably concerning. When industrial policy is applied more narrowly, however, and tailored to a specific problem set, it can be an effective tool for policymakers.

Industrial policy defined as "actions by a country's leadership to develop, grow, or reorient parts or all of its economy to achieve a specific objective" is synonymous with the idea of government-led technology strategy.[4] U.S. leaders have applied some form of industrial policy throughout the country's history.[5] In 1791, Alexander Hamilton wrote the "Report on the Subject of Manufactures," which called on Congress to use tariffs and subsidies to support domestic U.S. manufacturing.[6] In it Hamilton argues, "There is no purpose, to which public money can be more beneficially applied, than to the acquisition of a new and useful branch of industry."[7] U.S. industrial policy was instrumental throughout the Cold War, particularly in competition with the Soviet Union in the Space Race.[8] Policymakers also used targeted industrial policy in the mid-1980s to help the U.S. semiconductor industry compete against a rising Japanese market. In 1987, the government partnered with and financially supported SEMATECH (or Semiconductor Manufacturing Technology)—a consortium of 14 U.S.-based semiconductor firms—which helped contribute to the recovery of the semiconductor industry by the mid-1990s.[9]

Robert N. Noyce, an American engineer and co-inventor of the integrated circuit, played an important role in creating SEMATECH (or Semiconductor Manufacturing Technology) and served as its first president. (Intel Free Press)

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

Policymakers once again are calling for industrial policies in the United States for a number of reasons and have proposed various options, to include bolstering the U.S. alternative power industry to combat climate change, infrastructure projects to address rising income inequality, and funding to advance domestic semiconductor production.[10] Chief among these reasons, however, is China, whose technological advancement poses a serious challenge for the United States, and its anti-competitive economic practices have substantially distorted a free and fair global market.[11] Lawmakers and government officials are crafting ideas for a new form of U.S. industrial policy in response.[12] In 2019, Senator Marco Rubio called for a "21st-century pro-American industrial policy" to counter China, and since taking office, the Biden administration has crafted and promoted concepts with clear roots in industrial policy.[13] President Joe Biden's Build Back Better economic plan was described by Scott Paul, the president of the Alliance for American Manufacturing, as "the closest thing we've had to a broad industrial policy for generations."[14]



Summit, a supercomputer at the U.S. Department of Energy's Oak Ridge National Laboratory, is one of the world's most advanced supercomputers for AI applications. With recent U.S. Commerce Department trade restrictions levied against China's People's Liberation Army–linked supercomputing entities, such technologies will continue to be at the heart of U.S.-China technology competition. (U.S. Department of Energy/Oak Ridge National Laboratory)

U.S. industrial policy—when scoped and narrowly tailored—can be useful in resetting the terms of global competition with China. The United States must be careful, however, to balance the sometimes-competing priorities of protecting U.S. industry and trade and preserving fair global competition. As Shannon O'Neil argues in *Foreign Affairs,* industrial policy "built on more global cooperation and competition, better U.S. access to international markets, and public investments at home . . . can avoid the pitfalls of protectionism."[15] If the United States relies solely on protectionist measures to defend its markets and mitigate domestic supply chain vulnerability, it runs the risk of leaving a market void of cost-competitive technologies in critical sectors. Alternatively, a more proactive and unified U.S. approach—with elements of industrial policy—can be used to ensure that reliable, cost-effective technologies are acquired, and to initiate a long-term strategic approach toward funding new and emerging technologies.

"National Security" Should be Redefined for a New Era of Technology Competition

The United States can no longer treat economic security and national security as equally important, but disparate goals. Over time, modernization and global competition for technological leadership have increasingly caused the two to converge—inextricably linking U.S. economic and national security. Understanding the implications of this linkage is critical for ensuring long-term U.S. security and competitiveness.

While U.S. policymakers and government officials have acknowledged the interplay between economic and national security in public statements and strategy documents, the policies and tools that are relied on most heavily have not followed suit.[16] The authorities that empower the U.S. government to control, defend, or shape technology or critical industries, such as export controls and the Defense Production Act (DPA), are focused largely on the national defense context. As economic and military priorities continue to intertwine, the U.S. government will need to formulate strategies that expand from just national defense to national *needs*. Christopher Darby and Sarah Sewall succinctly argue this point in *Foreign Affairs*,

explaining that the U.S. government "needs to back not only those technologies that have obvious military applications, such as hypersonic flight, quantum computing, and artificial intelligence, but also those traditionally thought of as civilian in nature, such as microelectronics and biotechnology."[17]

Biotechnology—including synthetic biology, pharmaceuticals, and genomic editing—has the potential to transform the geopolitical landscape. (iStock/Getty Images)

The interconnections between America's economic and national security also have implications for the country's national security establishment. The U.S. military and defense communities are increasingly dependent on civilian critical infrastructure and technological innovation. This reliance is primarily due to the relative decline in U.S. federal research and development (R&D) spending. The federal government funded two-thirds of U.S. R&D in the 1960s, but today that percentage has dropped to less than one quarter.[18] While the private sector has filled the R&D gap, this shift has implications for the Defense Department's ability to acquire critical technologies. Center for a New American Security scholars Paul Scharre and Ainikki Riikonen explain that the growth in private sector R&D spending,

> … presents both a challenge and an opportunity for the DoD. The opportunity is that the DoD can piggyback off of innovation that is happening elsewhere and free ride on others' R&D funding … The challenge is that the DoD no longer has the same freedom of action in driving the shape of technological innovation. The DoD can make bets in key technology areas, but the bulk of R&D funding is outside of the DoD's hands.[19]

This reliance on the private sector for critical infrastructure and a reliable and secure supply of critical technologies may leave the United States at a strategic disadvantage in ways that do not strictly implicate military, national defense, or other security equities. Advances in technology areas such as artificial intelligence, 5G wireless telecommunications, and quantum sciences will have massive implications for labor markets, economic prosperity, and the global economy itself. In addition to economic security, however, emerging technologies, and the norms and standards around their use, will help shape societal structures, civil liberties, and the global response to issues like climate change or pandemics. The United States must continue to play a substantive, leading role in a critical or emerging technology, otherwise its ability to shape international standards, norms of behavior, or its own long-term security environment will be fundamentally limited.

Information Gaps Pose Risks to U.S. Success in Technology Competition

The U.S. government faces knowledge gaps in areas key to strategic decisionmaking on matters of technology policy. These gaps fall in several broad categories: understanding the scope and direction of science and technology (S&T) research efforts in the United States and foreign countries; horizon scanning and technology forecasting; research, development, and acquisition processes; and supply chain security and resilience. The U.S. government has departments and agencies focused on these areas, but this work is underutilized and underappreciated by decision makers or lacks foundational information by which to generate thoughtful, prescient analysis.

Having a pulse on what research is being conducted and where is an elemental factor in mapping out a coherent national strategy for technology. While creating a central repository for such knowledge is infeasible—there is too much information to be collected, assessed, and updated—routine net assessments of specific technology areas should be part of the strategy setting process. At the same time, U.S. decision makers must be able to view these developments in the context of what other countries, allies and adversaries alike, are doing in the same fields.

These net assessments would bolster efforts to identify opportunities and threats pertaining to technology development to minimize the risk of technology surprise. Horizon scanning is a technique that "incorporates research from a wide variety of sources with the goal of detecting change, exploring problems and challenges in emerging technology fields, and discerning trends."[20] Technology forecasting is a complementary methodology that anticipates how technologies could be used in the future. Both techniques provide valuable insight on civilian and military uses of technologies necessary for smarter decisionmaking.

To understand how specific technologies are adopted by militaries worldwide, knowledge of a country's research, development, and acquisition processes—everything from setting requirements, funding, testing and evaluation, and fielding a weapons system—is a must. Assessing technology development through this lens provides U.S. military planners with better information on when an adversary is likely to obtain certain capabilities, what threats those capabilities pose, and how best to mitigate them.

Having a comprehensive understanding of key supply chains is foundational to sound national security decisionmaking. Supply chain mapping is necessary to identify vulnerabilities and to manage risk. Knowing the supply chain risks that other countries face presents opportunities for economic statecraft measures such as export controls and sanctions, or areas for cooperation with allies and partners.

The development of hypersonic weapons, designed to travel at five times the speed of sound, is a key element of the U.S. Department of Defense's modernization efforts. Hypersonic weapons, like this prototype missile, will require investment in critical technologies and a long-term vision for deployment. (U.S. Department of Defense)

Four trends contributed to widening the knowledge gaps in these areas since the 1970s. The first is the general diffusion of technological capabilities. Because the United States in 2021 is no longer as overwhelmingly dominant globally in matters of science and technology as it was in the 1950s and 1960s, more and more important breakthroughs happen in other countries. Detailed insight on such developments is harder to come by, even when the work is conducted largely in open sight.

The second trend is the shift of innovation and technology development from government to private industry. Corporations account for a much larger share of R&D spending and activity compared to 50 years ago. Much of this work is proprietary to individual companies. Efforts to protect intellectual property and know-how from competitors also pose barriers to analysts in government having a comprehensive understanding of what research is under way. These same barriers also complicate understanding matters such as supply chain vulnerabilities.

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

Third is the ever-increasing amount of information and data. Even while much insight is difficult to obtain because it takes place in areas that are challenging for government analysts to access—companies domestic and foreign, and in foreign government research labs—the volume of information that *is* available is growing at a staggering pace. The digitization and diffusion of information enabled by the internet means that there is much more information than could ever be processed and understood by people. It also means these data are readily available to friend and foe alike, meaning that a competitive edge in knowledge is increasingly rare.

