

MAY 2023

Optimizing Export Controls for Critical and Emerging Technologies

Semiconductors, Quantum Technology, AI, and Biotechnology

AUTHORS

William A. Reinsch

Emily Benson

Thibault Denamiel

Margot Putnam

A Report of the CSIS Scholl Chair in International Business

CSIS

CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

MAY 2023

Optimizing Export Controls for Critical and Emerging Technologies

Semiconductors, Quantum Technology, AI, and Biotechnology

AUTHORS

William A. Reinsch

Emily Benson

Thibault Denamiel

Margot Putnam

A Report of the CSIS Scholl Chair in International Business

CSIS | CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

© 2023 by the Center for Strategic and International Studies. All rights reserved.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Acknowledgments

This report is made possible through generous support from the Smith Richardson Foundation. The authors would also like to thank the numerous current and former government officials who agreed to be interviewed for this project, as well as private sector experts who provided their valuable input.

Contents

Introduction	1
National Security	5
Critical Technologies	12
Recommendations	32
Conclusion	35
About the Authors	37
Endnotes	39

Introduction

“The post-Cold War world has come to an end, and there is an intense competition underway to shape what comes next. And at the heart of that competition is technology. Technology will in many ways retool our economies. It will reform our militaries. It will reshape the lives of people across the planet. And so it’s profoundly a source of national strength.”

—Secretary of State Antony Blinken, October 2022¹

Today, the United States’ strategic technology framework faces new challenges. It must contend with multiple adversaries, including China, and it is being challenged in both the security and economic realms. The importance of exports to U.S. economic growth—particularly in the information and communications technology (ICT) sector—has also complicated trade and security policy. If controls are too loose, U.S. adversaries gain technology they can use against the United States; if they are too tight, the United States starves its high-tech companies of the revenue they need to develop next-generation products.

The United States is already rethinking its long-term strategy toward China, knowing there is an increasingly small window of opportunity to effectively counter Chinese strategic technology goals. With technological advancements such as faster machine learning, smarter supercomputing, and more durable autonomous weapons, speed of innovation and the ability to scale up production are important. Additionally, in the wake of the Russian invasion of Ukraine, the United States now needs to avoid actions that would push China and Russia closer together. Given the importance of maintaining U.S. technological superiority and responding to China’s ambitions, it is important to envision what a new strategic technology framework should look like.

The United States' post-World War II export control structure began in 1949 as a result of the Cold War. When the Export Control Act became law that year, its three main purposes were to protect the domestic economy, advance U.S. foreign policy interests, and control sensitive exports to enhance national security. The initial concept was simple: the United States and its allies in the North Atlantic Treaty Organization wanted to prevent the Soviet Union from acquiring critical dual-use technology that would benefit their military. To do so, they set up an export licensing system that required allied permission to export sensitive items. There was broad agreement on the goal and, in the early years, a surprising degree of operational consensus among the participating countries. Enforcement was straightforward. The items subject to control were, for the most part, physical—if not manufactured products, then intellectual property embodied in blueprints or schematics—and, if necessary, they could be stopped and inspected at the point of departure.

Over the past 30 years, following the collapse of the Soviet Union, the United States has transitioned to a control system based largely on end-user analysis rather than the broader approach used with the Soviet Union, though the latter has not disappeared entirely. To implement an approach based primarily on determining the *bona fides* of end users, the Department of Commerce's Bureau of Industry and Security (BIS) issues export licenses that include conditions that might, for example, only allow specified users engaging in specified activity to use the exported item. Further, in 2018, Congress replaced the long-expired Export Administration Act (EAA) with the Export Control Reform Act of 2018 (ECRA), which updated the law and made it more relevant to post-Cold War conditions.²

There are two policy elements that have proved difficult to reconcile over the past 30 years: ensuring military capability and national security versus maintaining an economic advantage. The law permits controls to protect the former but not the latter, although the latter clearly impinges on the former. In seeking to protect U.S. national security interests, the government is controlling technologies that would incrementally improve foreign adversaries' military capabilities, including their proliferation capabilities and missile delivery systems; however, those controls also have commercial implications, since the items in question often have both civil and military applications. That is particularly true with respect to semiconductors and emerging technologies—such as quantum technology and artificial intelligence (AI)—which are rapidly changing the nature of warfare and can help foreign adversaries enhance their military capabilities more quickly. That places a greater burden on regulators to make faster judgments as well as to take into account broader impacts on the civilian economy.

The United States needs to define more clearly what merits control and what does not. That means designing a policy that permits the growth of industries that do not aid foreign military capabilities, while controlling items that could harm U.S. national security. The government must take care to focus on goods and technology that are essential to U.S. national security—rather than imposing controls on items with minimum security significance, which are deemed vulnerable simply because they are made elsewhere. Autarky, or self-sufficiency, is an unrealistic goal in a globally integrated economy, and efforts to achieve it will only result in excessive controls that impose economic costs without enhancing security.

Control Considerations

Inadequate controls spur U.S. adversaries' technological progress and encourage proliferation. They also reduce the ability of the U.S. government to gain insights into the destination and end uses of domestically-produced technology. Failure to control dual-use technologies is particularly problematic given China's ongoing pursuit of its civil-military fusion strategy as well as its theft of intellectual property which had thus far enabled the West to maintain a technological edge. Revelations that Chinese-based Semiconductor Manufacturing International

Corporation (SMIC) has achieved the ability to produce 7-nanometer semiconductors highlight the challenge Western export control policymakers face in trying to restrain, let alone degrade, Chinese military capabilities.³ This makes it even more essential for the U.S. government to reassess its current export control regime and consider how it can more effectively tighten controls without stifling U.S. innovation for the next generation of cutting-edge technology.⁴ For example, in 2014 the BIS estimated that U.S. industry had lost between \$988 million and \$2 billion in sales due to export controls from 2009 to 2012.⁵ As the United States considers additional controls, the burden borne by the private sector is bound to expand.

Some elected officials have advocated a policy of far broader controls where nearly everything is deemed important. This policy would seek to isolate China by selling them nothing with any security implications, but it would also deny U.S. firms access to an important foreign market and the revenue that comes with it. While it is not necessary from a security point of view for the United States to produce t-shirts or eyeglasses, it is vital that the United States maintain the ability to produce semiconductors used in military aircraft and advanced weapons. Deciding what is, and is not, important is the essence of export control policy.

The real issues, of course, lie not at the ends of the spectrum but in the middle. An important distinction, which the United States has long maintained, is between the end product and the equipment used to manufacture it. In the case of semiconductors, the chip is the end product, while lithography and other advanced machines are the equipment used in semiconductor fabrication. The United States has never controlled the end product as tightly as the means of making it—adhering to the reverse of the old proverb “give someone a fish, you feed them for a day; teach them to fish, you feed them for a lifetime.” In other words, allowing strategic adversaries to access high-end manufacturing technologies allows them to advance several generations in technology development and ultimately surpass us.

Frederick the Great said, “He who defends everything defends nothing.” Unfortunately, there is no Goldilocks solution, no level of controls that is “just right.” If there were, the United States would already have developed and implemented it. Any solution carries risks and costs, and the best a government can do is sort these out and judge how to structure a policy that protects its domestic technology industries from avoidable revenue losses while also restricting the export of technologies that would enable a more rapid advancement of rival states’ technological capabilities. The most obvious implication of a poorly designed export control policy is that China enhances its strategic and military capabilities by acquiring technologies that help offset the advantage that the United States currently retains.

The Chinese government has been proactive in making structural changes to encourage critical technology research and development (R&D). Its leadership is overhauling the science and technology ministry’s organization by merging its education and research arm with practical applications.⁶ The changes also establish a “national technology transfer system” and expand the ministry’s role in formulating country-wide initiatives and leading policymaking efforts to give it more capacity to reduce Chinese reliance on U.S. advanced technology. The Chinese government is supporting its ambitions with the necessary capital. China accounts for half of the nearly \$30 billion in global public funding destined for quantum computing.⁷ It has allocated \$145 billion to the semiconductor industry through state capitals such as its Integrated Circuit Investment Fund, in addition to designating the sector as China’s top industrial initiative priority.⁸

China is also poised to double its investment in AI to almost \$27 billion by 2026, at which point it would account for 9 percent of global AI investments.⁹ Already last year, the People’s Liberation Army’s (PLA) investment in AI was on par with the Pentagon’s.¹⁰ Lastly, the Chinese Communist Party’s latest five-year plan shows that the country seeks to overtake U.S. biotechnology market share within the next decade, as the

country's biotech firms jumped from investing \$11.2 billion in 2020 to \$16.6 billion in 2021.¹¹ In short, China is changing its state infrastructure to ensure that the country continues to innovate in critical technology sectors while becoming less dependent on imports from other key players in advanced technology supply chains.

Using a trade lens to evaluate geostrategic competition and how best to maintain U.S. military superiority, this report assesses what the optimal export control policy should be, knowing that there are serious political constraints domestically as well as with key allies. The first in a series of three, this report seeks to reimagine the current approach to export controls in particularly sensitive areas of emerging technologies that pose the greatest challenges. It begins by comparing current control lists to see where they overlap, which in turn provides greater clarity on the current U.S. definition of national security critical sectors. After comparing control lists, the report evaluates quantum computing, AI, semiconductors, biotechnology, and intangible goods to determine whether additional controls are necessary—and, if so, what economic costs such controls would entail.

The second report will examine other parts of the Commerce Control List (CCL) beyond the technologies featured in this report, along with other elements of U.S. export control policy such as the Entity List, country listings, and catch-all controls. It will also evaluate foreign availability of inputs into these national security critical supply chains and assess the advantages and challenges of building an improved multilateral framework to constrain Chinese civil-military fusion. The third report will address multilateral export control structures—presenting the existing ones and discussing whether new ones are necessary—as well as the question of how to integrate foreign availability considerations into U.S. control policy. Overall, this project examines how to construct a new policy that is better able to meet the demands of the current geostrategic and technological environment, evaluating what is politically and economically feasible when rethinking the U.S. approach to export controls.

National Security

Definitions of what is critical to U.S. national security are moving away from strict nonproliferation goals and toward much more expansive definitions that blur the lines between national security and economic security.

Reimagining the U.S. approach to export controls depends first on determining which technologies are critical to U.S. national security, which hinges on how that term is defined. The United States' export control policy evolved out of the 1949 Export Control Act, which sought primarily to protect the U.S. domestic economy, advance U.S. foreign policy objectives, and control exports that affect U.S. national security. The Code of Federal Regulations defines national security as “those activities which are directly concerned with the foreign relations of the United States, or protection of the Nation from internal subversion, foreign aggression, or terrorism.”¹² This definition displays a vagueness appropriate to the breadth of changes that U.S. strategy has experienced in the post-WWII era.

In the second half of the twentieth century, U.S. national security was characterized primarily by a nonproliferation agenda—that is, preventing adversaries from gaining the technology necessary for nuclear weapons capabilities. This approach focused primarily on the Soviet Union. In multilateral institutions, such as the Coordinating Committee for Multilateral Export Controls (COCOM), national security policies were designed around these objectives, resulting in a fairly narrow approach to what the U.S. government and its allies considered critical to security. The United States began to recalibrate its understanding of national security after the collapse of the Soviet Union. The issues of terrorism and non-state actors, which peaked in the wake of the 9/11 attacks, dramatized the new threats, although it had a minimal impact on control lists aside from moderate expansions into the use of controls for foreign policy and human rights objectives.

Other considerations, such as economic and diplomatic tools, were integrated into the security picture. While the initial reforms were modest, there has been a more recent push to approach national security from a wider

perspective. This realization has led to the Biden administration's National Security Strategy, which connects domestic economic prosperity and national security interests by making the case that new investments "will enable the United States to anchor an allied techno-industrial base that will safeguard our shared security, prosperity and values." Per the National Security Strategy, "this means working with allies and partners to harness and scale new technologies, and promote the foundational technologies of the 21st century, especially microelectronics, advanced computing and quantum technologies, artificial intelligence, biotechnology and biomanufacturing, advanced telecommunications, and clean energy technologies." The National Security Strategy also makes clear that "the Administration is ready to emphasize a modern industrial and innovation strategy to achieve its foreign policy objectives."¹³ The infusion of techno-industrial concerns into the administration's most foundational national security document underscores a significant broadening of what it considers critical to national security.

This shift in thinking is also captured in several speeches by top administration officials. In September 2022, National Security Advisor Jake Sullivan delivered remarks that cited "three families of technologies" that "will be of particular importance over the coming decade." The three technology categories are: 1) Computing-related technologies such as quantum information systems, AI, and microelectronics; 2) Biotechnologies and biomanufacturing; 3) Clean energy technology Sullivan then noted that the "first pillar" of the Biden administration's technology strategy is "recharging the engine of American technological dynamism and innovation, especially in these foundational sectors." He described U.S. leadership in each sector as a "national security imperative."¹⁴

Under Secretary for Industry and Security Alan Estevez has clarified that BIS looks "to see what's available in the world and whether it makes sense [to apply controls]. If I stop a US firm from shipping something that is ubiquitous in the world, I'm really not doing anything. . . . can feel good about ourselves [sic], but we're not stopping the national security threat."¹⁵ To that end, BIS may relax rules when it determines that controlling a certain technology's export is no longer critical to national security and would benefit U.S. producers. For instance, the agency recently eased its licensing policy on certain satellite exports: components going to members of the Missile Technology Control Regime.¹⁶ Countries participating in the regime will be reviewed on a case-by-case basis instead of a presumption of denial, helping satellite manufacturers gain access to foreign markets.

The infusion of techno-industrial concerns into the administration's most foundational national security document underscores a significant broadening of what it considers critical to national security.

While there is some convergence across export control and other technology control lists, they differ significantly because each list serves a distinct purpose.

A factor that complicates defining national security—and which therefore complicates the design and implementation of export controls—is that existing lists do not always agree on what is important. These divergences give U.S. agencies greater authority to promulgate controls over goods that they consider relevant. The multiplicity of lists thus provides greater agility to the U.S. government, but it can also complicate the ability of the private sector to discern what the government regards as critical to national security. The chart

below provides a snapshot of the difficulties of using a list-based system to delineate what the U.S. government regards as national security critical.