Finally, U.S. policymakers generally have not considered S&T intelligence to be a particularly high priority except in certain fields such as nuclear technology and defense modernization. Since the end of the Cold War, and especially after the 9/11 attacks, threats to the homeland and counterterrorism efforts have comprised the bulk of policymakers' consumption of intelligence products. When the focus is on nation-states, it is most often on questions of military capabilities and leadership intentions. Scientific and technical intelligence, with some exceptions, are rarely the main story. Capabilities such as understanding foreign weapons research, development, and acquisition processes and mitigating the risk of "technology surprise" have withered as a result.

The first and most straightforward response to these trends should be clear guidance from policymakers that S&T intelligence is an issue of importance and urgency. U.S. intelligence agencies are responsive to the wonts of the nation's decision makers and will adjust their collection posture and analytic output to meet demand. Some near-term action is achievable without requiring reorganizations and additional resources. The Central Intelligence Agency, Defense Intelligence Agency, Federal Bureau of Investigation, and National Security Agency among others have existing capabilities that can be brought to bear more effectively. However, addressing this gap permanently will require a more sustained effort by the Office of the Director of National Intelligence in being responsive to and forcefully prioritizing collection and resources relevant to understanding technology competition. Detailed recommendations follow.

Technology and Supply Chain Diffusion Means the U.S. Cannot Compete Alone

The era of U.S. technological preeminence is over. The current environment is one in which there is no single global market, supply chains are increasingly diffuse, and the United States does not have a monopoly over the technologies it needs to compete economically and militarily. As other countries have worked to close the innovation gap with the United States, the U.S. government's ability to dictate the terms of global competition has diminished. Many in the U.S. policymaking community have acknowledged this new reality—accepting the United States no longer enjoys unfettered unilateral influence over international trade, supply chains, and standard-setting.

Semiconductor supply chains are emblematic of this new globalized market. Semiconductors—advanced computer chips—are essential components of nearly every modern-day technological device. No one country has the resources and talent needed to indigenize the entire semiconductor supply chain. As Saif Khan explains, however, in his Center for Security and Emerging Technology report, "the United States and its allies—above all, Japan, the Netherlands, Taiwan, South Korea, the United Kingdom, and Germany—enjoy a competitive advantage at nearly every step of the supply chain needed to produce these chips."[21] In the semiconductor market and in countless other areas, the U.S. government knows it can no longer afford to go it alone.

President Biden, joined by Vice President Kamala Harris and Secretary of State Antony Blinken, participate in a virtual Quad Summit with Indian Prime Minister Narendra Modi, Japanese Prime Minister Yoshihide Suga, and Australian Prime Minister Scott Morrison. (The White House)

With this new international environment in mind, the United States and its allies have begun exploring a number of different arrangements for long-term multilateral collaboration. Earlier this year, the Quadrilateral Security Dialogue partners—Japan, India, Australia, and the United States—established a new Critical and Emerging Technology Working Group designed to collaborate on issues such as international standards-setting, telecommunications infrastructure, and securing critical supply chains.[22] Senator Mark Warner also has called for the creation of a new State Department office to coordinate U.S. technology strategies with other like-minded nations.[23] A 2020 CNAS report went further, recommending the establishment of a new coordination mechanism for multilateral technology policy.[24] Regardless of the exact arrangement, the United States and its allies must work to establish sustainable and effective avenues for collaboration to ensure the security of critical supply chains and the health of the global market.

Recommendations

The White House and Congress can take numerous concrete steps to improve the U.S. government's ability to execute strategic technology policies. The following recommendations comprise four categories that can have profound impact on America's ability to secure its long-term competitiveness. The categories are bolstering the Department of Commerce, mitigating supply chain and technology transfer risk, streamlining technology policy coordination and implementation, and increasing capacity to pursue international technology partnerships. Specific actions concern legal and regulatory changes and bureaucratic and organizational improvements. Some comprise straightforward adjustments and updates; others combine existing capabilities into new entities or create new ones altogether. All would contribute to successful implementation of a national technology strategy.

BOLSTER THE DEPARTMENT OF COMMERCE

Technology competition lies at the intersection of trade and supply chain and economic security—issues that, among all federal departments and agencies, the Department of Commerce is almost singularly equipped to address. The Department of Commerce is nearly unique among federal departments and agencies in its responsibilities for both economic security and national security, a distinction it shares with the Department of the Treasury. However, while Commerce's prominence and role in national security policy has grown in recent years, there has been little change in structure, budget, or organization of the department.

To successfully implement a national technology strategy and to bolster the United States' ability to compete internationally, the Department of Commerce will need to be strengthened commensurate with its growing role and importance. Doing so will mean a reevaluation and reorganization of some of the department's existing missions. Responsibilities for intelligence, supply chain, and technology security, in particular, are decentralized and distributed across a variety of department bureaus. This model is unsustainable in the long term because it leads to conflicting priorities and approaches, inefficient use of resources, and an inability to build supporting programs that benefit from economies of scale. Furthermore, this model deprives both industry and other departments and agencies of a central coordinating authority for compliance, enforcement, information sharing, and policy deconfliction. This report attempts to address some of these issues and provide a long-term vision for the department that reflects its unique status and capabilities.

Expand the mission of the Bureau of Industry and Security (BIS)

Congress should expand the mission of BIS by reorganizing it modeled on the Department of the Treasury's Office of Terrorism and Financial Intelligence (TFI). Like the Department of the Treasury, the Department of Commerce straddles the economic and national security arenas, and is uniquely suited to combat an emerging, nontraditional national security threat. At first glance, threats to the U.S. technology supply chain (including threats of intelligence exploitation, disruption, and availability) would appear to be far removed from terrorism or illicit finance. However, the challenges each pose to U.S. national security and the corresponding U.S. approach to address them, have striking similarities. Both are nontraditional national security threats: foreign threats that manifest domestically. Both stem from broader national security concerns: global terrorism for illicit finance and great state competition for supply chains. And both occur in the same context of the global financial system and international trade. More fundamentally, as both issues occur largely in the context of economic policy, regulation and enforcement—rather than military or homeland security measures—are the primary and most effective tools in combating the threat.

The Department of the Treasury responded to the challenge of illicit and terrorist finance by leaning into its role in national security. It established the TFI, which centralized and consolidated policy, intelligence, enforcement, and regulatory authorities related to anti-money laundering, illicit finance, and terrorist finance. Despite the growing threat that supply chain and technology competition poses to the United States and the Department of Commerce's expanding authority to address it, there has not been a corresponding growth or interest in the department being similarly equipped. From a budget, structural, and organizational perspective, little has changed despite a sizable increase in visibility and responsibility. For Commerce to play its role most effectively, it will need to draw on the lessons provided by the Department of the Treasury and adopt a model similar to that established by TFI.

For simplicity and efficiency, the Department of Commerce should not create a new undersecretary position, but rather it should seek to consolidate authorities and resources under an existing one. The BIS, despite its name, has been focused almost exclusively on export controls, but remains well placed to expand beyond this remit to take on broader national security equities related to regulation and protection of the U.S. technology supply chain.

The reorganization would centralize and consolidate the Department of Commerce's intelligence, policy, regulatory, and enforcement authorities related to export controls and security of the technology supply chain. Centralization would afford BIS greater insight and control over key programs involved in technological competition. Specific steps include:

- *Creating an assistant secretary for supply chain and technology security:* This position would consolidate and centralize departmental policy and regulatory programs that relate to efforts to ensure the availability and integrity of the U.S. information and communications technology and service supply chain. The assistant secretary would oversee program reviews under Executive Order 13873 (or subsequent legislation), certain Committee on Foreign Investment in the United States (CFIUS) reviews, Defense Production Act programs, and planning and administration of BIS industry surveys.

- *Creating an assistant secretary for intelligence:* This position would centralize and consolidate the disparate intelligence support functions already extant across the department, including the Strategic Intelligence Division under BIS and the Office of Intelligence under the Office of Intelligence and Security within the Office of the Secretary. This office would be responsible for providing intelligence support to department leadership and national security–related programs, liaising with the Intelligence Community, and fusing department information with classified information to yield new insights for analysis, production, and dissemination.

- *Establishing centralized enforcement and compliance:* A reorganization should rename BIS's current assistant secretary for export enforcement to the assistant secretary for enforcement and compliance, who thereafter would support requirements for all regulatory programs under BIS.

Designate the Department of Commerce as a U.S. Intelligence Community member

Congress should designate the Department of Commerce as a member of the U.S. Intelligence Community and create the position of assistant secretary for intelligence. These actions are needed to address the fact that the Department of Commerce lacks a fulsome intelligence analysis component that can support the expanding array of department programs that draw on national security information for decisionmaking. This component also should provide new analysis on economy, trade, and technology increasingly sought by policymakers in the White House and across the U.S. government.

While the department has made small steps toward expanding intelligence support for department programs, such as through the creation of a deputy assistant secretary for intelligence and security in 2019, significant limitations remain. Intelligence support efforts remain decentralized and incommensurate with the growing need of the department. Furthermore, there is significant opportunity cost in the department lacking an intelligence function that can fuse the wide array of data, insights, and expertise at its disposal with classified intelligence made available through a deeper collaboration with the Intelligence Community.

To be clear, the department's designation as a member of the Intelligence Community would not immediately solve the department's budgetary or administrative constraints in making better use of intelligence, but it would prompt a critical administrative shift that, over time, would expand and institutionalize the program that can be suited to department needs.[25] These shifts comprise:

- *Creating a new scope of responsibility:* The Department of Commerce intelligence component should focus on building a cadre of analysts able to provide intelligence and analysis on foreign supply chain dependency on critical technologies, export control circumvention, anti-dumping/countervailing duties, weapons sales, trade in export-controlled items, and other national security–related trade and economic transactions. Long-term assessments should include assessments of strength and vulnerabilities of foreign trade, supply chains, and industrial strength.