Control Category	Control Lists					
	Commerce Control List (Commerce Department)	Wassenaar Arrangement (Commerce Department and State Department)	Committee on Foreign Investment in the United States Executive Order (White House and Treasury Department)	Outbound Investment Executive Order (likely forthcoming) (White House and Treasury Department)	Commerce Review of Controls for Certain Emerging Technologies ¹⁷ (Commerce Department)	Critical and Emerging echnologies (Office of Science and Technology Policy)
Nuclear Materials, Facilities and Equipment (and miscellaneous items)	✓	✓	✗	✗	✗	✗
Materials, Chemicals, Microorganisms, and Toxins	✓	✗	✗	✗	✗	✗
Materials Processing	✓	✓	✗	✗	✗	✗
Electronics	✓	✓	✗	✗	✗	✗
Computers	✓	✓	✗	✗	✗	✗
Telecommunications	✓	✓	✗	✗	✗	✗
Information Security	✓	✓	✗	✗	✗	✗
Sensors and Lasers	✓	✓	✗	?	✗	✗
Navigation and Avionics	✓	✓	✗	✗	✓	✗
Marine	✓	✓	✗	✗	✗	✗
Aerospace and Propulsion	✓	✓	✗	✗	✗	✗
Special Materials and Related Equipment	✗	✓	✗	?	✓	✗
Advanced Computing	✓	✗	✗	?	✓	✓
Advanced Engineering Materials	✓	✗	✗	✗	✗	✓
Advanced Gas Turbine Engine Technologies	✗	✗	✗	✗	✗	✓
Advanced Manufacturing	✗	✗	✗	?	✓	✓
Advanced and Networked Sensing and Signature Management	✓	✗	✗	?	✓	✓
Advanced Nuclear Energy Technologies	✓	✗	✗	POSSIBLE	✗	✓
Artificial Intelligence	✗	✗	✗	LIKELY	✓	✓

Autonomous Systems and Robotics	X	X	X	POSSIBLE	✓	✓
Biotechnologies	✓	X	✓	POSSIBLE	✓	✓
Communication and Networking Technologies	✓	X	X	X	X	✓
Directed Energy	X	X	X	X	X	✓
Financial Technologies	X	X	X	X	X	✓
Human-Machine Interfaces	X	X	X	POSSIBLE	✓	✓
Hypersonics	X	X	X	X	✓	✓
Renewable Energy Generation and Storage	X	X	X	X	X	✓
Microelectronics	✓	X	✓	LIKELY	✓	X
Quantum Computing	✓	X	✓	LIKELY	✓	X
Advanced Clean Energy	X	X	✓	X	X	X
Climate Adaptation Technology	X	X	✓	X	X	X
Critical Minerals	X	X	✓	X	X	X
Elements of the Agriculture Industrial Base	X	X	✓	X	X	X
Data Analytics Technology	X	X	✓	?	✓	X
Logistics Technology	X	X	✓	X	✓	X

Note: This chart is a simplified description of the lists. It does not include subcategories, for example, and it is intended as a helpful guide rather than a comprehensive blueprint.

Source: CSIS combination and retooling of existing lists from multiple government sources, such as the Department of Commerce, Department of Treasury, Department of State, and the White House.

The lists are tailored to their respective individual agency’s purposes, but their overlap provides insight into the greater control capabilities of the U.S. government. The BIS list closely resembles the Wassenaar Arrangement’s dual-use list, while the Committee on Foreign Investment in the United States (CFIUS) executive order list and the White House Critical and Emerging Technologies List highlight key priority areas of the administration. A single list could lead to more administrative consistency and more certainty for exporters, but a single list would depend on a single definition of national security—and it is not clear that the United States had one in the past, much less now. Because lists are designed by different agencies and for different purposes, it makes sense that they do not completely overlap. However, as the above chart highlights, it is nearly impossible to develop a clean and definitive definition of national security based solely on a comparison of lists. Nevertheless, assessing where they do overlap can shed light on definitions of national security and provide guidelines, although not a blueprint, for thinking about retooling existing lists. Each of the lists is presented in more detail below.

Wassenaar Arrangement

The Wassenaar Arrangement is the world’s largest multilateral export control regime, consisting of a diverse set of 42 countries.¹⁸ The Wassenaar dual-use list includes the following categories: 1) Special Materials and Related

Equipment; 2) Materials Processing; 3) Electronics; 4) Computers; 5.1) Telecommunications; 5.2) Information Security; 6) Sensors and Lasers; 7) Navigation and Avionics; 8) Marine; and 9) Aerospace and Propulsion. In 2019, the Wassenaar Arrangement produced a series of significant updates on new controls.¹⁹ These included controls on emerging technologies such as cyberwarfare software, suborbital aerospace vehicles, lithography equipment and technology, hybrid machine tools, and a host of other technologies such as digital investigative tools and forensic systems that can detect digital crime. During that process, member states also significantly relaxed some controls, for example on commercial components with embedded cryptography.

Although many countries, such as the Netherlands, maintain lists that are legally tied to the Wassenaar control list, implementing them remains the prerogative of participating states, which they do through domestic statutes. G7 countries have traditionally opted to align their lists with the Wassenaar Arrangement list, in addition to other export control mechanisms, and the United States is no exception. The official organization of the CCL shows the close alignment of the BIS classifications with the Wassenaar Arrangement dual-use list.

Commerce Control List

The existence of control lists helps define what the United States and its international partners deem national security critical. The CCL consists of roughly 3,100 items that adhere to the Export Administration Regulations (EAR), which govern the export of physical commodities, software, and technology.²⁰ There are 10 main categories of the CCL: 0) Nuclear materials, Facilities, and Equipment (and Miscellaneous Items); 1) Materials, Chemicals, Microorganisms, and Toxins; 2) Materials Processing; 3) Electronics; 4) Computers; 5) Part 1 - Telecommunications and Part 2 - Information Security; 6) Sensors and Lasers; 7) Navigation and Avionics; 8) Marine; and 9) Aerospace and Propulsion. If an item falls under the Department of Commerce's jurisdiction and is not listed on the CCL, it is designated as EAR99. EAR99 items generally consist of low-technology consumer goods and do not require a license in most situations. However, if a business plans to export an EAR999 item to an embargoed country, to an end user of concern, or in support of a prohibited end use, that business may be required to obtain a license.

The CCL includes items from the following lists:

1. Items on the Wassenaar Arrangement dual-use list;²¹
2. Nuclear-related dual use commodities (compiled in the Nuclear Suppliers Group's Nuclear Referral List);²²
3. Dual-use items on the Missile Technology Control Regime List;²³
4. Chemical Weapon (CW) Precursors, biological organisms and toxins, and Chemical and Biological Weapon (CBW) related equipment on the Australia Group lists;²⁴
5. Items controlled in furtherance of U.S. foreign policy and other objectives, including anti-terrorism, crime control, Firearms Convention, regional stability, UN sanctions, and short supply reasons; and
6. Unlisted items when destined for specified end uses or end users (catch-all controls).

In short, the CCL includes items on the Wassenaar dual-use list but goes beyond it. The United States' authority to promulgate unilateral controls arises from the ECRA, which differs significantly from the authorities of key allies. ECRA also mandates that BIS determines a list of "emerging" and "foundational" technologies for control, referred to as Section 1758 Controls. The label of "emerging" technology was intended to target more nascent sectors, such as AI and quantum computing, while "foundational" technologies included hardware such as microelectronics. To date, however, BIS has not produced a

definitive list, although it has regularly added items under the “emerging” category that have then been adopted by the Wassenaar Arrangement.²⁵

In November 2018, the Department of Commerce published an advanced notice of proposed rulemaking, entitled “Review of Control for Certain Emerging Technologies.”²⁶ There are 14 categories in this list, all of which include several subcategories.²⁷ While the technological categories are relatively broad, the list is considered to have set the precedent for several of the controls that followed shortly thereafter. Last year, BIS published the “Implementation of Certain 2021 Wassenaar Arrangement Decisions on Four Section 1758 Technologies.” This updated the CCL for the following four items: “two substrates of ultra-wide bandgap semiconductors (Gallium Oxide (Ga₂O₃) and diamond), Electronic Computer Aided Design (ECAD) software specially designed for the development of integrated circuits with any Gate-All-Around Field-Effect Transistors (GAAFET) structure, and pressure gain combustion (PGC) technology for the production and development of gas turbine engine components or systems.”²⁸

Critical and Emerging Technologies

A list that does not directly deal with export controls but which sheds light on U.S. definitions of national security is the Critical and Emerging Technologies (CET) list.²⁹ This list, published in February 2022, contains a different set of technologies than those outlined in other similar government documents. The list includes 18 primary categories and their subsets. The CET update was drafted by the Fast Track Action Subcommittee on Critical and Emerging Technologies of the National Science and Technology Council, which was established in 2020, when the White House published the initial report on CETs.³⁰ It is unclear whether the subcommittee will update the list again in two years. Furthermore, this list does not have a regulatory function.³¹ According to a report by the Fast Track Action Subcommittee, CETs are a “subset of advanced technologies that are potentially significant to U.S. national security.”³²

CFIUS Guidance

On September 15, 2022, President Biden signed an executive order, “Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States,” which directs the Treasury Department’s Committee on Foreign Investment in the United States³³ (CFIUS) to consider evolving risks and security factors. This executive order included a list of new sectors and technologies to consider, not only for investments within the defense industry but also outside of defense. According to the official presidential document:

The Committee shall consider, as appropriate, the covered transaction’s effect on supply chain resilience and security, both within and outside of the defense industrial base, in manufacturing capabilities, services, critical mineral resources, or technologies that are fundamental to national security, including: microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy (such as battery storage and hydrogen), climate adaptation technologies, critical materials (such as lithium and rare earth elements), elements of the agriculture industrial base that have implications for food security, and any other sectors identified in section 3(b) or section 4(a) of Executive Order 14017³⁴ of February 24, 2021 (America’s Supply Chains).³⁵

This list underscores several areas that the administration deems critical to national security, ranging from quantum computing and biotechnology to AI.

Outbound Investment Reviews

In addition to export controls, the administration is currently drafting an executive order that would establish a new mechanism to screen and potentially ban certain outbound financial transactions.³⁶ This is based on the belief that the United States controls inbound capital flows via CFIUS and outbound items via export controls, leaving a gap in national security by failing to cover outbound investments. The private sector and several U.S. government agencies have expressed concern about the implementation of a tool that could potentially chill financial exchanges in emerging sectors, such as quantum computing, and have recommended significantly paring back proposals so that this new control would target primarily knowledge transfers or establishes a high threshold for review to only a select set of entities. The executive order has been significantly scaled back over time but will likely cover quantum technology, AI, and microelectronics.

It has historically been the job of the government to identify national security priorities. The private sector does not have the authority to make those judgments and, in any event, lacks the information to do so. It is thus incumbent upon the government to determine what constitutes a national security threat and to weigh the severity of the threat against the economic costs of pursuing controls. Based on the above lists, as well as on public statements from administration officials, it can be reasonably assumed that priority areas of the administration include the following four sectors: quantum technology, AI, semiconductors, and biotechnology. The below section evaluates the benefits and drawbacks of applying additional export controls to these sectors—along with a new category of intangible items, which this report recommends be added.

Critical Technologies

As economic security is increasingly conflated with national security, the U.S. government must clearly define its strategic objectives to avoid the appearance that its policies are protectionism in disguise. At the same time, controlling emerging and foundational technologies can deprive firms of export-based revenue, potentially imperiling long-term security goals. It is therefore vital that additional controls in sectors such as AI and quantum technologies are surgical and narrowly targeted.

Determining criticality depends on the division of technology into more specific thematic areas. This includes a taxonomy that separates technologies into distinct categories based on their specific applications. For instance, it is important to differentiate technologies with 1) warfighting capabilities with direct applications in ground, sea, air, and electronic warfare; 2) ICT applications that allow allied parties to communicate with each other, the importance of which was demonstrated during the Balkan conflict in the 1990s and which continues to be important in today's threat environment; and 3) intelligence capabilities that allow for the collection of data to wage war, such as the location targeting data used in High Mobility Artillery Rocket System (HIMARS) strikes in Ukraine.

The hardware-software distinction is important, but intangible items such as software can also be critical to U.S. national security interests. The latter is significantly more difficult to control because it is not available for physical inspection at docks and airports and can be exported digitally. This problem arises across myriad technologies, ranging from quantum computing to biotechnology and AI. While controlling hardware is in some ways simpler, it is also incomplete since many emerging dual-use technologies require data as an input. As demonstrated below, reimagining the export control regime requires a significant retooling of how the United States governs data exports—but also a targeted reassessment of how the government handles physical inputs and knowledge transfers, or “deemed exports.” As developing national capabilities in critical technologies depends on a highly intertwined and often international ecosystem of research collaboration,

U.S. leaders in critical technology rely on research made possible through knowledge transfers from U.S. persons to foreign nationals, or “deemed exports,” and vice versa.

Deemed Exports

Regulated information or technology released to a foreign national in the United States is deemed to be an export to the home country of that national or entity.

This does not apply to permanent residents or protected individuals.

According to the Export Administration Regulations (EAR), an export of technology or source code is “deemed” to have occurred when:

- it is available to foreign nationals for visual inspection
- technology is exchanged orally; and
- technology is made available by practice or application under the guidance of persons with knowledge of the technology.

Controlled commodities, such as critical technologies, therefore have a license requirement to authorize their use by foreign individuals, even if this use takes place within the United States. For instance, commodities may be considered exported during training involving controlled equipment or when controlled data is disseminated by email or in conversations.

Source: “Deemed Exports and Fundamental Research for Biological Items,” Bureau of Industry and Security, Department Commerce, [https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear/14-policy-guidance/deemed-exports#:~:text=What%20is%20a%20Deemed%20Export,permanent%20residents%20or%20protected%20individuals.](https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear/14-policy-guidance/deemed-exports#:~:text=What%20is%20a%20Deemed%20Export,permanent%20residents%20or%20protected%20individuals.;); and “Deemed Exports,” Research and Department, University of Maryland, Baltimore, <https://www.umaryland.edu/ord/export-compliance/procedures/deemed-exports/>.

Control of deemed exports is an issue that applies to each of the technologies under discussion in this report; indeed, they are an important element of the United States’s recent October 7, 2022, rules on semiconductor controls, which will be discussed in detail in a later section. While the requirement to license a deemed export has been in existence for years, the increased complexity and sophistication of technologies has contributed to more international collaboration on their development, which has made the deemed export issue more important. The biggest problem with the concept, however, has not been with respect to licensing but with respect to enforcement: it is inherently difficult for enforcement authorities to discover when technical discussions with foreign parties go beyond the limitations of a deemed export license.