- *Providing funding from the U.S. intelligence budget:* The designation would avail the Department of Commerce with a portion of the intelligence budget, establishing a National Intelligence Program that would be used to fund analysts, programs, and infrastructure that provide trade, economic, and supply chain expertise and appropriately secure the department's classified information.

- *Enacting needed administrative changes:* Designation as a member of the Intelligence Community would enable the Department of Commerce to institute key administrative changes that would expand its ability to access and protect classified information. Additionally, Commerce would be responsible for adjudicating certain clearance levels, which would alleviate potential bottlenecks stemming from a dependence on other agencies for the service.

- *Creating a firewall from certain commerce activities:* Legislation or any other designation of the Department of Commerce as a member of the Intelligence Community should be clear that the intelligence activities of the department are to be separate and distinct from other activities that have an international remit or that handle data on U.S. citizens and other residents, such as those led by the National Institute of Standards and Technology (NIST), U.S. Commercial and Foreign Services, Bureau of Economic Analysis (BEA), and the Census Bureau. This should be done in order to preserve the trust necessary for international work and avoid any perception that these activities are influenced, supporting, or acting at the behest of the Intelligence Community.

Establish an information fusion center, headquartered in the International Trade Administration's Office of Industry & Analysis

In crafting a comprehensive understanding of adversary technological and economic development, the Department of Commerce should avail itself fully of the wide array of open-source and proprietary information. The private sector has made extensive use of open-source intelligence information to understand foreign and domestic economic industrial capacity, technology developments, and relative strength of certain industrial sectors. This is particularly true for business intelligence firms that advise private equity and finance firms on investment. While the Department of Commerce shouldn't seek to recreate this capability wholesale, these firms' offerings demonstrate both the depth of insight that can be gleaned from the marriage of open-source collection and subject matter expertise and the quality of proprietary services available for the government's own analysis.

The center would be essential in integrating and fusing the department's myriad nonclassified efforts to understand foreign and domestic industrial and technological trends. Additionally, assuming foreign adversaries are collecting and utilizing open sources extensively, this center will play a key role in ensuring U.S. economic and national security policy can attain or maintain an information advantage in great power competition. Two areas of focus should be:

- *Integrating department statistics, open-source, and proprietary information:* This center should work to establish mechanisms to integrate Department of Commerce statistical data and nonpublic information streams into its analysis. This will be a key differentiator in enriching any information collected or ingested from open-source or proprietary sources.

- *Engaging academic and subject matter experts:* This center should seek to engage with subject matter experts in industry and academia to fill knowledge gaps in areas including U.S. and foreign capabilities in specific technology areas—and to help foster better understanding in industry of U.S. government information needs and activities for technology policy analysis and decisionmaking.

Expand the use of existing industrial survey authorities

Congress should amend existing laws to expand the use of industrial surveys. The Department of Commerce maintains strong authorities in compelling or soliciting economic and industrial information from the private sector. Section 705 of the DPA gives the Department of Commerce's BIS the authority to conduct "industry studies assessing the U.S. industrial base to support the national defense."[26] Additionally, the International Investment and Trade in Services Survey Act authorizes the BEA to solicit information on foreign investment in the United States and U.S. investment abroad. Together, these surveys are powerful tools used to collect information unattainable from other sources.[27] Under the law, recipients of these requests, which can include for-profit and nonprofit organizations, academic institutions, and government agencies, are obliged to produce the requested information within a certain time period.[28] This information is critical in availing the department of more information that, when fused with other sources, can yield greater insight into strengths, weakness, opportunities, and vulnerabilities of the supply chain or economic security of the United States and its adversaries—all critical data for technology competition.

Specific steps should include:

- *Requiring routine use of Defense Production Act industry surveys.* Congress should amend the Defense Production Act to require that BIS conduct routine surveys at set time intervals related to foundational and emerging technologies or other technology-related items on the Commerce Control List. By standardizing the use of these surveys, BIS can equip the U.S. government and private industry with accurate and up-to-date data on R&D developments, capacity, and potential supply chain risks of critical industries, materials, and technologies.

- *Revising the International Investment and Trade in Services Survey Act to allow information sharing:* Congress should amend the International Investment and Trade in Services Survey Act to allow information collected to be shared, in an anonymized and minimized form, with other portions of the Commerce Department as well as other departments and agencies. This would ensure the foreign investment information collected is being fully utilized for economic and industrial analysis while preserving business equities of those involved.

- *Expanding appropriations and establishing an "Industrial Survey Fund":* The expanded use of industrial surveys should be met with a commensurate increase in appropriations. Additionally, Congress should establish in the Treasury an "Industrial Survey Fund" with multi-year money that can be utilized by Commerce for ad hoc surveys meant to address an exigent or pressing national security need. Heretofore, Commerce has been limited by lack of available funding in disseminating surveys, often having to rely on other departments and agencies as a "client" for funding. This would ensure the U.S. government has optimal flexibility to collect information relatively quickly to inform policy and regulatory action.

Establish a Defense Production Act "Title III" Office under the Department of Commerce

Congress should expand the scope of the DPA. Title III of the DPA "authorizes appropriate incentives to create, expand or preserve domestic industrial manufacturing capabilities for industrial resources, technologies, and materials needed to meet national security requirements."[29] In other words, the executive branch has broad authority to use economic incentives, such as direct loans, loan guarantees, or purchase commitments, to ensure the timely availability of domestic industrial resources and materials critical to U.S. national security and defense.[30]

The U.S. Department of Defense has used Title III of the Defense Production Act to implement COVID-19 response projects, including increasing domestic production of personal protective equipment. (U.S. Department of Defense)

Presently, the Department of Defense is the only federal agency with the capability to execute DPA Title III authorities, although other agencies and departments can partner with the DoD on individual projects.[31] Title III authorities have been used in a variety of ways over the years to mitigate potential supply chain risks and promote production capacity of critical resources. The Defense Department frequently uses Title III authorities to acquire and scale advanced technologies or capabilities, such as unmanned aerial systems, advanced thermal batteries, or rare earth elements.[32] More recently, Title III played a crucial role during the COVID-19 pandemic as Congress appropriated $1 billion under the Coronavirus Aid, Relief, and Economic Security Act to the Defense Department's DPA Fund to "prepare for, prevent and respond to the coronavirus."[33]

While the DPA's definition of "national defense" is broad, it includes non-military priorities that are nonetheless critical to U.S. security and competitiveness.[34] Under this model, the Defense Department's Title III office would continue overseeing projects related to military and defense, and a Title III office under the Department of Commerce would oversee projects related to economic or technological competitiveness, while also removing some of the burden from the Defense Department.[35] This office, similar to that within DoD, would be responsible for managing non-military and non-defense commercial loans, grants, and subsidies. The establishment of a Title III office within Commerce would remove a key limitation in establishing a tailored, narrow U.S. industrial policy by providing a bureaucratic element capable of implementing key economic measures to shape and bolster industrial capacity for critical resources.

Address Department of Commerce resource constraints

An expansion of the Department of Commerce's authorities must be met with a commensurate increase in its resources by Congress—both on the fiscal and human capital front. The department faces a number of constraints in this regard. On the financial side, while there has been a steady increase in funding levels, they consistently fall short in meeting the burgeoning mission requirements of the department. On the human capital side, Commerce, like many other departments and agencies, struggles to recruit and retain technically proficient personnel or those with subject matter expertise on emerging technologies. The talent gap is a particularly insidious problem, as many of the department's most pressing priorities, such as export controls in foundational and emerging technologies, require significant subject matter expertise in order to craft appropriate and impactful regulation.

While there is no single silver bullet to solve these problems, steps Congress should take include:

- *Funding certain programs through the national defense budget:* The national defense budget (code "050") is routinely used to fund national defense–related programs outside of the Department of Defense, such as nuclear programs in the Department of Energy and infrastructure security work under the Cybersecurity and Infrastructure Security Agency. The

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

White House and Congress should consider using this budget to fund certain Commerce programs, such as military-related export controls, counter-proliferation, and information and communication technologies and services (ICTS) supply chain prohibitions—areas where the military has a direct stake. The move would relieve the department of considerable budgetary pressure while also providing assurances to the military that sufficient attention will be applied to issues within the Department of Commerce's remit that have a direct impact on foreign military capability and U.S. military mission assurance.

- *Establishing special hiring authorities and incentive pay:* Faced with similar talent gaps for cyber-related positions, Congress has created special hiring authorities and incentive pay for the Department of Homeland Security and the Department of Defense. Congress should codify new authorities for the Department of Commerce modeled on the cyber approach, authorizing noncompetitive, "direct hiring" authority and establishing 10–25 percent incentive pay to attract and retain highly skilled talent. These authorities would go far in ensuring the department can hire personnel quickly and maintain sufficient expertise to craft policy and regulation addressing the evolving challenges of technology competition.

MITIGATE SUPPLY CHAIN AND TECHNOLOGY TRANSFER RISK

Successfully implementing a national technology strategy will require more proactive measures to shape the global supply chain and shore up the domestic industrial base. These efforts must be matched by robust defensive measures to mitigate national security risks to the United States. The U.S. government has taken important steps over the last few years to equip itself to address global technology competition; however, significant limitations remain. Congress has an important role to play in tackling those shortfalls by updating existing laws and regulations and enacting new ones.