Quantum Technology

Quantum-enabling technologies have come to the forefront of national security considerations. In February 2022, the White House’s Critical and Emerging Technologies List Update divided quantum into the following five categories: 1) quantum computing; 2) quantum computing materials, isotopes, and fabrication techniques for quantum devices; 3) post-quantum cryptography; 4) quantum sensing; and 5) quantum networking.³⁷

In May 2022, the Biden administration released its “National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems.”³⁸ This

document outlines the Biden administration’s quantum computing strategy. Per the document, promoting U.S. leadership in quantum technology and mitigating certain associated risks will also rely on government protections of quantum: “Protection mechanisms will vary, but may include counterintelligence measures, well-targeted export controls, and campaigns to educate industry and academia on the threat of cybercrime and IP theft.”³⁹ In November 2022, Undersecretary for Industry and Security Alan Estevez alluded to potential restrictions on quantum technology exports, saying about controls on quantum computer equipment: “So will we end up doing something in those areas? . . . If I was a betting person, I would put down money on that.”⁴⁰

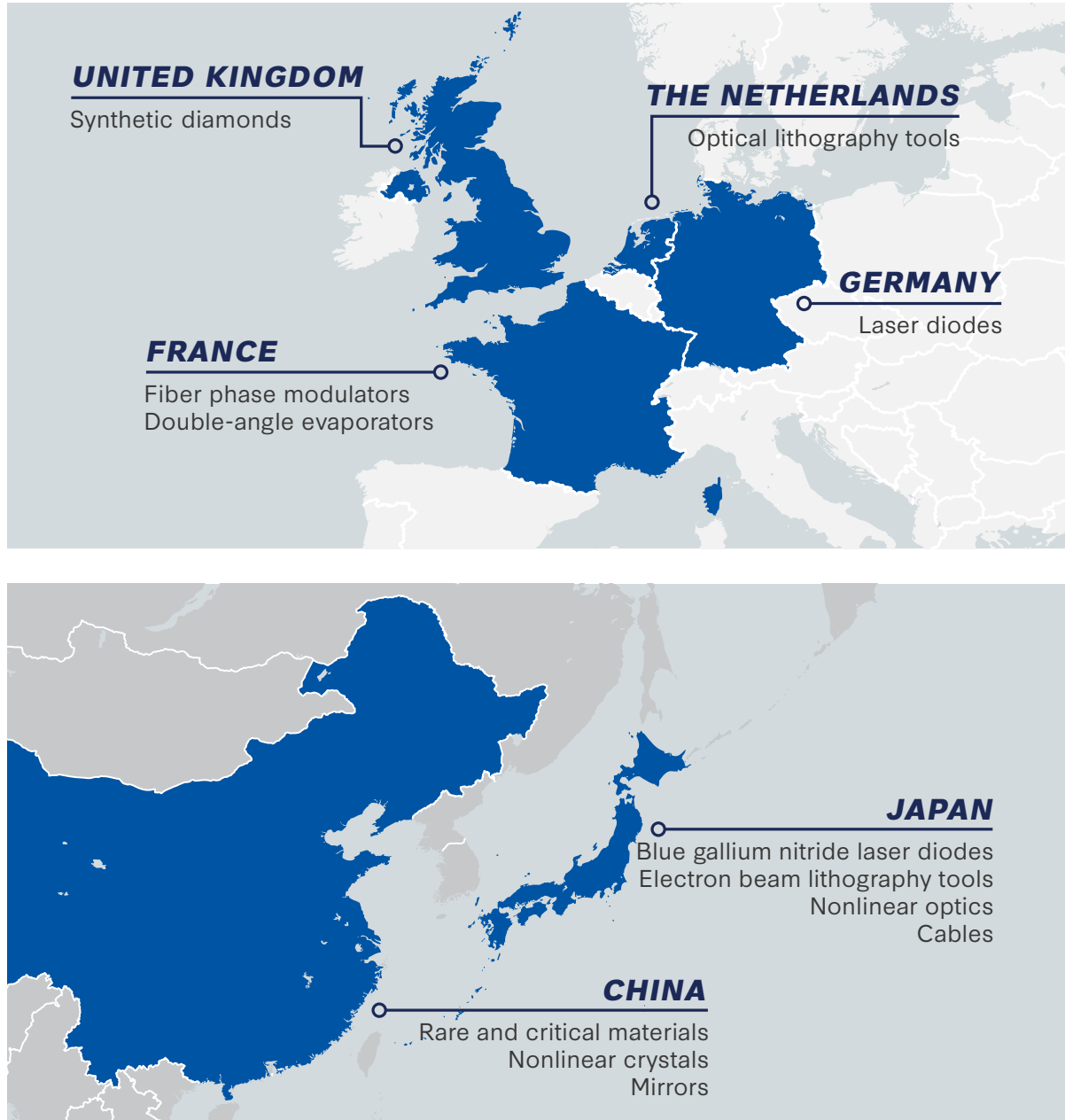
A Congressional Research Service study on quantum computing highlights the Defense Science Board’s conclusion that there are three applications of quantum technology with significant implications for national defense tools: quantum sensing, quantum computers, and quantum communications. According to the Congressional Research Service, quantum sensing is currently “poised for mission use” as it provides a number of enhanced capabilities such as alternative positioning, navigation, and timing options that could allow militaries to continue to operate at full performance in GPS-degraded or GPS-denied environments.⁴¹ It also plays an intelligence, surveillance, and reconnaissance (ISR) role.

Quantum computing, the second set of quantum technologies highlighted by the CRS, is still emerging. However, at capacity, it could facilitate breakthroughs in machine learning, which would improve recognition and machine-based target identification capabilities.⁴² In addition, quantum computers have the potential to break the encryption of classified or controlled unclassified information. However, only drastic advances would allow quantum computers to break current encryption methods.⁴³ A quantum computer would need to process 20 million qubits to break current encryption methods, and the most advanced quantum computers today usually have less than 433 qubits.⁴⁴ These practical applications can only be achieved after improvements in error rates and development of new algorithms, software tools, and hardware. The third set of technologies, quantum communications, also remains nascent but could lead to the secure networking of quantum military systems. For instance, quantum key distribution deploys communications that, in theory, cannot be intercepted.

The quantum industry overall remains relatively small. Recent estimates show that the current quantum technology market reached \$761 million in 2022, although it is expected to reach \$1.09 billion in 2025, at a compounded growth rate of 13 percent annually. The same analysis shows that the quantum cryptography market remains quite small, totaling \$106 million in 2022.⁴⁵ The small current value of the quantum market means that controls on the industry are particularly risky since they could stifle an industry on the cusp of growing. In addition, estimates over the size of the market vary widely. For instance, the World Economic Forum claims that government and business investment in quantum computing alone is reaching \$35.5 billion, contrasting Yole Group’s more conservative estimate that the quantum market will reach \$4 billion by 2035.⁴⁶ The fact that estimates about the size of the industry present such large differences illustrates that quantum technologies may be too nascent a field for accurate economic projections, let alone export controls. On the other hand, a sector is much easier to control when it is small, and controls are more effective when applied early to prevent leakage and minimize political pushback.

Although there is not a consensus view on whether China or the United States currently leads in the quantum race, recent RAND Corporation analysis finds that the United States leads the world in most, but not all, quantum technologies.⁴⁷ The United States has provided stable and globally competitive scientific research output in quantum information science (QIS). Aside from the U.S. government’s significant funding of open QIS research, the private sector drives U.S. quantum technology deployment. As a result, the United States is the global leader in quantum computing and sensing, but not in quantum communications. China’s quantum

Sources of Country-Specific Quantum Technology Inputs



Source: CSIS graphical representation of data from Edward Parker et al., *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology* (Santa Monica, CA: RAND Corporation, 2022), https://www.rand.org/pubs/research_reports/RRA869-1.html; and “Quantum Computing and Communications: Status and Prospects, U.S. Government Accountability Office, October 20, 2021, <https://www.gao.gov/products/gao-22-104422>.”

technology capabilities are rapidly developing, and it also presents high research output in every application domain. China has committed to spending \$15 billion on quantum research—twice as much as the United States and the European Union combined.⁴⁸ The government-funded laboratories’ quantum technology R&D has wielded quick technical progress, such as Baidu’s new quantum computer.⁴⁹

The United States has begun to mitigate its investment gap with China by teaming up with key allies leading global QIS innovation on research and development efforts. Last February, the United States and the Netherlands announced a new joint endeavor in quantum information sciences and technologies R&D, representing the fourth partnership of this kind undertaken by the Biden administration. The White House is concerned about the significant risks that quantum computing advances in countries of concern pose to U.S. economic and national security. Chief among these concerns is the cryptanalytically relevant quantum computer (CRQC), which could eventually break the public-key cryptography used on digital systems across the world.⁵⁰ Breaking public-key cryptography could usher in a period of total transparency on the internet. For example, bank account statements, health records, and state secrets would be available publicly online. Quantum researchers in China claimed to have designed an algorithm that could break public-key encryption years ahead of schedule, and while the findings were quickly debunked, attention surrounding the initial announcement shows the underlying tension concerning the potential disruptions that quantum computing could have on our current cybersecurity apparatus.⁵¹

A 2021 Government Accountability Office report about the United States' capabilities vis-à-vis quantum computing and communications established how one of the largest obstacles to quantum technology development is a lack of suitable and reliable components and equipment, as they all depend on specific countries and producers.⁵² Examples include specialized lasers and high-quality optical fibers (which are produced in Denmark and Germany), cryogenic components (Finland), specialized synthetic diamonds (the United Kingdom), and rare and critical materials (China).⁵³ As a result, the quantum supply chain includes potential single points of failure located in other countries. These have the potential to disrupt development if certain supporting technologies are unavailable. However, the existence of multiple chokepoints in different jurisdictions highlights the fundamentally globalized nature of the quantum technology supply chain.

There is ongoing debate as to how to frame the performance of quantum computing for control purposes. The industry focuses on qubits, while others have suggested that other thresholds have value, such as error correction software. James Sanders, the principal analyst for quantum computing at CCS Insight, suggested that physical components of quantum computers—such as helium dilution refrigerators, cryogenic ion trap packages, and magneto-optical traps—would be a better basis for controls.⁵⁴ Another key control obstacle is that most of the current software behind quantum is open source. However, some aspects of quantum computing software are proprietary and therefore easier to control.

Despite these challenges, the U.S. government has initiated formal steps to regulate quantum technology exports. In the spring of 2021, BIS added Export Control Classification Number (ECCN) 4A006 to “control quantum computers and related electronic assemblies and components including specified qubit devices and circuits and quantum control components and measurement devices.” It further explained that “quantum computing is expected to have a significant impact in many commercial and military areas, and early implementation of this proposal is warranted.”⁵⁵ In response, companies and researchers have urged caution regarding the costs of controlling the early-stage quantum sector.⁵⁶ In comments to the Trump administration regarding definitions of emerging and foundational technologies, IBM outlined the following recommendation:

We believe any new controls should be narrowly focused, because broad application of new controls could significantly harm U.S. industries and put American businesses at a competitive disadvantage while failing to actually restrict access by parties of concern. For example, Artificial Intelligence (AI) generally is a poor candidate for control as an “emerging technology,” but specific applications of AI using certain data sets could prove to be an effective chokepoint.

IBM, one of the leading quantum firms in the United States, also expressed similar reservations about the application of export controls to the nascent field of quantum computing. IBM argues that “Quantum Computing (QC) is still a nascent technology with its roots in fundamental research. . . . QC continues to require a large ecosystem to derive not only the correct technology to apply but also the relevant commercial opportunities to explore. Any new controls in this space should adopt a ‘do no harm’ principle that promotes innovation.”⁵⁷ IBM also recommended in consultation rounds with U.S. officials that “regulations cover potentially problematic uses of quantum computing rather than limiting the technology based simply on processing power.”⁵⁸

When it comes to export controls, Washington should be wary of falling into a “metrics” trap when attempting to identify specific thresholds for controls. The number of qubits that a quantum computer can process, for instance, does not provide an adequate baseline. First, networked supercomputers could circumvent the threshold by combining the processing power of multiple computers by enabling parallel and synchronized computing cycles, each below a given designated qubit control threshold. Second, quantum computers with enough processing power to break encryption (about 20 million qubits to break a 2048-bit RSA in eight hours⁵⁹) are still far from being developed anywhere.⁶⁰ Officials from the National Institute of Standards and Technology are currently working to develop quantum-resistant algorithms that could withstand hacking attempts from such computers by 2024 or 2025, aiming to roll them out throughout the following decade.⁶¹ Looking at specific physical components necessary to power quantum computers, such as helium dilution refrigerators, provides more concrete control solutions. However, manufacturing many of these components is already within the grasp of Chinese industry. Identifying what countries of concern—especially China—can already accomplish without the United States and allies is essential. Again, in the quantum computing realm, China has already delivered a commercial 24-qubit quantum computer based on superconducting technology.⁶² When it comes to components, China also manufactures its own digital-to-analog converters, optics and raw materials, and nonlinear crystals, to name a few.⁶³

Another challenge for quantum controls is the multiple ways quantum computers can be built, as the different methods require their own inputs. A quantum computer based on nuclear magnetic resonance (which uses a spectrometer to measure and wield the magnetic field in the atomic nuclei in molecules) that will require cooling a magnet using liquid nitrogen and helium.⁶⁴ On the other hand, ion-trapped quantum computers are based on steel vacuum chambers containing an integrated circuit with electrodes chilled to a very low temperature. For this modality, the qubits are the ions trapped in the steel chamber by electric fields and manipulated by high-quality lasers.⁶⁵ A quantum computer can be also based on a superconducting chip, in which two lithium superconductors create a qubit functioning as an atom with two quantum energy levels.⁶⁶ As microwave pulses are sent to a resonator coupled to the qubit, the duration of these pulses creates a state of superposition. To eliminate any resistance, that system requires materials to be cooled below a certain temperature, requiring hardware like helium dilution refrigerators.⁶⁷

Developers are currently pursuing at least 12 different kinds of quantum modalities.⁶⁸ The impact of blocking China’s access to one specific type of hardware (i.e., of targeting one of the modalities) would be ineffective in curbing China’s capabilities in the long run, as they could just utilize another method of building a quantum computer. Additionally, the application of controls on one modality could artificially push investment towards another modality that may not otherwise have prevailed, thus hurting U.S. technological advancement. Such artificial creation of winners and losers should be avoided. In other words, for controls to be effective in this sector, they would have to be extraterritorial and extensive, potentially hobbling an industry where foreign availability is already accelerating and in which the United States does not maintain a significant lead—if any.

The absence of horizontal integration also makes current quantum technology production much more expensive than it will be later on. As quantum technology companies rely on a small number of suppliers for a wide array of inputs, costs are substantially higher for the quantum industry now than they likely will be within the next decade, making the application of additional controls even more burdensome for the private sector. To the extent that there exists a consensus within the quantum technology sector, it is that the application of controls would primarily restrain innovation, and now is not the appropriate time for new controls.

Instead, the U.S. government should focus on ramping up domestic quantum technology capacity. The race for talent is one of the first areas of focus for policymakers. An important step towards boosting a nascent industry is to cultivate its talent pool, primarily by loosening immigration restrictions in the sector. For example, following the Russian invasion of Ukraine, Russian quantum scientists sought refuge in Western European countries but were turned away at the border due to fear of violating sanctions and export controls. This likely unintended consequence of export controls and sanctions directly contravenes long-term strategic objectives and highlights the need to build in flexibility where possible, along with increasing educational support for high-tech sectors.

To the extent that there exists a consensus within the quantum technology sector, it is that the application of controls would primarily restrain innovation, and now is not the appropriate time for new controls.

Semiconductors

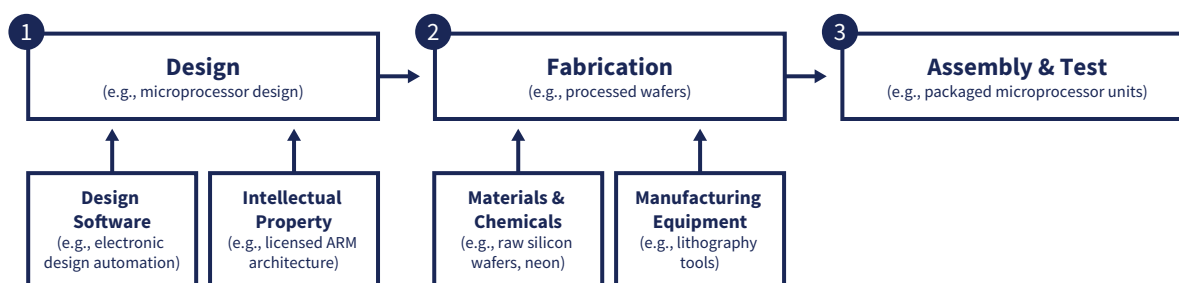
Semiconductors are one of the most critical national security technologies as well as a key part of the civilian economy—the ultimate dual-use good. Semiconductors function as “the brains of modern electronics” and serve as high-tech inputs in a wide range of sectors, such as healthcare, clean technology, and advanced computing.⁶⁹ They are used in most advanced weapons procured by the Pentagon and are vital components of a range of technologies, including hypersonic weapons, AI, and advanced telecom applications. U.S. exports of semiconductors constitute the largest share of all U.S. electronic product exports.⁷⁰

Semiconductor global value chains (GVCs) are highly complex and thus replete with potential chokepoints. Their nature highlights the need for the United States to promulgate export controls in partnership with key allies, since unilateral controls risk “damming half the river” if foreign producers can step in to supply market demand.