Codify and tailor the information and communications technology and services Executive Order 13873

Executive Order 13873 (Securing the Information and Communications Technology and Services Supply Chain), signed on May 19, 2019, represents one of the most powerful and wide-ranging tools for the United States to identify and mitigate technology supply chain risks to domestic critical infrastructure.[36] Developed over two years, the executive order delegates significant authority to the secretary of commerce to mitigate risks or block transactions involving information and communications technology and services of "foreign adversaries," which a subsequent rule lists as China, Russia, Iran, North Korea, Cuba, and Venezuela. The Interim Final Rule, issued in January 2021, identifies a wide-ranging set or classes of technology under which the rule would apply, including technology used in critical infrastructure, cloud computing and data storage, telecommunication infrastructure, consumer devices, and "emerging technologies," among others.[37]

The executive order and its implementation rest on shaky ground. The order's reliance on an emergency declaration, which can be revoked, raises questions on the appropriateness of utilizing extraordinary powers under the International Emergency Economic Powers Act (IEEPA) for what an enduring fixture in the U.S. regulatory environment could be. For comparison, an emergency declaration under IEEPA was utilized for over 20 years as the statutory basis for export controls after previous export control laws had expired. In that case, political disagreement on export control reform hampered any renewal, and it wasn't until Congress passed the Export Control Reform Act in 2018 that BIS had a firm statutory basis for its work once again.

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

Emergency declarations, while pragmatically expedient, should not be a substitute for legislative action if the interests of national security demand a more long-term, permanent solution. Additionally, the Commerce Department, never a fount of budgetary bounty, is limited in its ability to fulsomely resource transaction reviews from its existing budget, to say nothing of compliance and enforcement efforts required under such a program.

The executive order also has been rightly criticized for being overly broad in its scope of review and unclear in its implementation. For instance, it allows the secretary of commerce to review and block *all* transactions, including foreign investment, which overlaps with the Department of Treasury's authorities under the CFIUS. Industry has publicly raised concerns with the expansive nature of the executive order, stating that it lacks specificity for criteria of review or what products and services fall under the review, introducing significant uncertainty and burden in the procurement and acquisition process. Furthermore, U.S. businesses are calling for a "licensing" process by which they can "pre-clear" foreign transactions for safe harbor. While necessary to reduce business uncertainty, this process will strain departmental resources as it will vastly expand the required number of transaction reviews.

While the final rule for the executive order, and its licensing regime, has yet to be determined, significant limitations remain irrespective of the shape the program will ultimately take. A codified Executive Order 13873 should authorize the secretary of commerce to review, grant, or block licenses for certain foreign companies to import, sell, and distribute certain classes of information and communication technologies and services within the United States. This import-focused model, which shifts the focus from "prohibitions" of previous transactions to a more proactive review process, takes much of the burden off U.S. businesses, who, instead of seeking clarity for each transaction, can tailor their procurement and acquisition from a public record of foreign companies licensed to do business in the United States. Additionally, codification provides a firmer foundation for the program, eliminating dependence on an emergency declaration and establishing a statutory basis by which necessary program funding can be appropriated. The updated executive order should include:

- *Creating a new office and program:* The codification of Executive Order 13873 should accompany the establishment of an assistant secretary for supply chain and technology security under the BIS. This would ensure that the program can benefit from compliance and enforcement resources already in place (though that should be expanded). This would also give the BIS greater oversight and control of the full measure of U.S. trade in ICTS—both import and export—by which to craft policy that preserves the national security and economic security interests of the United States.

- *Modeling thresholds on CFIUS process:* The law should adopt review thresholds modeled on, but not identical to, the CFIUS process. Any qualifying ICTS product or service imported into, sold, or distributed within the United States by a company that has a controlling interest or undue influence by a foreign adversary, as determined by the secretary, would be subject to review and license requirements.

- *Issuing blocking and exclusions:* The law should allow the secretary to issue narrow, tailored exclusions for companies with a non-controlling foreign interest in instances where the import, sale, or distribution of a qualifying product or service poses an extraordinary or demonstrated risk to U.S. national security, economic security, or public health and safety.

- *Focusing on specific classes of technology and services:* The law should focus on national-level risks to sensitive data and critical infrastructure, limiting review to a core set of classes of ICTS products and services. These should include cloud services and data hosting, telecommunications equipment, semiconductors, and consumer devices and software that meet a certain threshold of products sold or number of daily active users.

- *Issuing conditional licenses:* The law should allow for the secretary to issue and establish regulations for "conditional licenses," or licenses that prescribe certain conditions that foreign companies would have to meet (such as data localization, product security standards, etc.) in order to be able to import, sell, or distribute their product or service within the United States. These licenses would be critical in shaping and mitigating security risks stemming from foreign made and manufactured products and services.

- *Addressing carve-outs and deconfliction with CFIUS process:* To ensure deconfliction, consistency, and greater certainty with U.S. and foreign business, the law should preserve and prioritize CFIUS equities in reviewing transactions on foreign direct investment. Any instance where a shift in ownership or non-controlling interest in a company would meet the threshold for CFIUS review, the CFIUS process should proceed ahead of any Department of Commerce regulatory action related to ICTS products and services.

Update the IEEPA Berman Amendment

Congress should provide the current and future administrations sufficient leeway to act on online data privacy and espionage threats by revising the Berman Amendment to exclude prohibitions against regulations on commoditized data. The exception for informational materials in the IEEPA requires updating to reflect the different technological landscape and the unprecedented creation, collection, and exploitation of data in the 21st century. Congress passed IEEPA in 1977 with the original intent of placing limits on presidential emergency powers. Since then, IEEPA has been increasingly used to impose economic-based sanctions by placing limits on a range of international transactions by foreign states and governments, and non-state actors such as terrorist groups.

Congress amended IEEPA in 1988 and 1994 with the so-called Berman Amendment to protect the rights of U.S. persons in the exchange of information published in a wide array of formats including postal and telephonic communication, films, photographs, news wire feeds, and various electronic media.[38] The intent for this amendment, an informational materials exception, was to maintain the legality of communications, such as certain exchanges with scientific communities in embargoed countries including Cuba, Libya, and Sudan.

Despite this attempt at clarification, conflicting readings of the law persisted. In 2003, the Treasury Department's Office of Foreign Assets Control (OFAC) interpreted the updated act such that substantive revisions to manuscripts that would "significantly alter" the document constitutes a "substantive enhancement" and a "benefit" to a sanctioned nation, and thus be illegal.[39] In practice, this meant that U.S. organizations could not edit or ultimately publish articles by authors from countries embargoed by the United States.[40] By early 2004, several scientific publishers had pushed back on or ignored these restrictions.[41] OFAC ultimately relented and in May 2004 ruled that manuscripts from U.S.-embargoed countries could be edited and published.[42]

A more complex and consequential challenge to IEEPA, anchored in the Berman Amendment, arose in the wake of the Trump administration's 2020 executive order on the Chinese social media app TikTok. The order would have effectively banned TikTok by making transactions—such as hosting it on app stores and providing internet hosting services—between ByteDance, TikTok's parent company, and U.S. persons illegal.[43] The Trump administration pursued similar action against the social media application WeChat, owned by TenCent Holdings.[44]

TikTok sued the Trump administration in September 2020 and was granted a preliminary injunction on the basis that the executive order violated the informational materials exception of the Berman Amendment.[45] In a final ruling in December 2020, the court further rejected the Trump administration's argument that there was a cyber espionage exception to the Berman Amendment.[46] The court cases remained on hold as the Biden administration took office in January 2021. On June 9, 2021, President Biden issued an executive order that revoked the Trump-era bans on TikTok and WeChat and outlined new criteria for assessing the risks posed by such applications.[47]

The Biden administration's hands are effectively tied now when it comes to using IEEPA to address the national security concerns associated with social media applications and websites, which obtain vast amounts of data associated with U.S. persons that could be exploited by foreign governments. A ban of such applications and sites would be nigh impossible to achieve given prior court rulings. The Berman Amendment was written at a time when data generation, harvesting, and exploitation of the scale and scope as it occurs in 2021 was almost unfathomable. The resulting commoditization of data, such as through predictive analytics and data services that transcend and supersede an individual's right to exchange information, means that the informational materials exception should be revised. An updated amendment should account for these ubiquitous and expansive data flows and their potential malicious exploitation at scale, while maintaining the original purpose of the amendment.

Establish minimum cyber and personnel security standards and requirements for recipients of federal R&D funding

The Office of Science and Technology Policy (OSTP), in conjunction with the Department of Justice, the Cybersecurity and Infrastructure Security Agency, and other federal entities must act to set cyber and personnel security standards and requirements for recipients of federal funding. In recent months, U.S. policymakers and government officials have renewed efforts and explored new avenues to protect the country's R&D infrastructure from intellectual property theft. Throughout U.S. history, both adversaries and allies have engaged in illicit practices to secure U.S. technology or know-how, but China's technology transfer efforts are unmatched in scale and effectiveness.

In response to this threat, the United States has attempted to bolster its research security, both in the private and public sector. While the U.S. government is limited in its authority to enact policies and regulations around private sector R&D, there are measures lawmakers and officials can take to better secure federally funded R&D efforts.[48]

The Government Accountability Office (GAO) published a report in late 2020 documenting some of the weaknesses it observed in five federal agencies' foreign influence policies.[49] The report focused on the National Institutes of Health, National Science Foundation, NASA, DoD, and Department of Energy—which account for 90 percent of all federal R&D funding. In its report, the GAO concluded, "Effectively addressing the critically important threat of foreign influence in federally funded research depends, in part, on agencies having agency-wide policies on conflicts of interest, written procedures on how to improve policies and address foreign threats."[50]

Building off of the GAO's efforts, OSTP should work with federal agencies to craft consistent reporting requirements for research institutions and universities.[51] Unified reporting requirements not only would help government agencies combat intellectual property theft and foreign influence in federally funded R&D, but also would provide higher education and research institutions with consistent requirements to meet.