Broadly speaking, there are six different regions where semiconductor supply chains are concentrated: the United States, China, Taiwan, South Korea, Japan, and Europe.⁷¹ Key supply chain chokepoints include electronic design automation (EDA) and core IP; manufacturing equipment; wafer fabrication; and assembly, testing, and packaging. The United States largely leads in R&D-intensive activities, such as EDA and IP, manufacturing equipment, and chip design.⁷² Japan and Europe are also key players in these areas. Assembly, testing, and packaging (ATP) capabilities are far more concentrated in China and Taiwan.⁷³

Concentration in wafer fabrication capacity, or the process of turning chips into completed circuits, also varies by region and depends on the type of chip. While South Korea is the primary wafer fabricator for memory chips (accounting for 33 percent of the global market⁷⁴), fabrication of the most advanced chips, sub-10 nanometer chips, is heavily concentrated in Taiwan, which boasts 92 percent of the fabrication capacity.⁷⁵ Concentration is more dispersed with other advanced nodes, such as 10- to 22-nanometer chip fabrication, with the United States maintaining 43 percent of the market versus Taiwan’s 28 percent.⁷⁶ Taiwan additionally maintains a 47 percent and 31 percent market share, respectively, of fabrication capacity for more mature 28- to 45-nanometer chips and greater than 45-nanometer chips, respectively. The United States and Taiwan thus represent the world’s strongest chokepoints over advanced chips. As the demand for increasingly advanced technology grows, the geopolitical might of the United States and Taiwan will commensurately grow if the two can maintain their dominance in advanced chip design and production.

Simplified Depiction of the Semiconductor Value Chain



Source: Gregory Allen and Emily Benson, “Clues to the U.S.-Dutch-Japanese Semiconductor Export Control Deal Are Hiding In Plain Sight,” CSIS, CSIS White Paper, March 1, 2023, <https://www.csis.org/analysis/clues-us-dutch-japanese-semiconductor-export-controls-deal-are-hiding-plain-sight>.

The globalization of semiconductor manufacturing has been the key component of China’s civil-military fusion doctrine.⁷⁷ For instance, chips that are specifically designed for AI applications can be exponentially more efficient than general-purpose chips, such as central processing units (CPUS), and are more cost-effective. The Chinese military AI systems use U.S. chips, meaning that export controls on advanced semiconductors could degrade current Chinese AI capabilities. More than 95 percent of chips used in China are designed by U.S. firms.

National Security Advisor Jake Sullivan announced the United States would be shifting its export control approach toward China. Instead of trying to maintain an advantage, the United States would now try to “maintain as large of a lead as possible” and that instead of using them as preventative measures, U.S. export controls would be “implemented in a way that is robust, durable, and comprehensive.”⁷⁸ Rather than a moving target that allowed China to obtain older generation technology as U.S. technology advanced, thus keeping them behind while the United States maintained its leadership, the new controls aim to establish a static ceiling above which Chinese semiconductor capabilities would not be able to develop.

On October 7, 2022, the United States implemented a series of new unilateral controls on advanced AI chips to China, in what CSIS has described as a “two-pronged approach” to controlling China’s access to semiconductors.⁷⁹ These controls included new licensing requirements for deemed exports and also levied new controls on hardware and EDA software exported to China.⁸⁰ In addition, the controls add license requirements for chips destined for use in supercomputers, the manufacture of semiconductors, and manufacturing equipment. They also add requirements for items destined for fabs in China that manufacture logic chips with non-planar transistor architectures or with a “‘production’ technology node of

16/14 nanometers (‘nm’) or below; DRAM memory chips of 18nm half-pitch or less; or NAND flash memory chips with 128 layers or more.”⁸¹

Most semiconductor controls can be found under ECCN 3A001 of the CCL in the EAR. The October 7 export controls imposed greater restrictions on chip exports to China. ECCNs 3A090 and 4A090 have had the biggest impact on U.S. companies, namely Lam Research and KLA. ECCN 3A090 includes various processing units, logic devices, and application-specific ICs, while ECCN 4A090 comprises computers, electronic assemblies, and components containing ICs that exceed the limits outlined by 3A090.⁸² The rules themselves are both hardware- and parameter-driven, and software companies have not been as significantly hit by the regulations. Because there are not many companies in China producing supercomputing technologies, several companies have asked BIS for a list of companies with whom they are still able to contract, which BIS should supply.

News broke during the summer of 2022 that China’s SMIC had produced 7-nanometer chips, which, if confirmed, would mean that China had leapfrogged significantly into new advanced chip territory. There is doubt that SMIC would be able to produce these high-grade chips at scale, and it is likely that the IP used to manufacture the chips was stolen from TSMC. Following this revelation, Chinese leadership grew concerned that the Biden administration would use this news to implement new controls, leading China to acquire an unusually large amount of inputs and machine tools used in the manufacturing of advanced semiconductors. This stockpiling led to concerns about the long-term integration of advanced chip programs with military programs in China, in line with their civil-military fusion doctrine that blurs lines between civil and military pursuits. To block the proliferation of this advanced technology, the United States implemented what were initially unilateral controls on chips and manufacturing tools, although in January 2023 the Biden administration succeeded in bringing the Japanese and Dutch on board—since these countries produce key inputs, such as machine tools and advanced imaging technology.

Because the United States only controls one chokepoint of the advanced semiconductor supply chain on EDA software, it needed to encourage other advanced economies to join. In March and April 2023, the Netherlands and Japan announced additional controls on their semiconductor exports to China, effectively joining the U.S. chip controls.⁸³ However, wary of economic retaliation from China and also reluctant to get involved in what is increasingly seen as a contentious power struggle between China and the United States, neither the Netherlands nor Japan explicitly referenced a “deal” with the United States when announcing new controls. The two primary chokepoints targeted in this additional trilateral tranche of controls roughly distill into controls on manufacturing inputs and equipment and controls on EDA software. China currently maintains critically low market capabilities when it comes to advanced manufacturing equipment.⁸⁴

As mentioned previously, prior to the October 7 rules, U.S. policy embraced a “moving target” approach that aimed at keeping adversaries one or two generations behind technologically. The United States would raise the level of controls as new technology emerged and then release older generations for export. As a result, China was denied access to the most advanced technology; U.S. companies were able to sell older technology to China and use the revenue generated for research and development; and permitting those exports reduced the incentive for the development of Chinese alternatives. The new policy seeks not simply to keep China behind but to degrade its military capabilities by keeping U.S. controls at the current level regardless of future technology developments. That means the set of controlled items and technologies will become much larger over time, with a concomitant increase in the difficulty of enforcement and the cost to U.S. producers.

While the October 7 rules did not say so directly, they also imply the end of a licensing policy based on identifying reliable end users. China’s publicly articulated civil-military fusion doctrine means that, effectively, there are no longer reliable end users in China, as all are subject to demands from the government to make their technology and

products available for military purposes. The administration has not yet formally taken that step. Instead, it has chosen simply to add companies to its Entity List, effectively denying them “reliable” status. This report does not recommend taking that step at this point, but it is clearly an issue that deserves further consideration.

In addition to the export controls, part of the United States’ strategy is the CHIPS & Science Act, which includes “guardrails”: provisions restricting the legislation’s funds from bolstering enterprises that could pose a national security threat to the United States.⁸⁵ Namely, recipients of CHIPS funding cannot engage in a “significant transaction” to enable the expansion of chip manufacturing facilities in “countries of concern,” including China. The “guardrails” provision broadly interprets which chips are critical to national security, working from a Commerce Department list, in coordination with the Department of Defense and the intelligence community, that includes both leading-edge and mature-node chips. In March 2023, the Department of Commerce proposed an implementation rule that “aligns prohibited technology threshold for memory chips” between export controls and the CHIPS guardrails but also presents a more stringent threshold for logic chips.⁸⁶

In terms of the overall economic health of the industry—and therefore its ability to withstand additional controls—the data are contradictory. The market is anticipated to shrink by 4 percent in 2023, the first semiconductor market contraction since 2019. This is particularly acute in the memory market and is driven primarily by weakened consumer demand. Gartner projects that semiconductor revenue will grow at 7.4 percent—significantly less than the 2021 growth rate of 26.3 percent fueled by the pandemic’s accelerated digitization, which pushed the industry’s collective annual sales past \$500 billion for the first time.⁸⁷ The surplus in demand caused a shortage crisis, and experts estimate that the global chip shortage cost the U.S. economy \$240 billion in 2021. Some U.S. manufacturers had under five days’ worth of inventory, in comparison to 40 days in 2019.

Some firms—such as Lam and Applied Materials, which are affected by the October 7 controls—anticipate a revenue slowdown, although it is difficult to determine with certainty what that contraction may look like. However, Lam anticipates a 2023 revenue drop of roughly \$2.5 billion, while Applied Materials, the largest chip equipment producer in the United States, could lose \$250–550 million.⁸⁸ KLA, meanwhile, anticipates a revenue drop of nearly \$900 million in 2023.⁸⁹ ASML, Lam Research, and KLA have estimated that the October 7 restrictions would cost them a combined \$5.9 billion in lost sales this year alone.⁹⁰

Another major topic on the horizon is whether, in retaliation for more aggressive allied export controls, China will weaponize the trade of mid-tier chips. Overcapacity of Chinese semiconductors would depress the revenue of non-Chinese firms and potentially usher in a more sustained period of sectoral contraction. Depressed revenue, which additional export controls would also likely facilitate, could lead to a decline of R&D funding, potentially imperiling long-term innovation in the sector. However, if the implementation of the CHIPS Act occurs quickly enough and companies see returns on their investments, it would better enable them to weather storms from additional controls on exports as well as any increase in pressure from Chinese overcapacity of legacy chips.

One of the issues with the October 7 controls, according to SemiAnalysis, is “that there is no such thing as equipment for 16nm or less or NAND equipment suitable for less than 128-layers, but not more.”⁹¹ In other words, equipment used to make less advanced memory chips could still be used to make cutting-edge semiconductors—albeit at a much less effective rate. The U.S. government may have to regulate exports of less advanced memory chip processes, such as 64-layer NAND and 20-nm DRAM, to close perceived loopholes in controls.

Due to the use of memory chips in a wide array of civilian goods, additional controls would have disproportionate effects on the economy as they could derail large memory manufacturers’ operations. China represents a large share of global memory chip demand: SK Hynix sold 25 percent of their memory

chips to China, while Micron and Samsung sold China 11 and 10 percent of theirs, respectively, in 2022. These companies' memory chips have applications across the civilian economy—in passenger vehicles, coffee machines, iPhones, and more.⁹² They are also essential to companies' data centers as they are key components of server memory and U.S. organizations' IT operations depend on their supply⁹³. For instance, key sectors—such as telecommunications, banking and financial services, retail and e-commerce, and cybersecurity firms—all require strong server hosting services.⁹⁴ Pursuing policies that would significantly curtail commercial operations in China could usher in a fresh round of supply chain disruptions at a time when neither U.S. nor EU chips packages have been sufficiently deployed. Since an insufficient amount of production in memory chips has moved to the United States, the supply chain disruption risks are very high.

In considering additional semiconductor controls, the U.S. government will need to determine how the new rules affect U.S. company revenue and whether the rules will push China to accelerate its pursuit of indigenous development. The United States will also have to evaluate whether the rules will lead to the “designing out” problem, whereby other countries develop products that contain no U.S. technology and are thus outside the reach of U.S. controls.

On the U.S. revenue question, while the short-term impact is likely small on chip manufacturers and large on equipment makers, as the set of controlled items grows, the negative revenue impact will also likely grow (unless they find alternative markets, like India), and U.S. companies could find themselves short of capital unless they can quickly find other markets with similar growth opportunities. This could slow development of future-generation technology and make U.S. companies less competitive.

Foreign companies “designing out” U.S. semiconductor manufacturers is already a pressing issue. Commerce Secretary Gina Raimondo has expressed worries about the potential for losing additional U.S.-based chip production, pointing out that chip companies are growing: “They’re going to build future facilities . . . they’re not going to build them in America. They’re going to continue to build them in Asia and in Europe, and we risk losing out on that.”⁹⁵ Experts have also raised the issue: even before the October 7 controls, the Boston Consulting Group estimated that the “designing out” concern from previous U.S. semiconductor sanctions would lead to drops in revenue, forcing companies to cut in R&D and capital expenditures leading to the loss of 15,000 to 40,000 highly skilled jobs.⁹⁶ Furthermore, the effects of U.S. government spending on chips could be rendered less effective over time if China pursues retaliation via overcapacity of mature node chips.

Likewise, as China decreases its dependency on semiconductor imports and the Chinese chip industry continues expanding revenues from its growing trailing-edge capacity, its homegrown firms have the space to capture market share from U.S. companies.⁹⁷ Overseas investors have already bought into the idea that Chinese companies will be able to rise to the challenge: Vertex China, for example, raised nearly \$500 million for a new Chinese semiconductor fund to fill in the gaps from the U.S. controls.⁹⁸ Complementing this expansion, China is leveraging specialized education, higher pay, and the hiring of foreign experts to develop its domestic semiconductor innovation landscape and advanced chip manufacturing know-how.⁹⁹

Another consideration is the porousness of controls enforcement. Some controls do not capture all subsidiaries, effectively leaving open a window for firms to acquire controlled items via legal means since their subsidiaries are not covered. CNAS researcher Sam Howell notes that China’s largest facial recognition startup, SenseTime, has used the loophole to avoid the October 7 controls by acquiring advanced U.S. chips through subsidiaries.¹⁰⁰ This indicates that U.S. exporters that continue to sell chips abroad to subsidiaries may not lose revenue in the short term. If the companies indirectly acquiring their technology from U.S. firms through subsidiaries cannot find alternatives, they may be willing to pay more to maintain their supply—potentially raising the revenue of

U.S. firms in the short term. Another way that Chinese entities have circumvented the controls is by using cloud service providers to access advanced chips on which the entities train their language models. For example, the Shanghai-based cloud computing company AI Galaxy has been reportedly charging \$10 for one-hour access to eight advanced A100 Nvidia chips, which are critical to developing novel AI applications and services.¹⁰¹ Currently, U.S. export regulations do not cover cloud providers, even if controlled chips are used.

This means that the long-term costs of the new U.S. policy may be larger than expected, with them becoming a drag on the U.S. industry's ability to compete while at the same time inspiring other entrants into the market that are beyond U.S. control. So far, the controls have resulted in creative workarounds from targeted entities, increased infusion of capital into China's advanced capabilities, and novel "design out" attempts. The best action at this point would be to maintain the October 7 controls but return to the previous policy of treating them as a moving target, which would at least mitigate the revenue and "designing out" issues. This policy would also recognize that China's civil-military doctrine forces an end to a licensing policy based largely on reliable end-users and approved end uses. In the interest of providing a greater degree of certainty for U.S. companies, the policy should be clear that the semiconductor controls apply to all end users and end uses in China through a policy of denial of license applications. Such a policy would leave room for an occasional exception if the U.S. government deemed it in its security interest to permit a specific export.

One of the arguments for changing policy to an invariable control level, as was done on October 7, was that since the Chinese had clearly adopted a policy of indigenous innovation, the opportunity to obtain older technology from Western sources was no longer an incentive to limit their own development. There is merit to that argument, but it also demonstrates that there is no "silver bullet" that will fully control U.S. technology exports at no cost to the domestic industry. That means the best policy is one which assesses both costs and benefits to maintain the best benefit-to-cost ratio. This would be best achieved by combining the October 7 controls with a "moving target" framework going forward, along with recognizing the relevance of civil-military fusion to licensing decisions.