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

Enact a National Data Protection and Privacy Law

Congress should pass legislation to effectively address national security risks, streamline regulations, mitigate barriers to innovation, and create a better environment for global influence on data protection and privacy issues. The patchwork of U.S. data protection and privacy laws presents hurdles to identifying and mitigating national security risks associated with foreign investments in the United States. Fundamentally, there are inconsistent standards across the landscape of federal and state jurisdictions that govern private companies' use, disposal, and stewardship of U.S. persons' data. A comprehensive national data protection and privacy law would serve as the primary means to regulate data practices of foreign companies operating in the United States, a function that is currently intermittently assumed by the CFIUS process on a de facto basis. These baseline requirements would serve as a more universal standard when evaluating the risk of a foreign company's investment, merger, or acquisition in the United States—allowing for a more consistent framework for risk assessment under programs like CFIUS and the EO13873. Beyond these programs, such a law would establish reliable and efficient compliance mechanisms neither limited nor reliant on federal national security programs for occasional review and enforcement. Finally, a national data security and privacy law also would benefit tech development and applications and facilitate setting shared norms and standards with like-minded countries.

Federal statutes for protecting personal data or cybersecurity are focused on specific sectors—for example, banking and finance under the Gramm-Leach-Bliley Act and healthcare under the Health Insurance Portability and Accountability Act—and are enforced by different agencies such as the Consumer Finance Protection Bureau and the Department of Health and Human Services.[52]

Two states have enacted their own data privacy laws that differ from federal statutes in that they apply across sectors. The New York SHIELD Act concerns protections from data breaches of personal information. The California Consumer Privacy Act introduced broad individual consumer rights and places stipulations on any entity or person that collects personal information about or from a California resident.[53]

While these privacy laws primarily are U.S.-focused, there is growing interest in restricting the transfer of personal data abroad. The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) gave the Committee on Foreign Investment in the United States (CFIUS) new authorities pertaining to foreign data access. The FIRRMA rules identify 11 categories for "sensitive personal data" that could be exploited in a way that threatens national security. The categories span industries and sectors, and include data on health, finance, biometrics, and geolocation. The rules for CFIUS review only apply, however, if the data targets executive branch personnel or contractors, or if it concerns aggregated data of one million Americans or more, unless it concerns genetic data. In other words, there are major exemptions that provide openings for data exploitation that may not be in the national interest.[54]

Data protection and privacy is of concern in the context of supply chain risk management as well. Securing data and ensuring data privacy are increasingly regarded as key contract award criteria.[55] Such controls also form a baseline to protect the integrity of a system and to manage information security risk. The National Institute of Standards and Technology has published a set of security and privacy safeguarding measures for computing platforms.[56] These controls are mandatory for federal information systems; there are no equivalent requirements for private industry. The Solar Winds supply chain hack—where the cyber attack was carried out via malicious updates to a seemingly innocuous and trusted software product—underscores the need for a comprehensive rethink of software supply chain risks and associated information sharing.

In May 2021, the Biden administration issued an executive order on cybersecurity that removes contractual barriers to sharing threat information between the federal government and information and communication technology service providers. The directive also mandates that service providers promptly report cyber incidents affecting software or services provided to government agencies.[57] Any firm seeking to do business with the U.S. government will have to meet higher security standards and performance.[58] While an important step in the right direction, addressing data security, data privacy, and related supply chain risk management for government contracts addresses only part of the problem.

This piecemeal approach to data protection and privacy is untenable. Beyond the direct effect on national security decisionmaking, a haphazard quilt of rules across the United States hinders innovation and economic competitiveness and makes it challenging for the United States to shape global norms similar to the approach the European Union has adopted under the General Data Protection Regulation (GDPR).[59]

Momentum for such a law is growing. A bill addressing consumer data privacy regulation, the Information Transparency and Personal Data Control Act, was introduced in March 2021.[60] Numerous lawmakers in the House of Representatives and Senate also reportedly plan to introduce or reintroduce other data protection and data privacy bills during the 117th Congress.[61] A roll-up and harmonization of these varied efforts could form the foundation for comprehensive legislation on par with laws such as GDPR.

STREAMLINE TECHNOLOGY POLICY COORDINATION AND IMPLEMENTATION

Ensuring a unified and coherent implementation of a national technology strategy will be near impossible without creating mechanisms for interagency coordination. The United States in the past few years has created new authorities—such as the Federal Acquisition Supply Chain Security Act and the Export Control Reform Act — to shape the global technology ecosystem (and has expanded the use of existing ones, including the DPA and CFIUS). Left unaddressed, however, is that these authorities are dispersed across a number of departments and agencies with few mechanisms to establish a common understanding of a particular problem and often ad hoc decisionmaking on related issues. Further compounding these hurdles is the lack of universal agreement on concepts such as “unacceptable risk” or what are “critical” technologies. These recommendations go at the heart of those problems.

Establish a Technology Security Coordination Group (TSCG)

The White House should set up this group to coordinate technology and supply chain security–related regulatory and policy actions. It should be an interagency coordination group modeled on the Cyber Response Group. The proliferation of different supply chain and technology–related authorities in the past few years, and the increasing willingness to use them, has prompted questions as to how these programs will be integrated, coordinated, and deconflicted. They are myriad and spread across departments and agencies. While the full suite of authorities is too numerous to list here, the most prominent include: CFIUS for foreign investment, the ICTS Supply Chain Executive Order for products and services in the United States, the Federal Acquisition Security Council (FASC) for products and services used by the U.S. government, and the “Team Telecom” process for reviewing licenses for foreign telecommunications providers. While certain programs have relatively narrow scope of authorities, in some cases they intersect or overlap. For example, the ICTS Executive Order authorizes the secretary of commerce to review foreign investment transactions related to ICTS (an overlap with CFIUS) and ban products or services from being used by the U.S. government if they pose a national security risk (an overlap with FASC).

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

Despite the intersection and overlap within these programs, there doesn't exist a central, standing mechanism for their routine coordination. While certain programs do require interagency coordination (CFIUS, ICTS executive order, etc.) in their transaction reviews, this falls short of the type of systematic and deliberate coordination afforded in other, complex areas of national security. Cybersecurity, for instance, relies on a suite of interdependent and interlocking authorities spread across nearly all U.S. departments and agencies. The success of U.S. cyber strategy ultimately means utilizing these authorities in lockstep for greatest possible effect with common awareness of actions and priorities. In supply chain and technology security, the U.S. government should adopt a similar model, driving closer coordination across a mutually dependent epistemic group among the interagency.

The purpose of the group will be to routinely coordinate and deconflict current and prospective cases under their respective authorities, share information, and ensure the United States is taking a consistent and unified approach. While the group should not undercut or circumvent any secretary's departmental authority, it should act as a forum to identify appropriate tools to use, either alone or in concert, to address a policy objective or an identified emerging threat to national security. The TSCG should be cochaired and managed by the Office of the National Cyber Director and a new Deputy National Security Advisor for Technology Competition.

Key components of the TSCG should be:

- *Inclusion of programs:* The TSCG should include representatives from the CFIUS (Department of the Treasury), the FASC, the BIS (representing Export Control equities), the Department of Commerce (representing Information and Communication Technology and Service supply chain programs), and the Department of Justice (representing "Team Telecom").

- *Forum for strategic harmonization:* The ultimate goal of this group should be to harmonize and make consistent the approach utilized in their respective programs. The TSCG should act as a primary forum to establish common risk matrices and frameworks for evaluating technology-related "high-risk" vendors, foreign investment, and supply chain threats to U.S. infrastructure. Additionally, the TSCG should work toward identifying common mitigations that can be used across a variety of different foreign transaction review programs.

- *Inclusion of Intelligence Community:* Similar to the Cyber Response Group, the TSCG should include representatives from the Office of the Director of National Intelligence and other members of the Intelligence Community to routinely brief on new and emerging threats to the U.S. economic and technology supply chain that can be addressed by authorities represented in the group.

Craft a government-wide definition for "critical technology" and create a framework and mechanism for making prioritization decisions

A panel of experts from across the federal government must converge to establish a uniform definition for critical technology and a technology prioritization schema. A fundamental necessity for crafting and executing a national technology strategy is determining what technology areas are most relevant to achieving the United States' strategic vision and how to prioritize those technologies to allocate resources accordingly. So far, U.S. leaders have failed to do so. The myriad of efforts to identify "critical technologies" have proven parochial, ephemeral, inconsistent, and ill-defined.

It is no surprise that where a person sits shapes their priorities. As a result, the critical and emerging technologies mentioned in the 2017 National Security Strategy, the 2018 National Defense Strategy and the 2018–2022 Strategic Plans of the Departments of State and Commerce—all published within weeks of each other—have limited overlap. Presidential determinations for critical technologies under the Defense Production Act are far from comprehensive and are issued irregularly and on an ad hoc basis.[62] There is no mechanism or effort to harmonize these designations, nor to develop a set of baseline criteria by which departments and agencies—or the White House itself—can consistently define a comprehensive list.