Artificial Intelligence

Policymakers typically use AI to refer to computer systems that simulate human-level cognition.¹⁰² The National Artificial Intelligence Initiative Act of 2020 defines AI as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments."¹⁰³ The global AI market is estimated to have reached nearly \$60 billion in 2021. At an anticipated compound annual growth rate of nearly 40 percent, the market is likely to reach \$422.37 billion by 2028.¹⁰⁴ There are, however, distinct challenges associated with measuring the value of the AI industry, such as its widespread use throughout the economy, ranging from social media platforms to autonomous weapons systems.

In the AI supply chain, the first stage is the gathering of raw data which is then used as training data for AI models. AI models then train, learn, and optimize their functionality before being operationalized. While there are certain guardrails that can be implemented in the modeling phase of AI development, export controls in this case would relate to the data used to train AI models in the first place.

AI systems can be categorized as narrow AI, general purpose AI, and artificial superintelligence. Narrow AI systems are limited to the tasks that they were trained to perform, while general AI systems can also perform tasks that they were not specifically trained to perform. Superintelligence, on the other hand, has the additional capacity to surpass human-level cognition while performing most tasks. Though neither general nor superintelligence AI yet exist, these categories of AI would be vastly unpredictable and vulnerable to new types of manipulation, posing distinct threats to the future of military operations.¹⁰⁵

Aside from these three security-focused categories of AI, generative AI can be considered its own category. Generative AI has come under heightened scrutiny recently due to the proliferation of ChatGPT and similar tools. Generative AI is typically used to refer to an algorithm that can use data patterns to create new content, including audio, code, images, text, simulations, and videos.¹⁰⁶ In this sense, generative AI’s capacities extend beyond those typically thought of as narrow AI. Still, narrow AI systems offer distinct uses in a variety of fields, including intelligence, surveillance, reconnaissance, logistics, and semi-autonomous and autonomous vehicles. Narrow AI systems can react more quickly than systems that require operator input, analyzing exponentially larger amounts of data.

The U.S. government has focused on swarming as a new type of military operation offered by narrow AI. Swarming involves unmanned vehicles autonomously cooperating to complete a task. Swarming has a wide range of capacities, ranging from small groups of vehicles collaborating for the purposes of electronic attacks, fire support, or localized communication nets to large formations of vehicles performing operations designed to overwhelm defensive systems.¹⁰⁷

AI merits controls because of the distinct national security threats that it poses. Narrow AI has already led to significant military advances. The more novel national security domain created by AI, however, is associated with its ability to create and manipulate information.¹⁰⁸ This information could be used to deceive key decisionmakers as well as magnify the impact of potential national security threats.

In the context of supply chains, there are a few operational definitions of AI. According to the International Trade Administration, the AI industry largely consists of “(1) the goods and services that enable AI systems, such as algorithms, data, and computing power, and (2) AI-driven products across all industry verticals, such as autonomous vehicles.”¹⁰⁹ BIS first defined AI in 1994, but its 2022 presentation on export controls outlines how it currently conceptualizes the field.¹¹⁰ The table below compares this list with the White House’s categorization of AI in the February 2022 Critical and Emerging Technologies List Update.¹¹¹

Comparison: BIS and White House Categories of AI

BIS	White House
Neutral networks and deep learning	Deep learning
Evolution and genetic computation	Machine learning
Reinforcement learning	Reinforcement learning
Computer vision	Sensory perception and recognition
Expert systems	Next-generation AI
Speech and audio processing	Planning, reasoning, and decisionmaking
Natural language processing	Safe and secure AI
Planning	
Audio and video manipulation technologies	
AI cloud technologies	
AI chipsets	

Source: Tongele N. Tongele et al., “Emerging Technology Controls” (presented at the BIS 2022 Update Conference on Export Controls and Policy, Washington, DC, June 29, 2022), <https://www.bis.doc.gov/index.php/documents/2022-update-conference/3073-rev3-emerging-tech-update-2022-section-1758-controls-tongele/file>.

Compared with the White House categorization of AI, BIS's version more explicitly highlights hardware components. In addition to software, AI requires advanced hardware to run algorithms and protect privacy.¹¹² The nature of AI research tends to be collaborative and global, which presents new challenges for export controls.¹¹³ For instance, a significant amount of AI code is published on online sources like arXiv.org, which is meant to act as a free distribution service.¹¹⁴ As a result, export controls in the realm of AI typically focus on its hardware components, as demonstrated by the October 7 controls. However, as the encryption and quantum debate highlights, there is an urgent need to develop controls for intangible goods, such as algorithms, since the control of hardware in certain circumstances is insufficient in controlling dual-use algorithms.

While AI export controls will certainly impact adversaries, they will also have distinct implications for the U.S. economy. Matt Borman, deputy assistant secretary of commerce for export administration at BIS, noted that “we would never have a control that covers [all of] artificial intelligence. That would be completely ineffective and unworkable and, frankly, counterproductive . . . The way we craft these controls, we try to be as technical as possible so that everybody in the affected community can have a clear understanding of what is covered and what is not.”¹¹⁵

Export controls on AI capabilities have so far concentrated overwhelmingly on the hardware components that enable advanced AI, although that approach is incomplete. Recently, for example, Chinese AI companies including iFlytek have circumvented the October 7 controls by renting advanced chips through cloud service providers to run advanced AI training models.¹¹⁶ Still, only the White House CET and the Commerce Review of Controls for Certain Emerging Technologies lists explicitly identify AI as meriting its own categorization. Given the intricacies of controlling this evolving technology, developing uniquely tailored controls for it is critical.

Since language models for AI are often publicly available, it is more practical to consider a taxonomy for controlling data, which in the AI supply chain functions as an input. As CSIS has previously argued, assuming that controlling data is either too burdensome for BIS or that it is a politically unwinnable issue will not result in a more secure digital environment going forward.¹¹⁷ BIS should thus consider building new export control rules for dual-use data flows that feed AI systems, which will be discussed in more detail in a later section.

Biotechnology

Demonstrative of the crosscutting nature of data flows, AI, and biotechnology, National Security Adviser Jake Sullivan in his September 2022 speech said, “Computing-related technologies, biotech, and clean tech are truly ‘force multipliers’ throughout the tech ecosystem. And leadership in each of these is a national security imperative.”¹¹⁸ Advances in biotechnology have allowed researchers to create new services and products, providing opportunities for economic growth—economic activity related to biotechnology and biomanufacturing is referred to as “the bioeconomy.”¹¹⁹ As one interviewee for this project noted, there are intersectional considerations at the heart of export controls, data, and these emerging technology case studies. The interviewee said:

What technologies need to be mastered to win that game? And what are the threats? DNA reading and sequencing—who owns those technologies? Who is the best at writing DNA—who can figure out how to put this into cells? Which countries own this right? And then: who owns all the data when you program a cell? AI is a supporting technology to this—run next to it to see what else you can do.¹²⁰

Recently, the U.S. government has pursued policies on biotechnology to remediate the multifaceted risks of relying on China for this technology as well as its vast dual-use capabilities. In 2018, the U.S. government passed the Foreign Investment Risk Review Modernization Act (FIRRMA), which extended the scope of CFIUS's

review to the biotechnology sector. Further, to spur U.S. investment in biotechnology, President Biden signed an executive order, “Advancing Biotechnology and Biomanufacturing Innovation for a Sustainable, Safe, and Secure American Bioeconomy,” in September 2022, which underscores the administration’s elevation of biotechnology as a sector key to U.S. national security concerns. The executive order aims to use biotechnology and biomanufacturing as vehicles for addressing health, climate change, energy, food security, and national security issues. One of its primary objectives is to “bolster and coordinate Federal investment in key research and development (R&D) areas of biotechnology and biomanufacturing in order to further societal goals.”¹²¹

In addition to “running faster” policies in the bioeconomy, the administration has also applied new export controls to biotechnologies. In November 2018, BIS designated biotechnology as an emerging technology—which now accounts for 2 of the 38 emerging technology controls. In February 2022, BIS added China’s leading contract drugmaker, WuXi Biologics Co., Ltd., to the Unverified List, along with one of its subsidiaries.¹²² WuXi Biologics lost a fifth of its market value in one day. It has since been removed from the list, although its subsidiary remains listed. Despite the edge, this may have provided to U.S. competitors, investment banking group Jefferies has found that replacing Chinese drugmaker production would cost the United States \$18 billion, not accounting for annual labor costs. Controls on biotechnology thus face the obstacle of remaining strict enough to protect national security but sufficiently flexible to facilitate further growth in a robust non-military economy.

Commensurate with the growing recognition of biotechnology as a key industry of the future is growing concern that the proliferation of biotechnology as a weapon poses serious national security risks. A foreign adversary could bioengineer a super pathogen and plant it in an environment that makes it difficult to identify. For example, warming temperatures in the spring and summer in Ukraine could lead to a cholera outbreak. A foreign adversary could bioengineer a strain of cholera that would make the outbreak magnitudes deadlier and nearly impossible to identify as an attack.

Another potential application of biotechnology is a foreign adversary gaining access to DNA. In February 2021, the National Counterintelligence and Security Center raised the concern that since 15 Chinese companies are licensed to provide genetic testing or genomic sequencing on U.S. patients, Chinese firms could directly access Americans’ genetic data.¹²³ This would potentially enable China to develop pathogens specific to parts of the U.S. population or, more likely, to use DNA information as blackmail against people in power. For example, a foreign adversary could predict that a politician’s child is likely to develop cancer and offer to preemptively cure the cancer in exchange for political concessions.

Recent conversations around brain computer interface (BCI) also highlight the enormous complexities involved with designing export controls. For example, with BCI, a brain could be made to “drive” an autonomous vehicle, even if the person is not physically inside the vehicle.¹²⁴ BIS undersecretary Alan Estevez has likened BCI to a “superman in combat.”¹²⁵ While brain computer interface (BCI) technology has extensive military capabilities, it also has the potential to assist people with ALS and other diseases.¹²⁶

With BCI, the benign applications probably outnumber the military ones, which also seem largely theoretical at this point. The dilemma of these technologies is that in each case, there is a non-zero possibility of malign use. No matter how “civilian” it appears, there is always some application that could compromise security, even if it is decades away. Over-controlling BCI during its nascence could imperil vital medical advances that could significantly improve the lives of people living with ALS and other diseases. It is thus incumbent on BIS to determine what risks the proliferation of this technology would entail, and whether they would warrant a possible delay in medical advancements. Minimizing security harm

while utilizing the medical innovations of BCI is a direct example of the ethical dilemmas involved in the implementation of export controls on biotechnology.

The development and use of biotechnology are constrained by two key chokepoints. The first and most obvious is the people who are involved in the development of biotechnology advancements with national security implications. Much like enhancing hardware involves cross-border technology transfers, know-how is best developed by cultivating talent from multiple countries. Biotechnology has benefitted from knowledge-sharing among the international community: U.S. research institutions specializing in the field, such as the National Human Genome Research Institute, count on researchers from abroad to contribute to their work. Exchanging information about technology with foreign individuals, however, can be considered an export even if it takes place on U.S. soil—clashing with export controls meant to curb transfers of knowledge to entities of concern. Moreover, restricting these “deemed exports” is a difficult undertaking for U.S. authorities.

The dilemma of these technologies is that in each case, there is a non-zero possibility of malign use. No matter how “civilian” it appears, there is always some application that could compromise security, even if it is decades away.

AI and data experts remain suspicious of the more hawkish claims about the need to control biotechnology inputs because early identification of cancer, for example, requires the precise convergence of several data sets. For example, an accurate assessment of someone’s health requires not only the data available via health tracking apps but also information about their exercise routines, smoking habits and drug use, as well as their food intake and periodic check-up information. While it is theoretically possible that an adversary could gain access to these datasets simultaneously, it is a stretch of the imagination to regard that possibility as a present threat. At the same time, these technological advances also hold the promise of positive medical benefits, which complicates efforts to block their proliferation.

The more alarmist examples of potential national security implications of biotechnology often point to their weaponized uses. The Australia Group—the multilateral export control regime responsible for coordinating control of bioweapons—already maintains the architecture capable of housing international discussions to stem the proliferation of dangerous bioweapons. In the examples above, the case of bioengineering a “super cholera” in Ukraine is clearly a weapon and would fall under the Australia Group, whereas using personal data as blackmail is less clearly a weapon and therefore may merit the application of dual-use controls. Rather than design a new set of controls on U.S. exports relevant to biotechnology, the U.S. government should work within the Australia Group to multilateralize controls on bioweapons. To the extent that the United States is not satisfied with work within the Australia Group, it could expand its controls on data and knowledge transfers, which are discussed in detail below.

Nevertheless, regulating the bioeconomy from a dual-use perspective fits squarely under the banner of export controls. Because not all genetic data is the same, the treatment of data in the bioeconomy needs to be sufficiently narrow. For example, certain healthcare data—DNA sequencing during pregnancy, for example—goes to a clinical diagnostic setting. Other types of data are used in government-sponsored research initiatives

and are clearly noncommercial in nature. Both of these examples contrast with data shared in applications like 23andMe, in which companies (in this case a foreign-owned company) are profiting from U.S. personal data that a foreign government could access and then leverage for nefarious purposes.¹²⁷ There are also profound concerns about the ability to control populations—for example ethnic minorities, such as the tactics used to track Uyghur Muslims in Xinjiang—through the use of DNA data.¹²⁸

Recent changes to regulatory regimes governing health data represent a step in the right direction. For example, the Department of Justice’s Trusted Exchange Cooperation Agreement encourages health institutions to join a network of trusted partners, elevating standards on exchanging data. However, this is probably insufficient in the long run and falls short of a hard regulatory mechanism like export controls, as these that would create a formal notification and licensing regime for outbound personal data flows, which is discussed in further detail below. In short, BIS should implement a new rule that would require exporters of personal sensitive biological data to obtain an export license for data flows with national security implications. This includes data about gene sequencing, for example, that could be used to control populations or aid the development of a bioweapon, such as a super strain of cholera. There will emerge instances in which it is vital that healthcare data flow freely, as exemplified during the early stages of the Covid-19 pandemic. In these instances, BIS should create an exemption process for healthcare data to move freely across borders in cases in which the health security of the U.S. population is directly imperiled by pathogens or other risks.

Intangible Goods

If World War I was a war of chemistry, and World War II was a war of physics, twenty-first-century conflicts will showcase the weaponization of data. Yet, an obvious feature of the above categories is that they often lack considerations for the control of intangible goods and their inputs, despite the inherently nonphysical nature of many of the dual-use items covered in export control and technology lists.

Intangible goods can include everyday items such as digital music files or non-fungible tokens ; on the other hand, they can also include AI-enabled software that tracks the movement of people, guides advanced weapons systems, and builds algorithms that can sway voters. In addition to supporting hardware, other enablers of AI deserve consideration for controls. These include AI development tools, training datasets, and machine learning models. Enhancing controls on intangible goods also aligns with the administration’s National Security Strategy. In the National Security Strategy document, the Biden administration writes, “We will also work to counter the exploitation of American’s sensitive data and illegitimate use of technology, including commercial spyware and surveillance technology, and we will stand against digital authoritarianism.”¹²⁹

As the above examples demonstrate, there is a clear linkage between hardware and software applications, and many data-driven malicious behaviors do not require advanced computers. The use of micro-data for targeting civilians (“hacking the consciousness”) can be carried out with relatively light combing of personal user data. This tactic was used in the Brexit vote and the 2016 U.S. presidential election, and combating it is likely to become an integrated part of election—and therefore national—security around the world.¹³⁰ The algorithms used to target voters in these cases are the same ones that can sell cheaper products to consumers or help them more easily find a location on Google Maps, highlighting the dual-use nature of these intangible goods.