Such lists generally don't have much longevity or provide meaningful detail as to why those technology categories are important. Department of Defense officials in particular have been prone to making regular pronouncements on what technologies should be a priority without providing the underlying rationale. At times, departmental leaders have made contemporaneous announcements on technology priorities that contradict each other.[63]

These deficits are most apparent in the document that should be setting the example: the 2020 National Strategy for Critical and Emerging Technologies.[64] Critical and emerging technologies are defined as "those technologies that have been identified and assessed by the National Security Council to be critical, or to potentially become critical, to the United States' national security advantage, including military, intelligence, and economic advantages." Such a definition falls well short of what is needed to identify technology priorities for long-term strategic planning. As a result, the document's annex comprises a list of 20 broad technology categories—such as advanced conventional weapons technologies and energy technologies—with no accompanying explanation or justification. Government leaders cannot take effective action with inadequate guidance.

To avoid these pitfalls and to provide the strategic direction needed to set realistic priorities, the National Security Council staff should lead an interagency effort to craft a shared definition and an associated decisionmaking framework. The most comprehensive definition of "critical technologies" is in Title 50 U.S. Code § 4565 and could be used as a starting point for a revised government-wide definition for the purposes of crafting a national technology strategy.[65] A viable definition of "criticality" should take into account what technologies are essential for the United States to compete economically and secure its national interests.

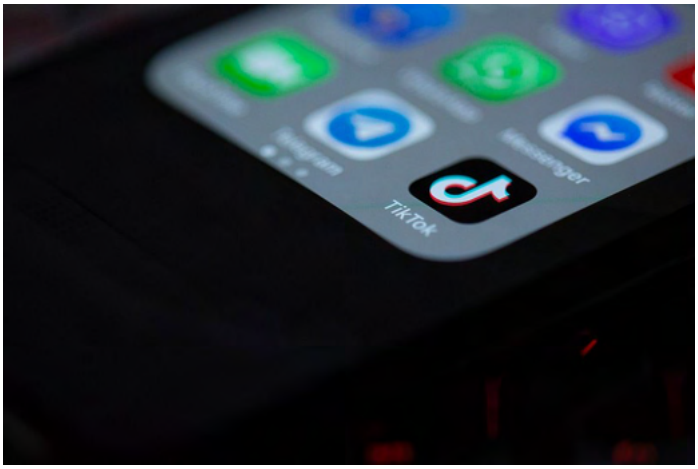
This effort should include:

- *Rigorous prioritization schema:* To guide prioritizing those technologies, the report "Taking the Helm" proposed a four-part schema: (1) leading-edge—the technology areas where the United States must strive to have the most advanced capabilities in the world; (2) world-class—the technology areas where the United States should strive to be among the world's best; (3) fast follower—the technology areas where the United States retains strong capabilities but can afford to not be among the world's best at the outset; and (4) over-the-horizon—longer-term R&D investments, primarily in basic research, spanning the spectrum of technological disciplines.[66]

- *Yearly report on presidential determinations:* The executive branch should conduct a yearly or biennial review on critical resource determinations and consider making such a cohesive list public—providing an assessment and update of additions, deletions, or changes from the previous year. This requirement would be a critical measure for "good governance" and a forcing function for the U.S. government to ensure that the totality of existing determinations reflect economic and strategic need and continue to align with U.S. national security policy.

Codify and designate the Department of Commerce International Trade Administration's Office of Industry & Analysis as the federal government center for foreign company risk information

Congress should pass a law making the Department of Commerce the U.S. government's central repository and clearinghouse for information related to foreign companies, specific sensitive information, and corporate due diligence information. Foreign investment, supply chain, and foreign transaction reviews each require in-depth knowledge of foreign companies participating in a particular transaction. In determining the national security risk that the transaction may pose, ownership structure, relations with a foreign government, business operations, and security practices (among other issues) are routinely examined to understand the risk profile of the particular corporation. Departments and agencies collect this information from a number of sources. For one, a basic capability is utilizing proprietary sources, such as those provided by Dun & Bradstreet or Bloomberg, for basic public information such as investors, corporate structure, board members, and subsidiaries. Specific programs often have unique authorities by which they can collect additional, nonpublic, sensitive business information. For instance, the ICTS executive order authorizes the secretary of commerce to issue subpoenas for documents, take testimony, and conduct interviews. Departments and agencies operating under the CFIUS additionally are routinely provided with nonpublic information throughout their process from the businesses in question. It is not uncommon for a foreign company, or its product or subsidiary, to be the primary subject of review across a variety of different programs. A good example of this is ByteDance, which in 2020 was subject to both a CFIUS review of its investment in Music.ally and a ban of its app TikTok under the ICTS executive order.



President Biden has recently ordered a Department of Commerce review of security concerns posed by TikTok, owned by ByteDance. (Solen Feyissa , license cc-by-sa-2.0)

Despite these programs relying on identical information (and asking the same questions) related to a foreign company that may be at issue in their respective reviews, there exists no interagency mechanism to routinely share or compile basic corporate due diligence or risk information between them. Information collected in the course of these reviews is not routinely centralized or compiled for a comprehensive, living risk profile of foreign companies. In some instances, the barrier is procedural or programmatic; sharing information simply has not been instituted in the process. In others, no department or agency has been designated or charged with collecting and compiling this information for distribution. The most problematic barrier, however, is legal. The underlying statute for CFIUS specifically prohibits sharing nonpublic, sensitive business information outside of the personnel involved in the foreign investment review process. As CFIUS is one of the most active, long-standing, and prolific sources of this information, this is a considerable limitation in establishing a common risk profile on certain foreign companies.

The new law therefore should address:

- *Sharing of foreign company sensitive information:* The law should amend the Foreign Risk Review Modernization Act (FIRRMA) to remove prohibitions against sharing sensitive business information outside the CFIUS review process, but limit distribution to other, designated foreign transaction or supply chain review programs, such as those under the ICTS executive order and the FASC.

- *Corporate due diligence shared services:* The law should direct the executive branch to consolidate department and agency contracts for corporate due diligence information (through vendors such as Bloomberg, Dun & Bradstreet, etc.) into a single shared service provided by the Department of Commerce. This model would reduce program redundancies across departments and agencies and ensure that irrespective of funding each department or agency is sufficiently informed from a common set of information by which to conduct their risk-based assessments.

- *Procedures for mandatory sharing and consolidation:* In implementing this law, the executive branch should establish additional procedures and requirements for departments and agencies to share with the Department of the Treasury any nonpublic information related to foreign corporations collected in the course of their reviews, to include other supply chain and foreign transaction review programs.

- *Expanded use of the International Investment and Trade in Services Survey Act:* To fully empower this capability, the Department of Commerce should expand its use of the International Investment and Trade in Services Survey Act, which authorizes the department to compel industry surveys on foreign investment in the United States.

Establish a National Economic and Technology Security Intelligence Center (NETSIC) housed in the Office of the Director of National Intelligence

Congress should establish a dedicated economic and technology security intelligence center. The U.S. government lacks a centralized capability to properly research, analyze, and assess the full suite of issues related to technology competition. While the federal government has made substantial progress on resourcing issues related to economic, technology, and supply chain security, these efforts will be incomplete without routine assessments of foreign adversary technology development, supply chain dependencies, and industrial capacity. Further, without sustained attention and prioritization by the Office of the Director of National Intelligence, Intelligence Community elements are unlikely to shift collection requirements or programmatic funding necessary to keep policymakers abreast of issues relevant to technology competition.

The center, composed of elements drawn from the Economic Security and Financial Intelligence Executive and the National Counterintelligence and Security Center, among other offices, should be staffed with personnel from the Department of Commerce, Department of Defense, Department of Homeland Security, Department of Treasury, and the Department of State. It should include representatives from intelligence agencies such as the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency, and the Federal Bureau of Investigation. The NETSIC would work hand-in-hand with existing functions of the Office of the Director of National Intelligence, such as the National Intelligence Officer and National Intelligence Manager for Science and Technology, each of whom manage existing programs to understand and counter threats to the U.S. economy and its supply chain.

- Key functions: Key functions of the NETSIC should include the centralization and aggregation of intelligence related to vulnerabilities in the industrial base of foreign countries, track foreign emerging technology developments, and establish a “map” of foreign supply chain and economic dependencies. Such information will be vital in informing U.S. economic and technology policy in an era of great power competition, which will require identifying risks to the U.S. industrial base and crafting courses of action necessary to address them.

- International cooperation: The NETSIC should seek broader engagement on economic and technology-related intelligence with allied countries, such as through the "Five Eyes" intelligence partnership (Australia, Canada, New Zealand, United Kingdom, United States) and with countries that maintain similar concerns over technology competition with China, such as Taiwan and Japan.

- Support to the Technology Competition Coordination Office: The NETSIC would be critical in supporting the Deputy National Security Advisor for Technology Competition and the cross-cutting "Technology Competition Coordination Office" proposed in "Trust the Process," the second report in this series. "This office should include directorates focused on the strategy pillars of promote, protect, and partner, as well as a critical technologies directorate for implementation relevant to priority technology areas, each charged with staffing and coordinating interagency policy processes."

INCREASE CAPACITY TO PURSUE INTERNATIONAL TECHNOLOGY PARTNERSHIPS

Collaboration with U.S. allies and other tech-leading democracies is a necessary component of an effective and pragmatic U.S. national technology strategy. America and its allies together comprise an unmatched powerhouse of technological expertise, human capital, and science & technology infrastructure. Increasingly, these countries are aligned on a range of technology issues.

The Biden administration and Congress are taking action to enhance technology collaboration with key countries. President Biden is engaging bilaterally with Japan, the Quadrilateral Security Dialogue, and the European Union among others on aligning policies and exploring joint R&D in areas including wireless communications, semiconductors, and supply chain integrity. A flurry of recent bills in Congress, such as the CHIPS for America Act, the USA Telecommunications Act, and the U.S. Innovation and Competition Act of 2021, all contain provisions for international cooperation.

Create a Technology Partnership Office at the Department of State

Congress should expand the U.S. government's capacity to initiate, maintain, and expand international technology partnerships by establishing a dedicated office with this mandate. This office, headed by an assistant secretary for technology, would be responsible for managing America's technology partnerships. At present, the National Security Council staff is managing the Biden administration's efforts in this area. Maturing and managing a growing array of such partnerships will require a permanent office with requisite bureaucratic clout to sustain this pillar of the strategy. The ultimate goal for this office should be to create a technology alliance of a small group of countries to serve as the core of a constellation of partnerships. The United States Innovation and Competition Act of 2021 contains a provision for the creation of such an office.

Conclusion

Crafting sound strategy is difficult. Executing a strategy well is more challenging still. An effective and realistic national technology strategy requires vision, process, an executable framework, and a commitment to addressing bureaucratic, legal, and regulatory hurdles to implementation. Policymakers and thought leaders like to focus on the big picture. The visionary elements of articulating strategy make for catchy soundbites. What often gets short shrift are the decisions and actions necessary to put a strategy in motion. Processes are essential to impactful execution of strategy. Once a vision is articulated, a framework crafted, and processes identified, the focus must be on actions required to operationalize the national technology strategy. How and whether those actions are implemented will have outsized influence over the strategy's ultimate success.

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

[1] Martijn Rasser and Megan Lamberth, "Taking the Helm: A National Technology Strategy to Meet the China Challenge," CNAS, January 13, 2021, https://www.cnas.org/publications/reports/taking-the-helm-a-national-technology-strategy-to-meet-the-china-challenge.
[2] Loren DeJonge Schulman and Ainikki Riikonen, "Trust the Process: National Technology Strategy Development, Implementation, and Monitoring and Evaluation," CNAS, April 20, 2021, https://www.cnas.org/publications/reports/trust-the-process.
[3] Anshu Siripurapu, "Is Industrial Policy Making a Comeback?" Council on Foreign Relations, March 16, 2021, https://www.cfr.org/backgrounder/industrial-policy-making-comeback; Dylan Gerstel and Matthew P. Goodman, "From Industrial Policy to Innovation Strategy," Center for Strategic & International Studies, September 2020, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200901_Gerstel_InnovationStrategy_FullReport_FINAL_0.pdf; and Robert D. Atkinson, "The Case for a National Industrial Strategy to Counter China's Technological Rise," Information Technology & Innovation Foundation, April 13, 2020, https://itif.org/publications/2020/04/13/case-national-industrial-strategy-counter-chinas-technological-rise.
[4] Rasser and Lamberth, "Taking the Helm."
[5] Gerstel and Goodman, "From Industrial Policy to Innovation Strategy."
[6] Siripurapu, "Is Industrial Policy Making a Comeback?"
[7] Gerstel and Goodman, "From Industrial Policy to Innovation Strategy," 1; Alexander Hamilton, "Final Version of the Report on the Subject of Manufactures," December 5, 1791, https://founders.archives.gov/documents/Hamilton/01-10-02-0001-0007.
[8] For more information on how industrial policy was used throughout the Cold War, see Rasser and Lamberth, "Taking the Helm."
[9] Institute of Medicine, *Establishing Precompetitive Collaborations to Stimulate Genomics-Driven Product Development: Workshop Summary* (Washington: National Academies Press, 2011), https://www.ncbi.nlm.nih.gov/books/NBK54317/; National Research Council of the National Academies, *Securing the Future: Regional and National Programs to Support the Semiconductor Industry* (Washington: National Academies Press, 2003), https://www.nap.edu/read/10677/chapter/6#101. For more information on SEMATECH, see Robert D. Hof, "Lessons from Sematech," *MIT Technology Review*, July 25, 2011, https://www.technologyreview.com/2011/07/25/192832/lessons-from-sematech/; Michaela D. Platzer and John F. Sargent Jr., "U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy," R44544, Congressional Research Service, June 2016, https://crsreports.congress.gov/product/pdf/R/R44544/3; and Rasser and Lamberth, "Taking the Helm."
[10] Jennifer Harris and Jake Sullivan, "American Needs a New Economic Philosophy. Foreign Policy Experts Can Help," *Foreign Policy*, February 7, 2020, https://foreignpolicy.com/2020/02/07/america-needs-a-new-economic-philosophy-foreign-policy-experts-can-help/; Senator Charles Schumer, "S.1260 - United States Innovation and Competition Act of 2021," https://www.congress.gov/bill/117th-congress/senate-bill/1260.
[11] Atkinson, "The Case for a National Industrial Strategy"; Harris and Sullivan, "American Needs a New Economic Philosophy.""""
[12] Harris and Sullivan, "American Needs a New Economic Philosophy"; Jared Bernstein, "The Time for American to Embrace Industrial Policy Has Arrived," *Foreign Policy*, July 22, 2020, https://foreignpolicy.com/2020/07/22/industrial-policy-jobs-climate-change/; and Marco Rubio, "Exclusive: American Industrial Policy and the Rise of China," *The American Mind*, December 10, 2019, https://americanmind.org/memo/american-industrial-policy-and-the-rise-of-china/.
[13] Rubio, "Exclusive: American Industrial Policy and the Rise of China."
[14] Noam Scheiber, "The Biden Team Wants to Transform the Economy. Really," *The New York Times*, February 11, 2021, https://www.nytimes.com/2021/02/11/magazine/biden-economy.html. President Biden's Build Back Better plan is a three-part agenda to "rescue, recover, and rebuild the country." It includes the American Rescue Plan, the American Jobs Plan, and the American Families Plan. The White House, "Build Back Better," https://www.whitehouse.gov/build-back-better/.
[15] Shannon K. O'Neil, "Protection Without Protectionism: Getting Industrial Policy Right," *Foreign Affairs* , (January/February 2021), https://www.foreignaffairs.com/articles/united-states/2020-12-08/protection-without-protectionism.
[16] The White House, *National Security Strategy of the United States of America*, 2017, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf; the White House, *National Strategy for Critical and Emerging Technologies*, 2020, https://www.hsdl.org/?abstract&did=845571; and U.S. Department of Commerce, "Strengthen U.S. Economic and National Security," https://www.commerce.gov/about/strategic-plan/strengthen-us-economic-and-national-security.

[17] Christopher Darby and Sarah Sewall, ""The Innovation Wars: America's Eroding Technological Advantage," *Foreign Affairs* , (March/April 2021), https://www.foreignaffairs.com/articles/united-states/2021-02-10/technology-innovation-wars.
[18] Paul Scharre and Ainikki Riikonen, "Defense Technology Strategy," CNAS, November 17, 2020, 6, https://www.cnas.org/publications/reports/defense-technology-strategy.
[19] Scharre and Riikonen, "Defense Technology Strategy," 7.
[20] Martijn Rasser, Megan Lamberth, Ainikki Riikonen, Chelsea Guo, Michael Horowitz, and Paul Scharre, "The American AI Century: A Blueprint for Action," CNAS, December 17, 2019, 35, https://www.cnas.org/publications/reports/the-american-ai-century-a-blueprint-for-action.
[21] Saif M. Khan, "Securing Semiconductor Supply Chains," Center for Security and Emerging Technology, January 2021, 3, https://cset.georgetown.edu/publication/securing-semiconductor-supply-chains/.
[22] The White House, "Fact Sheet: Quad Summit," March 12, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/12/fact-sheet-quad-summit/.
[23] Cat Zakrzewski, "The Technology 202: Bipartisan bill would fund tech partnerships with allies to counter China," *The Washington Post*, March 4, 2021, https://www.washingtonpost.com/politics/2021/03/04/technology-202-bipartisan-bill-would-fund-tech-partnerships-with-allies-counter-china/.
[24] Martijn Rasser, Rebecca Arcesati, Shin Oya, Ainikki Riikonen and Monika Bochert, "Common Code: An Alliance Framework for Democratic Technology Policy," CNAS, October 21, 2020, https://www.cnas.org/publications/reports/common-code; Jared Cohen and Richard Fontaine, "Uniting the Techno-Democracies: How to Build Digital Cooperation," *Foreign Affairs*, November/December 2020, https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies.
[25] While there are constraints with designating a portion of Commerce as a member of the U.S. Intelligence Community (such as restrictions on handling citizens' personal data), it is important to note that these restrictions are largely limited to the specific office that is designated. For instance, Intelligence and Analysis, the IC element within DHS, remains distinct from the Cybersecurity and Infrastructure Security Agency, which, as a separate office, is allowed to handle U.S. persons data and is unfettered in working directly with U.S. industry.
[26] Bureau of Industry and Security, U.S. Department of Commerce, *U.S. Industrial Base Surveys Pursuant to the Defense Production Act of 1950* (Washington: 2015), 41426, https://www.federalregister.gov/documents/2015/07/15/2015-17388/us-industrial-base-surveys-pursuant-to-the-defense-production-act-of-1950; Andrew J. Grotto, "U.S. Policy Toolkit for Kaspersky Labs," *Lawfare*, March 15, 2018, https://www.lawfareblog.com/us-policy-toolkit-kaspersky-labs.
[27] Bureau of Industry and Security, U.S. Department of Commerce, "Industrial Base Assessments," https://www.bis.doc.gov/index.php/other-areas/office-of-technology-evaluation-ote/industrial-base-assessments.
[28] Jamie Baker, "A DPA for the 21st Century," Center for Security and Emerging Technology, April 2021, 20, https://cset.georgetown.edu/publication/a-dpa-for-the-21st-century/.
[29] Matthew Seaford, "Title III of the Defense Production Act," https://www.energy.gov/sites/prod/files/2014/03/f14/2_seaford_roundtable.pdf.
[30] FEMA, "Defense Production Act Authorities," https://www.fema.gov/disasters/defense-production-act/dpa-authorities; Taite McDonald and Sara Hochman, "Defense Production Act (DPA) Title III," Wilson Sonsini Goodrich & Rosati Professional Corporation, https://www.wsgr.com/PDFSearch/defense-production-act-title-iii.pdf.
[31] FEMA, "Defense Production Act Authorities"; Defense Production Act Title III Office, "Defense Production Act Title III Overview," https://www.businessdefense.gov/DPA-Title-III/Overview/; and Seaford, "Title III of the Defense Production Act."
[32] Shayan Karbassi, "Understanding Biden's Invocation of the Defense Production Act," *Lawfare*, March 4, 2021, https://www.lawfareblog.com/understanding-bidens-invocation-defense-production-act; Defense Production Act Title III Office, "Defense Production Act Title III Overview"; Defense Production Act Title III Office, "Defense Production Act Title III Presidential Determinations for Small Unmanned Aerial Systems,"June 12, 2019, https://www.businessdefense.gov/News/News-Display/Article/1873243/defense-production-act-title-iii-presidential-determination-for-small-unmanned/; Michael H. Cecire and Heidi M. Peters, "The Defense Production Act of 1950: History, Authorities, and Considerations for Congress," R43767, Congressional Research Service, March 2020, https://fas.org/sgp/crs/natsec/R43767.pdf; and Seaford, "Title III of the Defense Production Act."
[33] Jonathan Hoffman, "Statement on the Department's Use of Defense Production Act Title III," U.S. Department of Defense, September 23, 2020, https://www.defense.gov/Newsroom/Releases/Release/Article/2358713/statement-on-the-departments-use-of-defense-production-act-title-iii/; Jerry McGinn and Daniel Kaniewski, "Where Does the Defense Production Act Go from Here?" *Defense One*, November 24, 2020, https://www.defenseone.com/ideas/2020/11/where-does-defense-production-act-go-here/170301/.
[34] As James Baker explains in his report, "A DPA for the 21st Century," Title III authorities could be used to "generate a U.S. capacity." As Baker notes, "As the National Security Commission on AI has noted, a Dutch company is the only company in the world that produces Extreme Ultraviolet (EUV) lithographic scanners. Title III thus could be used