One example of an intangible good that deserves far more consideration for controls by the United States government is Pegasus spyware and its equivalents. The NSO Group’s Pegasus Software, which the New York Times describes as “the world’s most powerful cyberweapon,” has stimulated conversation regarding

the unprecedented capabilities of digital spyware.¹³¹ NSO Group is an Israel-based company that licenses surveillance software to government agencies. NSO argues that Pegasus prevents the ability of criminals and terrorists to go “dark” with encryption technology.

Spyware operates by infiltrating digital devices without phishing tactics. Once contact is made with a cell phone, for example by sending a text message, even if the user does not click on or open the message, the spyware can still be installed. Even if the device is powered down, the spyware can remotely turn on its recording capabilities, including its video recording device. Potentially more dangerous, however, is that Pegasus can infiltrate apps on devices, downloading entire email, message, and communications history, even in encrypted apps like WhatsApp and Signal. This creates a massive vulnerability for blackmail and the overall security of digital communications.

Pegasus has been under scrutiny for years.¹³² In October 2019, WhatsApp sued NSO Group for exploiting its services to spy on 1,400 phones. In November 2021, the Biden administration placed NSO on the blacklist.¹³³ And, in November 2022, Apple sued NSO Group in an attempt to block Pegasus from Apple devices.¹³⁴ However, it is intrinsically difficult to control, and though Pegasus’s capabilities have received a significant amount of media attention, it is not the only software that provides these spyware services. The European Parliament has also stood up a special investigative committee to evaluate the geopolitical risks of Pegasus.¹³⁵

In 2020, BIS implemented new controls on emerging technologies agreed to during the 2019 Wassenaar Arrangement plenary. One of these categories includes “digital forensics tools that circumvent authentication or authorization controls on a computer (or communications device) and extract raw data.”¹³⁶ This rule added 5D001.e technology control for surveillance software.¹³⁷ In March 2023, the Biden administration signed an executive order to ban the U.S. government from using commercial spyware that might present risks to national security or human rights.¹³⁸ At the same time, the U.S. government promised to continue combatting the use of commercial spyware to target U.S. government personnel overseas.

Intangible goods controls will more likely than not need to cover the data that feeds these applications. Data serves as the feed-in to algorithms, which in turn churn out end-use specific applications, as demonstrated by the capabilities of Pegasus. The computing power required to execute Pegasus commands, however, is markedly lower than AI-powered hypersonic missiles or even consumer autonomous vehicles. This means that solely controlling the advanced chips that are used to run the latter is insufficient and therefore less likely to result in a more secure or controlled environment over time. Data controls, coupled with targeted hardware controls, can help fill this gap.

As part of its mandate under FIRRMA, the Treasury Department has attempted to deal with questions of sensitive personal data, which it defines in its 2020 Final Rule on Provisions Pertaining to Certain Investments in the United States by Foreign Persons.¹³⁹ Under this rule, the U.S. government maintains the authority to exercise increased review authority over transactions that involve “sensitive personal data” or a U.S. user base of at least one million individuals.¹⁴⁰ Skeptics of this approach have argued that the threshold is far too high and that it would exclude critical transactions from scrutiny. While the U.S. government can exercise increased national security review under CFIUS, that process governs inbound investment—for example a foreign entity acquiring a U.S. firm that maintains large databases of customer DNA samples. This could and probably does provide some enhanced protection against the large-scale exfiltration of U.S. data, but the approach stops short of a wholesale control regime on exported U.S. data.

Efforts to ban data flows outright are counterproductive and can harm the ability of businesses to conduct business. Furthermore, banning certain applications, such as TikTok, invites a host of legal questions relating

to First Amendment freedom of speech rights and risks serious political blowback among U.S. voters. A tailored approach that creates a new licensing requirement for the export of sensitive data offers a middle ground, whereby BIS leads a new approach to the intangible economy, and consumers and companies think more strategically about the outflow of sensitive information.

Procedurally, BIS should add a new category to the CCL. As discussed above, the CCL is divided into 10 categories (0-9) and then contains a separate, more granular set of five product groups. The addition of a Category 10 on “Intangibles” would grow the CCL to 11 total categories. The Category 10 items would then rely on the existing set of product groups under Product Group C, which covers materials. This would more clearly define data as an input to an item. The Product Group C designation would merit further granularity and could consist of categories such as commercial data and personal data, which could then contain sub-categories of their own. This could create, for instance, a designation of 10C001 for commercial data flows with military applications, such as data used as an input into national security critical AI programs. 10C001.a could include commercial data flows with dual-use biotechnology applications; 10C002 could include personal data used by a malicious foreign entity with applicability in blackmail and political persuasion; 10C002.a could include personal health data; and so on.

A tailored approach that creates a new licensing requirement for the export of sensitive data offers a middle ground, whereby BIS leads a new approach to the intangible economy, and consumers and companies think more strategically about the outflow of sensitive information.

This new Category 10 would allow BIS to designate, as needed, certain bulk data flows as inputs to certain end users and end uses that could harm long-term U.S. national security interests. This designation would represent a significant departure from the traditional application of controls that conform largely to nonproliferation objectives, but making this change would better reflect today’s digital threat environment and advance the U.S. government’s ability to treat data as a commodity.

Given the persistent political complexities of passing comprehensive federal privacy legislation, the U.S. government should instead use the full capability of its administrative tool kit to create a new rule requiring export control licenses for the bulk export of data. With this expansion of the CCL, BIS should then publish a rule that requires exporters of bulk data to seek a license to export certain categories—such as personal data transferred via apps such as 23andMe—to foreign entities of concern. In the case of personal data, a condition of the export license should be the informed consent of users of digital applications. This license process should also create a new presumption of denial rule policy in cases in which the user has not provided explicit consent for the international export of their personal data. This could function similarly to the EU General Data Protection Regulation, which creates an opt-in widget for users of online platforms. While not a panacea, this informed consent condition of the license could significantly reshape the conversation around digital privacy in the United States, with far-reaching consequences in non-trade policy domains.

While some skeptics of increased data flow constraints have argued that new controls would significantly shift the United States away from its traditionally free trade approach to data flows, this approach represents a viable middle ground, whereby entities exporting large swaths of U.S. data would need a license to do so in cases in which BIS establishes a clear national security justification. Furthermore, this policy would obviate the need for a ban, which would more closely resemble a digital embargo.

The design of a new system for controlling intangible goods is far from perfect and will require tremendous work to ensure that it is both adequately surgical and not counterproductively porous. Another benefit to this approach is that it does not depend on comprehensive federal privacy legislation, which Congress has thus far been unable to pass. This approach would apply a novel export control rule to personal data. It would also simultaneously create a more direct consent mechanism for consumers and provide clearer parameters for firms exporting their data to foreign entities, particularly in countries of concern.

A key question is where to establish the threshold for requiring a license. The 1 million user parameter is arguably too high. In the cases of novel research, it is possible that a sample size of only 10,000 humans would offer tremendous leverage to a foreign adversary. However, these cases are relatively rare, and a threshold of 10,000 users would invite substantially more compliance paperwork for firms. Therefore, BIS would need to design a formula for determining which firms require licenses for sensitive data exports. This could cover end users and end uses.

As the global economy continues to shift from analog to digital, it is critical that countries develop a new model that moves beyond traditional export controls and toward a new taxonomy for intangible goods regulation. This new approach should more clearly delineate which types of sensitive, intangible goods merit which types of controls. The current gap in policymaking provides the United States with an opportunity to lead in creating the reimagined export control regime of the future—and in so doing, to regain some of the credibility it has lost by failing to pass comprehensive digital regulation.

Recommendations

The U.S. government has a variety of tools available to both restrain China and enhance the U.S. domestic technology sector, which is essential to providing the U.S. military with an advanced technological edge over adversaries. Such tools include export controls, investment screening mechanisms, and domestic innovation policy. If controls are too loose, U.S. adversaries gain access to technology they can use against the United States; if they are too tight, the United States may inadvertently starve its high-tech companies of the revenue they need to develop next-generation products. If implemented correctly, export control policy can both restrict the outflow of technology to foreign adversaries—thereby degrading their military capabilities—and advance industry interests that ultimately bolster U.S. technological leadership. Based on the above case studies, CSIS proposes the following recommendations aimed at helping the United States and its technodemocratic allies gain the upper hand.

Help domestic industry and allied economies “run faster” in the race by ensuring that government support is consistent, sufficient, and iterative.

In the development of emerging technologies, it is crucial to long-term U.S. and allied competitiveness that governments assist in helping emerging industries “run faster.” Governments can achieve this objective by loosening immigration restrictions to attract talent and by providing financial incentives that reduce costs and encourage risk-taking throughout new industries. The need for added support is particularly critical in the quantum technology field, where current firms incur greater costs due to the vertical nature of their operations and the relatively low degree of cross-firm collaboration.

Funding support must be sufficient. While industrial policy is largely a separate discussion from export controls, overly broad controls can depress the profitability of advanced technology firms, reducing the viability of the U.S. high-tech sector over time. In general, the need to loosen immigration restrictions and

provide additional funding aligns with the need to ensure that the export control side of policy is adequately coordinating with the incentive packages that governments provide.

Create a new category governing data exports. Clearly designate data as a commodity, treat it as an input, and require exporters of certain data categories to seek an export license.

The United States has long struggled to develop tools to regulate what has been the unfettered flow of data. The reluctance of the United States to pursue policies similar to the EU General Data Protection Regulation has resulted in the United States losing credibility in international negotiations, whether within the Indo-Pacific Economic Framework pillar on digital trade or within international standards bodies such as the International Telecommunications Union. As CSIS has previously written, “As the world barrels deeper into digitization, claiming that governing data and intangible goods cannot be done is a losing strategy.”¹⁴¹ Developing a policy to subject bulk personal data exports to additional export control licensing requirements would restore U.S. credibility within ongoing negotiations, including within the Joint Statement Initiatives at the World Trade Organization. It would also advance U.S. national security objectives. In turn, this policy would create an informed-consent mechanism that better alerts U.S. citizens about the use of their data, providing a more democratic opt-in format for sharing personal data with foreign entities. Overall, expanding the CCL with digitization in mind would advance the institutionalization of export controls on intangible goods.

Keep controls relatively light or flexible for emerging technologies, particularly quantum, as over-controlling industries can depress growth and innovation.

In very few cases is the need to “run faster” rather than to “trip the competition” as abundantly clear as with quantum technology. As it currently stands, there is no industry or government consensus on where the United States leads versus where China leads. Without sufficient information and given the nascent state of the quantum technology industry, additional controls on quantum technology risk hobbling an industry with immense potential in economic, security, and technological superiority terms. The decision against levying controls on the internet, for example, facilitated decades of growth throughout the United States and allied economies. Allowing the internet to proliferate has enabled the creation of a diverse digital ecosystem that has led to tremendous innovation, including among small- and medium-sized enterprises. Allied economies have a vested interest in avoiding policies that would further silo a nascent quantum technology sector, lest they end up on the receiving end of the next-generation technological ecosystem—particularly one designed by nondemocratic countries.

Increase knowledge base by institutionalizing communications with the private sector.

One longstanding shortcoming of the current approach to export controls is that there are gaps in communication between the private sector and the government. BIS, in concert with other government agencies and allied economies, should institutionalize the transfer of private sector knowledge on critical emerging technologies. Although the Technical Advisory Committee already assists in policy formulation, the establishment of targeted working groups on national security critical technologies, such as quantum, could provide an additional platform for a specific industry to educate the government about industry concerns and new technology developments.

Increase funding for BIS and ensure that it remains part of the Department of Commerce.

As CSIS has repeatedly written, providing additional funding for BIS is one of the best returns on investment available anywhere in national security.¹⁴² BIS has highly technical institutionalized knowledge about the

export control system that spans technology supply chains around the world. It is also uniquely positioned to promulgate policies at the nexus of foreign policy, commercial considerations, and national security. Because of these constituencies, BIS has been highly effective over time at soliciting input from the private sector. Resituating BIS inside a different agency would reduce its credibility throughout the private sector, which BIS depends on to gather intelligence and assist it in designing sufficiently surgical export control tools.

For the price of only one helicopter, BIS could substantially increase its staffing capabilities and obtain much-needed technologies to fortify its policymaking and foreign policy wing, not to mention to enhance its existing enforcement capabilities. In addition to providing funding for advanced technologies and human resources, additional appropriations should establish new positions at BIS that study the economic costs of controls. This would mirror new positions recently created within the Department of Treasury's Office of Foreign Assets Control. Given how high the stakes are today and the close nature of the race for technological superiority, it is imperative that BIS have the tools necessary to complete a full assessment of the economic and innovation risks of additional controls. While BIS currently maintains that ability, it lacks adequate capacity to build a more robust economic assessment team.

Conclusion

As a post-Cold War world order continues to develop, the United States and its allies must contend both with an increasingly multipolar world in the short run and with the possibility that it will further evolve into two blocs—democratic states and authoritarian states—with the majority of countries trying to avoid alignment with either. At the same time as political realignment is occurring, rapid technological change—including accelerating digitization and the proliferation of new dual-use technologies, as well as China’s adoption of its civil-military fusion doctrine—is creating greater economic and geopolitical risk for all countries.

For the United States, that has meant the conflation of national security with economic policy, which is leading to expanded export controls on advanced technology, a likely instrument to screen outbound investment flows into critical sectors, and greater government expenditures on industrial policy initiatives designed to help the United States maintain its technology leadership.

As it reexamines its approach to export controls, the U.S. government needs to begin by identifying its goals. Clearly establishing what is critical to national security and what is not reduces the probability that the government will apply controls that are either too broad or too narrow. Maintaining a clear strategy also assists allied economies in mapping their own critical supply chains and export controls, resulting in greater convergence over time.

The United States may no longer be in a position to control China’s actions, if it ever was. China is already pursuing its own technology development program in the semiconductor sector and other advanced sectors, such as quantum computing, and it is not likely to deviate from those ambitions regardless of U.S. actions. That means the important question is not how to hold China back, as the U.S. capability for doing that is limited, but rather how to stay ahead. A strategy for that lies in the various U.S. industrial policy initiatives enacted in the past two years, most notably the CHIPS and Science Act, but that alone will be insufficient to

achieve long-term U.S. strategic objectives. Private investment will also continue to be a critical element in U.S. competitiveness in emerging technologies, and U.S. export control policy should be tailored to encourage rather than deter it.

Because the quantum technology sector is so new, applying additional controls risks hobbling an industry at a time when it is important to run faster against the competition. The United States currently lags in public quantum technology spending, already putting the country at a disadvantage vis-à-vis other advanced technology producing countries. This shortage of financing, coupled with additional controls, could retard growth rather than accelerate it. If the primary policy goal is to maintain leadership, then U.S. efforts are better spent pursuing a more liberal immigration policy that attracts talent away from its adversaries and providing funding to scale up domestic production capabilities and accelerate research and development.

The field of AI is a highly dynamic one, in which open source language models proliferate, making the design and implementation of non-hardware controls nearly impossible. The biotech economy is similarly broad and diverse. While each of these is in some ways dependent on hardware inputs and deemed exports, particularly in the case of biotechnology, they both rely on a key critical input: data. The utility of controls is perhaps clearest in hardware, for example in advanced semiconductors, but controlling only hardware and enabling software leaves a broad category of inputs uncontrolled.

Controlling data presents unique challenges for the government, both conceptually and from the perspective of enforcement. Getting it wrong could have significant security and economic consequences. Nevertheless, the integral role of data in emerging technologies means the government has no choice but to address the issue.

Reimagining the current approach to export controls affects not only U.S. companies and long-term U.S. national security objectives. The expanded use of export controls as an instrument of foreign policy, particularly via the application of extraterritorial measures, also directly implicates allied economies in the pursuit of U.S. foreign policy objectives. Redesigning controls away from strict nonproliferation objectives and into emerging technology areas, including the potential designation of data as an input to intangible goods such as algorithms and language models, will directly affect key allies. As the United States and its partners begin rethinking export controls in the multilateral context—including building a fifth multilateral export control regime—the burden will fall on allies and the United States to produce a clearer definition of what is critical to national security and what the ultimate objectives are of this policy redesign. This report has provided some suggestions for how to approach that challenge, and the second report later in 2023 will elaborate on them.

About the Authors

William Reinsch holds the Scholl Chair in International Business at the Center for Strategic and International Studies (CSIS) and is a senior adviser at Kelley, Drye & Warren LLP. Previously, he served for 15 years as president of the National Foreign Trade Council, where he led efforts in favor of open markets, in support of the Export-Import Bank and Overseas Private Investment Corporation, against unilateral sanctions, and in support of sound international tax policy, among many issues. From 2001 to 2016, he concurrently served as a member of the U.S.-China Economic and Security Review Commission. He is also an adjunct assistant professor at the University of Maryland School of Public Policy, teaching courses in globalization, trade policy, and politics.

Reinsch also served as the under secretary of commerce for export administration during the Clinton administration. Prior to that, he spent 20 years on Capitol Hill, most of them as senior legislative assistant to the late Senator John Heinz (R-PA) and subsequently to Senator John D. Rockefeller IV (D-WV). He holds a BA and an MA in international relations from the Johns Hopkins University and the Johns Hopkins School of Advanced International Studies respectively.

Emily Benson is director of Project on Trade and Technology, and senior fellow of Scholl Chair in International Business at the Center for Strategic and International Studies (CSIS), where she focuses on trade, investment, and technology issues primarily in the transatlantic context. Prior to joining CSIS, she managed transatlantic legislative relations at a European foundation, focusing on trade relations and emerging technologies such as artificial intelligence. She also worked to combat money laundering via the illicit flow of art from conflict zones and spent several years at an international law firm focused on sanctions and export controls. During graduate school, Emily spent a summer in the trade section at the EU Delegation to the United States, working on digital regulation and trade remedies. Her commentary and research have appeared in publications such as the *New York Times*, *Washington Post*, *Wall Street Journal*, *Foreign Policy*, and *Politico*, and she is regularly quoted in domestic and international news outlets. She received her joint BA in international

affairs and political science from the University of Colorado and her MA in political science from the University of Geneva in Switzerland. Fluent in French, Emily has lived abroad in France, Indonesia, and Switzerland.

Thibault Denamiel is a research associate with the Scholl Chair in International Business at the Center for Strategic and International Studies (CSIS). His interests include the intersection of trade and U.S. national security, industrial policy, and trade policy as a diplomatic tool. His previous work with the Scholl Chair includes researching the role of immigration policy on innovation in advanced technologies, export controls, and transatlantic cooperation on climate and trade policy. His work has been featured in *Politico*, *Inside U.S. Trade*, as well as university publications such as NYU's *IR Insider*. During his time in graduate school, Thibault interned with, among others, the Office of the U.S. Trade Representative, the International Trade Administration, and the U.S. Chamber of Commerce. Thibault graduated from the Johns Hopkins School of Advanced International Studies (SAIS) with a master's degree in international relations and holds a bachelor's degree from the New York University honors international relations program.

Margot Putnam is an intern with the Scholl Chair in International Business at the Center for Strategic and International Studies (CSIS), where she researches export controls and equity provisions in trade agreements. While working at CSIS, she completed her MA in international relations at Johns Hopkins University School of Advanced International Relations (SAIS), focusing on states, markets, and institutions and Latin America. During graduate school, Margot spent a summer researching climate policy at the South African Reserve Bank. Before SAIS, Margot worked as a legal analyst on the Global Markets team at Goldman Sachs in New York. She received her BA in government with minors in art history and Chinese from Dartmouth College and has worked or studied in Chile, China, Italy, India, South Africa, and Spain.

Endnotes

- 1 “Remarks to the Press: Antony J. Blinken, Secretary of State, Stanford University Encina Hall Steps, Stanford, California,” U.S. Department of State, October 17, 2022, <https://www.state.gov/secretary-antony-blinken-remarks-to-the-press-3/>.
- 2 U.S. Congress, Senate, Committee on Banking, Housing, and Urban Affairs, *Export Administration Act of 1979*, S 737, 96th Congress, 1979, H. Rep. 96-482, <https://www.congress.gov/bill/96th-congress/senate-bill/737>; U.S. Library of Congress, Congressional Research Service, *Export Controls: Key Challenges*, by Christopher Casey (2021), [https://crsreports.congress.gov/product/pdf/IF/IF11154#:~:text=Export%20Control%20Reform%20Act%20\(ECRA\)&text=Congress%20passed%20the%20Export%20Control,XVII%20of%20the%20same%20act\)](https://crsreports.congress.gov/product/pdf/IF/IF11154#:~:text=Export%20Control%20Reform%20Act%20(ECRA)&text=Congress%20passed%20the%20Export%20Control,XVII%20of%20the%20same%20act)).
- 3 Che Pan, “China’s Top Chip Maker SMIC Achieves 7-nm Tech Breakthrough on Par with Intel, TSMC and Samsung, Analysts Say,” *South China Morning Post*, August 29, 2022, <https://www.scmp.com/tech/big-tech/article/3190590/chinas-top-chip-maker-smic-achieves-7-nm-tech-breakthrough-par-intel>.
- 4 There is literature on the stifling effect of export controls on innovation. See, for example, Tim Hwang and Emily S. Weinstein, *Decoupling in Strategic Technologies: From Satellites to Artificial Intelligence* (Washington, DC: Center for Security and Emerging Technology, July 2022), <https://cset.georgetown.edu/publication/decoupling-in-strategic-technologies/>; and Hugo Meijer, *Trading with the Enemy: The Making of US Export Control Policy toward the People’s Republic of China* (Oxford: Oxford University Press, March 2016), <https://academic.oup.com/book/11150>.
- 5 Office of Technology Evaluation, *U.S. Space Industry “Deep Dive” Assessment: Impact of U.S. Export Controls on the Space Industrial Base* (Washington, DC: U.S. Department of Commerce, February 2014), 28, <https://www.bis.doc.gov/index.php/documents/technology-evaluation/898-space-export-control-report/file>.
- 6 Ryan McMorro et al., “China Overhauls Ministries to Take on the West in Tech,” *Financial Times*, March 7, 2023, <https://www.ft.com/content/d1b4a726-c50c-452d-b954-d61f87cd16e8>.

- 7 Rob Jesudason, “China Will Win Quantum Computing Race unless West Ups Its Game,” *Nikkei Asia*, January 12, 2023, <https://asia.nikkei.com/Opinion/China-will-win-quantum-computing-race-unless-West-ups-its-game#:~:text=According%20to%20consultancy%20McKinsey%20%26%20Co.>
- 8 Elliot Ji, “Great Leap Nowhere: The Challenges of China’s Semiconductor Industry,” *War on the Rocks*, February 24, 2023, [https://warontherocks.com/2023/02/great-leap-nowhere-the-challenges-of-chinas-semiconductor-industry/#:~:text=The%20Chinese%20government%20has%20allocated; and Dieter Ernst, *From Catching Up to Forging Ahead: China’s Policies for Semiconductors* \(Honolulu, HI: East-West Center, September 2015\), <https://doi.org/10.2139/ssrn.2744974>.](https://warontherocks.com/2023/02/great-leap-nowhere-the-challenges-of-chinas-semiconductor-industry/#:~:text=The%20Chinese%20government%20has%20allocated; and Dieter Ernst, From Catching Up to Forging Ahead: China’s Policies for Semiconductors (Honolulu, HI: East-West Center, September 2015), https://doi.org/10.2139/ssrn.2744974.)
- 9 Ben Wodecki, “IDC: China Set to More Than Double AI Spending by 2026,” *AI Business*, October 12, 2022, <https://aibusiness.com/verticals/idc-china-set-to-more-than-double-ai-spending-by-2026>.
- 10 Jon Harper, “China Matching Pentagon Spending on AI,” *National Defense Magazine*, January 6, 2022, <https://www.nationaldefensemagazine.org/articles/2022/1/6/china-matching-pentagon-spending-on-ai>.
- 11 Guo Yingzhe and Luo Guoping, “China Launches First ‘Bioeconomy’ Five-Year Plan,” *Caixing Global*, May 11, 2022, <https://www.caixinglobal.com/2022-05-11/china-launches-first-bioeconomy-five-year-plan-101883683.html>; and Tristan Bove, “Biden’s New Executive Order Triggers New Front in US-China Economic Competition,” *Fortune*, September 12, 2022, <https://fortune.com/2022/09/12/biden-biotech-executive-order-compete-china/>.
- 12 “5 CFR § 1400.102 - Definitions and Applicability,” Cornell Law School Legal Information Institute, <https://www.law.cornell.edu/cfr/text/5/1400.102>.
- 13 The White House, *National Security Strategy* (Washington, DC: The White House, October 12, 2022), <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>.
- 14 “Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit,” The White House, September 16, 2022, <https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/09/16/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit/>.
- 15 Martijn Rasser, “A Conversation with Under Secretary of Commerce Alan F. Estevez,” CNAS, October 27, 2022, <https://www.cnas.org/publications/transcript/a-conversation-with-under-secretary-of-commerce-alan-f-estevez>.
- 16 Ian Cohen, “BIS Relaxes Export Review Policy for Certain Satellites, Parts,” *Export Compliance Daily*, March 17, 2023, <https://exportcompliancedaily.com/news/2023/03/17/bis-relaxes-export-review-policy-for-certain-satellites-parts-2303160042>.
- 17 Bureau of Industry and Security, “Review of Controls for Certain Emerging Technologies,” *Federal Register*, November 19, 2018, <https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies>.
- 18 Members of the Wassenaar Arrangement are: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, Romania, the Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Türkiye, Ukraine, the United Kingdom, and the United States.
- 19 “Wassenaar Nations Set New Export Controls,” *Arms Control Association*, April 2020, <https://www.armscontrol.org/act/2020-04/news-briefs/wassenaar-nations-set-new-export-controls>.
- 20 “Export Administration Regulations (EAR),” Bureau of Industry and Security, <https://www.bis.doc.gov/>

index.php/regulations/export-administration-regulations-ear.

- 21 Daryl Kimball, “The Wassenaar Arrangement at a Glance,” Arms Control Association, Last reviewed February 2022, <https://www.armscontrol.org/factsheets/wassenaar>.
- 22 “Nuclear Suppliers Group - Documents,” Nuclear Suppliers Group, <https://nuclearsuppliersgroup.org/en/nsg-documents>.
- 23 Missile Technology Control Regime, *Equipment, Software and Technology Annex* (Paris: MTCR, October 2022), https://mtcr.info/wordpress/wp-content/uploads/2022/10/MTCR-TEM-Technical_Annex_2022-10-21-Final.pdf.
- 24 “Australia Group Common Control List Handbooks,” The Australia Group, <https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/controlisthandbooks.html>.
- 25 Bureau of Industry and Security, “Implementation of Certain New Controls on Emerging Technologies Agreed at Wassenaar Arrangement 2019 Plenary,” Federal Register, October 5, 2020, <https://www.federalregister.gov/documents/2020/10/05/2020-18334/implementation-of-certain-new-controls-on-emerging-technologies-agreed-at-wassenaar-arrangement-2019>.
- 26 Bureau of Industry and Security, “Review of Controls for Certain Emerging Technologies,” Federal Register, November 19, 2018, <https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies>.
- 27 The 14 categories are: 1) Biotechnology; 2) Artificial Intelligence; 3) Position, Navigation, and Timing Technology; 4) Microprocessor Technology; 5) Advanced Computing Technology; 6) Data Analytics Technology; 7) Quantum Information and Sensing Technology; 8) Logistics Technology; 9) Additive Manufacturing; 10) Robotics; 11) Brain-computer interfaces; 12) Hypersonics; 13) Advanced materials; and 14) Advanced surveillance technologies.
- 28 Bureau of Industry and Security, “Implementation of Certain 2021 Wassenaar Arrangement Decisions on Four Section 1758 Technologies,” Federal Register, August 15, 2022, <https://www.federalregister.gov/documents/2022/08/15/2022-17125/implementation-of-certain-2021-wassenaar-arrangement-decisions-on-four-section-1758-technologies>.
- 29 Fast Track Action Subcommittee on Critical and Emerging Technologies of the National Science and Technology Council, *Critical and Emerging Technologies List Update* (Washington, DC: The White House, 2022), <https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf>.
- 30 Ibid.
- 31 Tongele N. Tongele et al., “Emerging Technology Controls” (presented at the BIS 2022 Update Conference on Export Controls and Policy, Washington, DC, June 29, 2022), <https://www.bis.doc.gov/index.php/documents/2022-update-conference/3073-rev3-emerging-tech-update-2022-section-1758-controls-tongele/file>.
- 32 Fast Track Action Subcommittee on Critical and Emerging Technologies of the National Science and Technology Council, *Critical and Emerging Technologies List Update*.
- 33 “FACT SHEET: President Biden Signs Executive Order to Ensure Robust Reviews of Evolving National Security Risks by the Committee on Foreign Investment in the United States,” The White House, September 15, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/15/fact-sheet-president-biden-signs-executive-order-to-ensure-robust-reviews-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states/>; and “The Committee on Foreign Investment in the United States (CFIUS),” U.S. Department of the Treasury, <https://home.treasury.gov/>

policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius.

- 34 Executive Office of the President, “America’s Supply Chains,” Federal Register, March 1, 2021, <https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains>.
- 35 Executive Office of the President, “Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States,” Federal Register, September 20, 2022, <https://www.federalregister.gov/documents/2022/09/20/2022-20450/ensuring-robust-consideration-of-evolving-national-security-risks-by-the-committee-on-foreign>. For more on Executive Order 14017, see Executive Office of the President, “America’s Supply Chains,” Federal Register, March 1, 2021, <https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chain>.
- 36 Emily Benson, Francesca Ghiretti, and Daniel Elizalde, “Transatlantic Approaches to Outbound Investment Screening,” CSIS, *CSIS Commentary*, January 17, 2023, <https://www.csis.org/analysis/transatlantic-approaches-outbound-investment-screening>.
- 37 Fast Track Action Subcommittee on Critical and Emerging Technologies, *Critical and Emerging Technologies List Update*.
- 38 “National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems,” The White House, May 4, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/>.
- 39 Ibid.
- 40 Joe Williams and Max A. Cherney, “Biden’s Push for New Quantum Controls Has One Big Problem: Nobody Knows Where to Draw the Line,” Protocol, November 2, 2022, <https://www.protocol.com/enterprise/quantum-computing-export-controls>.
- 41 U.S. Library of Congress, Congressional Research Service, *Defense Primer: Quantum Technology* by Kelley M. Saylor (2022), <https://crsreports.congress.gov/product/pdf/IF/IF11836>.
- 42 Ibid.
- 43 Ibid.
- 44 Emerging Technology from the arXiv, “How a Quantum Computer Could Break 2048-Bit RSA Encryption in 8 Hours,” *MIT Technology Review*, April 2, 2020, <https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/>.
- 45 Peter Clarke, “Quantum Market Has 13% CAGR as Supply Chain Forms,” eeNews Europe, February 23, 2023, <https://www.eenewseurope.com/en/quantum-market-has-13-cagr-as-supply-chain-forms/>.
- 46 World Economic Forum, *State of Quantum Computing: Building a Quantum Economy* (Geneva: WEF, September 2022), <https://www.weforum.org/reports/state-of-quantum-computing-building-a-quantum-economy/>; and Yole Intelligence, *Quantum Technologies 2023* (Lyon-Villeurbanne, France: Yole Group, February 2023), <https://www.yolegroup.com/product/report/quantum-technologies-2023/>.
- 47 Edward Parker et al., *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology* (Santa Monica, CA: RAND Corporation, 2022), https://www.rand.org/pubs/research_reports/RRA869-1.html.
- 48 “Betting Big on Quantum,” McKinsey & Company, September 13, 2022, <https://www.mckinsey.com/featured-insights/sustainable-inclusive-growth/chart-of-the-day/betting-big-on-quantum>.

- 49 John Russell, "China Expands Quantum Computing Development Push, Says Report," HPCwire, October 6, 2022, <https://www.hpcwire.com/2022/10/06/china-expands-quantum-computing-development-push-says-report/>.
- 50 "National Security Memorandum on Promoting United States Leadership," The White House.
- 51 Yan Bao et al., "Factoring Integers with Sublinear Resources on a Superconducting Quantum Processor," *arXiv:2212.12372 [quant-ph]*, Cornell University (December 2022), <https://doi.org/10.48550/arXiv.2212.12372>.
- 52 "Quantum Computing and Communications: Status and Prospects," U.S. Government Accountability Office, October 20, 2021, <https://www.gao.gov/products/gao-22-104422>.
- 53 Ibid.
- 54 Stefan Modrich and David DiMolfetta, "White House Mulling New Restrictions on AI, Quantum Equipment to China," S&P Global, October 24, 2022, <https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/white-house-mulling-new-restrictions-on-ai-quantum-equipment-to-china-72609040>.
- 55 "Export Controls for Quantum Computers -- View Rule," Office of Management and Budget, Office of Information and Regulatory Affairs, August 2021, <https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202104&RIN=0694-AH75#:-:text=BIS%20is%20proposing%20to%20add,control%20components%20and%20measurement%20devices>.
- 56 Williams and Cherney, "Biden's Push for New Quantum Controls Has One Big Problem: Nobody Knows Where to Draw the Line."
- 57 Brody Ford, "Quantum Computing Export Controls Discussed by IBM, Biden Administration," *Bloomberg*, November 9, 2022, <https://www.bloomberg.com/news/articles/2022-11-09/ibm-had-talks-with-biden-administration-on-quantum-controls>.
- 58 Ibid.
- 59 Dan Garisto, "Quantum Computers Won't Break Encryption Just Yet," Protocol, July 22, 2022, <https://www.protocol.com/manuals/quantum-computing/quantum-computers-wont-break-encryption-yet>.
- 60 Davide Castelvecchi, "Are Quantum Computers about to Break Online Privacy?" *Scientific American*, January 10, 2023, <https://www.scientificamerican.com/article/are-quantum-computers-about-to-break-online-privacy/#:-:text=Researchers%20typically%20estimate%20that%20it,data%E2%80%94faster%20than%20ordinary%20computers>.
- 61 National Institute of Standards and Technology, "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms," Press release, July 7, 2022, <https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms>.
- 62 Anton Shilov, "China's Origin Quantum Delivers a Commercial 24-Qubit Quantum Computer," Tom's Hardware, February 2, 2023, <https://www.tomshardware.com/news/chinas-origin-quantum-delivers-commercial-24-qubit-quantum-computer>.
- 63 Parker et al., *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology*.
- 64 David G. Cory, Amr F. Fahmy, and Timothy F. Havel, "Ensemble quantum computing by NMR spectroscopy," *Proceedings of the National Academy of Sciences* 94, no. 5 (1997): 1634-39.
- 65 Alvaro Ballon, "Trapped Ion Quantum Computers," PennyLane, August 2022, <https://pennylane.ai/qml/>

demos/tutorial_trapped_ions.html.

- 66 National Academies of Sciences, Engineering and Medicine, *Quantum Computing: Progress and Prospects*, eds. Emily Grumbling and Mark Horowitz (Washington, DC: The National, <https://doi.org/10.17226/25196>).
- 67 Ibid.
- 68 Sam Howell, “To Restrict, or Not to Restrict, That Is the Quantum Question,” *Lawfare*, May 1, 2023, <https://www.lawfareblog.com/restrict-or-not-restrict-quantum-question>.
- 69 Semiconductor Industry Association, *2021 State of the U.S. Semiconductor Industry* (Washington, DC: SIA, January 2022), <https://www.semiconductors.org/wp-content/uploads/2021/09/2021-SIA-State-of-the-Industry-Report.pdf>.
- 70 Ibid.
- 71 Antonio Varas et al., *Strengthening the Global Semiconductor Supply Chain in an Uncertain Era* (Washington, DC: SIA, April 2021), <https://www.semiconductors.org/strengthening-the-global-semiconductor-supply-chain-in-an-uncertain-era/>.
- 72 Ibid.
- 73 Ibid.
- 74 Eun-jin Kim, “South Korea’s Share Problematically Low in Global Fabless Market,” *BusinessKorea*, April 7, 2022, <http://www.businesskorea.co.kr/news/articleView.html?idxno=90422>.
- 75 Yimou Lee, Norihiko Shirouzu, and David Lague, “Taiwan Chip Industry Emerges as Battlefield in U.S.-China Showdown,” *Reuters*, December 27, 2021, <https://www.reuters.com/investigates/special-report/taiwan-china-chips/>.
- 76 Varas et al., *Strengthening the Global Semiconductor Supply Chain*.
- 77 Ming-Chin Monique Chu, “China’s Defence Semiconductor Industrial Base in an Age of Globalisation: Cross-Strait Dynamics and Regional Security Implications,” *Journal of Strategic Studies* (2023): 1-26, <https://doi.org/10.1080/01402390.2023.2164852>.
- 78 “Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit,” The White House.
- 79 Matthew Reynolds, “Assessing the New Semiconductor Export Controls,” CSIS, *CSIS Critical Questions*, November 3, 2022, <https://www.csis.org/analysis/assessing-new-semiconductor-export-controls>.
- 80 Gregory C. Allen, “Choking off China’s Access to the Future of AI,” CSIS, *CSIS White Paper*, October 11, 2022, <https://www.csis.org/analysis/choking-chinas-access-future-ai>.
- 81 “U.S. Imposes Additional Export Controls Restrictions on Advanced Computing and Semiconductor Manufacturing Items,” Covington & Burling LLP, October 10, 2022, <https://www.cov.com/en/news-and-insights/insights/2022/10/us-imposes-additional-export-controls-restrictions-on-advanced-computing-and-semiconductor-manufacturing-items>.
- 82 Andrew K. McAllister et al., “Commerce Department Rolls Out Measures to Strengthen Export Controls on China,” Holland & Knight, October 21, 2022, <https://www.hklaw.com/en/insights/publications/2022/10/commerce-department-rolls-out-measures-to-strengthen-export-controls#:~:text=ECCN%203B090%20%E2%80%93%20certain%20semiconductor%20manufacturing,a>.
- 83 Gregory C. Allen, Emily Benson, and Margot Putnam, “Japan and the Netherlands Announce Plans for

- New Export Controls on Semiconductor Equipment,” CSIS, *CSIS Commentary*, April 10, 2023, <https://www.csis.org/analysis/japan-and-netherlands-announce-plans-new-export-controls-semiconductor-equipment>.
- 84 Gregory C. Allen, “China’s New Strategy for Waging the Microchip Tech War,” CSIS, *CSIS White Paper*, May 3, 2023, <https://www.csis.org/analysis/chinas-new-strategy-waging-microchip-tech-war>.
- 85 U.S. Congress, House, *Chips and Science Act*, HR 4346, 117th Congress, August 9, 2022, <https://www.congress.gov/bill/117th-congress/house-bill/4346>; and William Alan Reinsch and Thibault Denamiel, “The Chips and Science Act Guardrails’ Implications for the U.S. Trade Agenda,” CSIS, *CSIS Critical Questions*, April 13, 2023, <https://www.csis.org/analysis/chips-and-science-act-guardrails-implications-us-trade-agenda>.
- 86 U.S. Department of Commerce, “Commerce Department Outlines Proposed National Security Guardrails for Chips for America Incentives Program,” Press release, March 21, 2023, <https://www.commerce.gov/news/press-releases/2023/03/commerce-department-outlines-proposed-national-security-guardrails>.
- 87 Dashveenjit Kaur, “Semiconductor Revenue to Contract for the First Time in Four Years,” TechHQ, January 6, 2023, <https://techhq.com/2023/01/semiconductor-revenue-expected-to-contract-for-the-first-time-in-four-years-in-2023/>.
- 88 “Lam Research Warns of up to \$2.5 Bln Revenue Hit from U.S. Curbs on China Exports,” Reuters, October 19, 2022, <https://www.reuters.com/technology/lam-research-warns-up-25-bln-revenue-hit-us-curbs-china-exports-2022-10-19/>.
- 89 Yu Yifan. “KLA Estimates Up to \$900m Revenue Hit in 2023 from China Chip Ban,” Nikkei Asia, October 26, 2022, <https://asia.nikkei.com/Business/Tech/Semiconductors/KLA-estimates-up-to-900m-revenue-hit-in-2023-from-china-chip-ban>.
- 90 Max Cherney, “Tough Times for Toolmakers: How New China Trade Rules Could Indirectly Hurt Applied, Lam and KLA,” *Silicon Valley Business Journal*, February 21, 2023, <https://www.bizjournals.com/sanjose/news/2023/02/21/how-new-china-trade-rules-could-hurt-tool-makers.html>.
- 91 Dylan Patel. “China and USA Are Officially at Economic War - Technology Restriction Overview.” SemiAnalysis, October 8, 2022, <https://www.semianalysis.com/p/china-and-usa-are-officially-at-economic>.
- 92 Eun-jin Kim, “Samsung’s and SK Hynix’s Sales in China Drop in Q3,” *BusinessKorea*, November 23, 2022, <http://www.businesskorea.co.kr/news/articleView.html?idxno=104639#:-:text=China%20accounted%20for%209.64%20percent,22>.
- 93 “Server Memory - the World’s Largest Data Centers Rely on Kingston Server Memory,” Kingston Technology Company, <https://www.kingston.com/en/memory/server-memory>.
- 94 Reddy G. Sreenivasa, “5 Sectors That Benefited Most from Server Hosting Services,” Medha Cloud, June 8, 2020, <https://medhacloud.com/5-sectors-benefited-most-server-hosting-services/>.
- 95 Terri Enborg, “US Semiconductor Manufacturing & Chips Act,” PRIDE Industries, July 28, 2022, <https://www.prideindustries.com/our-stories/us-semiconductor-manufacturing-and-the-chips-act>.
- 96 Antonio Varas and Raj Varadarajan, “How Restricting Trade with China Could End US Semiconductor Leadership,” BCG Global, March 9, 2020, <https://www.bcg.com/publications/2020/restricting-trade-with-china-could-end-united-states-semiconductor-leadership>.
- 97 Derek Yan and Cole Wenner, “US Export Control - Impact & Opportunity for China’s Semiconductor Industry,” KraneShares, November 1, 2022, <https://kraneshares.com/us-export-control-impact-opportunity-for-chinas-semiconductor-industry/>.

- 98 Evelyn Cheng, “Venture Capitalists Are Betting on a Part of China’s Chip Industry Safe from U.S. Bans,” CNBC, October 27, 2022, <https://www.cnbc.com/2022/10/28/foreign-investment-funds-bet-on-a-us-proof-china-chip-industry.html>.
- 99 Robyn Mak, “Taiwan Digs Trenches in Battle for Chip Talent,” Reuters, August 16, 2022, <https://www.reuters.com/breakingviews/taiwan-digs-trenches-battle-chip-talent-2022-08-17/>.
- 100 Howell, “To Restrict, or Not to Restrict, That Is the Quantum Question.”
- 101 Eleanor Olcott, Demetri Sevastopulo, and Qianer Liu, “Chinese AI Groups Use Cloud Services to Evade US Chip Export Controls,” *Financial Times*, March 8, 2023, <https://www.ft.com/content/9706c917-6440-4fa9-b588-b18fbc1503b9>; and Kif Leswing, “Meet the \$10,000 Nvidia Chip Powering the Race for A.I.” CNBC, February 23, 2023, <https://www.cnbc.com/2023/02/23/nvidias-a100-is-the-10000-chip-powering-the-race-for-ai-.html>.
- 102 U.S. Library of Congress, Congressional Research Service, *Defense Primer: Emerging Technologies* by Kelley M. Saylor (2022), <https://crsreports.congress.gov/product/pdf/IF/IF11105>.
- 103 “About Artificial Intelligence,” National Artificial Intelligence Initiative Office, <https://www.ai.gov/about/#ABOUT-ARTIFICIAL-INTELLIGENCE>.
- 104 PR Newswire, “\$422.37+ Billion Global Artificial Intelligence (AI) Market Size Likely to Grow at 39.4% CAGR During 2022-2028,” *Bloomberg*, June 27, 2022, <https://www.bloomberg.com/press-releases/2022-06-27/-422-37-billion-global-artificial-intelligence-ai-market-size-likely-to-grow-at-39-4-cagr-during-2022-2028-industry>.
- 105 U.S. Library of Congress, Congressional Research Service, “Defense Primer: Emerging Technologies.”
- 106 “What Is Generative AI?” McKinsey & Company, January 19, 2023, <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai>.
- 107 U.S. Library of Congress, Congressional Research Service, “Defense Primer: Emerging Technologies.”
- 108 Greg Allen and Taniel Chan, *Artificial Intelligence and National Security* (Cambridge, MA: Belfer Center for Science and International Affairs, July 2017), <https://www.belfercenter.org/publication/artificial-intelligence-and-national-security>.
- 109 “Overview of the International Trade Administration Support for Artificial Intelligence Industry,” International Trade Administration, Department of Commerce, <https://www.trade.gov/artificial-intelligence>.
- 110 “Bureau of Export Administration, *Critical Technology Assessment of the U.S. Artificial Intelligence Sector*” (Washington, DC: Department of Commerce, August 1994), <https://www.bis.doc.gov/index.php/documents/technology-evaluation/33-critical-technology-assessment-of-u-s-artificial-intelligence-1994/file>; and Tongele et al., “Emerging Technology Controls.”
- 111 Fast Track Action Subcommittee on *Critical and Emerging Technologies*, *Critical and Emerging Technologies List Update*..
- 112 “Artificial Intelligence (AI) Is One Thing, but Computer Hardware to Run Algorithms Plays a Part, Too,” *Military & Aerospace Electronics*, October