to incentivize the establishment of a domestic manufacturing capability and to guarantee purchase of a market-appropriate number of scanners." Baker, "A DPA for the 21st Century."
[35] McGinn and Kaniewski, "Where Does the Defense Production Act Go from Here?"
[36] The White House, "Securing the Information and Communications Technology and Services Supply Chain," Executive Order 13873, May 15, 2019, https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.
[37] U.S. Department of Commerce, "Securing the Information and Communications Technology and Services Supply Chain," 2021-01234, January 19, 2021, https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain.
[38] Christopher A. Casey, Dianne E. Rennack, Ian F. Fergusson, and Jennifer K. Elsea, "The International Emergency Economic Powers Act: Origins, Evolution, and Use," R45618, Congressional Research Service, July 14, 2020, https://fas.org/sgp/crs/natsec/R45618.pdf.
[39] Bruce Craig, "Sleeping with the Enemy? OFAC Rules and First Amendment Reforms," *Perspectives on History*, May 1, 2004, https://www.historians.org/publications-and-directories/perspectives-on-history/may-2004/sleeping-with-the-enemy-ofac-rules-and-first-amendment-freedoms.
[40] Jean Kumagai, "Will U.S. Sanctions Have Chilling Effect on Scholarly Publishing?" *IEEE Spectrum*, November 3, 2003, https://spectrum.ieee.org/at-work/tech-careers/will-us-sanctions-have-chilling-effect-on-scholarly-publishing.
[41] Lila Guterman, "Publishers Grapple With Trade Embargoes," *The Chronicle of Higher Education*, March 5, 2004, https://www.chronicle.com/article/publishers-grapple-with-trade-embargoes/.
[42] Simson Garfinkel, "A Ruling in Favor of Academic Freedom," *MIT Technology Review*, May 9, 2004, https://www.technologyreview.com/2004/05/09/232884/a-ruling-in-favor-of-academic-freedom/.
[43] The White House, "Executive Order on Addressing the Threat Posed by TikTok," August 6, 2020, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/.
[44] The White House, "Addressing the Threat Posed by WeChat, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain," Executive Order 13943, August 6, 2020, https://www.govinfo.gov/content/pkg/FR-2020-08-11/pdf/2020-17700.pdf.
[45] United States District Court for the District of Columbia, "TikTok Inc., et al., v. Donald J. Trump, President of the United States, et al.," Civil Action No. 1:20-cv-02658 (CJN), September 27, 2020, https://www.courtlistener.com/recap/gov.uscourts.dcd.222257/gov.uscourts.dcd.222257.30.0_3.pdf.
[46] Adam Berry and Barbra Kim, "Court Rulings Reinforce Limitations on Sweeping Executive Orders Based on IEEPA," JDSUPRA, December 15, 2020, https://www.jdsupra.com/legalnews/court-rulings-reinforce-limitations-on-80560/.
[47] The White House, "Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries," June 9, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/.
[48] As Melissa Flagg and Zachary Arnold address in their CSET report on research security, the bulk of U.S. R&D is happening in the private sector where the U.S. government is limited by authority, information, and trust. Melissa Flagg and Zachary Arnold, "A New Institutional Approach to Research Security in the United States," Center for Security and Emerging Technology, January 2021, 5, https://cset.georgetown.edu/publication/a-new-institutional-approach-to-research-security-in-the-united-states/.
[49] U.S. Government Accountability Office, "Federal Research: Agencies Need to Enhance Policies to Address Foreign Influence," GAO-21-130, December 2020, https://www.gao.gov/assets/gao-21-130.pdf.
[50] U.S. Government Accountability Office, "Federal Research."
[51] Ainikki Riikonen and Emily Weinstein, "Rethinking Research Security," *Lawfare*, June 24, 2021, https://www.lawfareblog.com/rethinking-research-security.
[52] Stephen P. Mulligan and Wilson C. Freeman, "Data Protection Law: An Overview," R45631, Congressional Research Service, March 25, 2019, https://fas.org/sgp/crs/misc/R45631.pdf.
[53] Angelique Carson, "Data privacy laws: What you need to know in 2021," Osano, June 22, 2021, https://www.osano.com/articles/data-privacy-laws.
[54] McDermott Will & Emery, "Spotlight on Sensitive Personal Data as Foreign Investment Rules Take Force," *The National Law Review*, February 18, 2020, https://www.natlawreview.com/article/spotlight-sensitive-personal-data-foreign-investment-rules-take-force.
[55] Chris Nissen, John Gronager, Robert Metzger, and Harvey Rishikof, "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War,"MITRE Center for Technology & National Security, August 26, 2019, https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-26AUG2019.pdf.
[56] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, September 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[57] The White House, "Executive Order on Improving the Nation's Cybersecurity," May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.
[58] Mychael Schnell, "Krebs on Biden's cybersecurity executive order: 'It's a really ambitious plan,'" *The Hill*, May 16, 2021, https://thehill.com/homenews/sunday-talk-shows/553772-krebs-on-bidens-cybersecurity-executive-order-its-a-really.
[59] Martijn Rasser, "The AI regulation wave is coming: Industry should ride it," *San Francisco Chronicle*, January 24, 2020, https://www.sfchronicle.com/opinion/openforum/article/The-AI-regulation-wave-is-coming-Industry-should-14999873.php.
[60] Philip J. Bezanson and Brittney E. Justice, "The Battle of the Bills Begins: Proposed Federal Data Privacy Legislation Aims to End Patchwork Problem But Increases Enforcement," *The National Law Review*, June 22, 2021, https://www.natlawreview.com/article/battle-bills-begins-proposed-federal-data-privacy-legislation-aims-to-end-patchwork.
[61] Sara Morrison, "This Democrat and ex-Microsoft employee has a federal privacy bill Republicans might actually like," *Vox Recode*, March 10, 2021, https://www.vox.com/recode/22301174/federal-privacy-bill-suzan-delbene.
[62] The White House, *National Security Strategy of the United States of America;* U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington: 2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf; U.S. Department of State and U.S. Agency for International Development, *Joint Strategic Plan FY 2018 – 2022* (Washington: 2018), https://www.state.gov/wp-content/uploads/2018/12/Joint-Strategic-Plan-FY-2018-2022.pdf; and U.S. Department of Commerce, *Helping the American Economy Grow* (Washington: 2020), https://www.commerce.gov/sites/default/files/2020-08/us_department_of_commerce_2018-2022_strategic_plan.pdf.
[63] Paul Scharre and Ainikki Riikonen, "The Defense Department Needs a Real Technology Strategy," *Defense One*, April 21, 2020, https://www.defenseone.com/ideas/2020/04/pentagon-needs-technology-strategy/164764/.
[64] The White House, *National Strategy for Critical and Emerging Technologies.*
[65] 50 U.S. Code § 4565, "Authority to review certain mergers, acquisitions, and takeovers," https://www.law.cornell.edu/uscode/text/50/4565#a_6.
[66] Rasser and Lamberth, "Taking the Helm."

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc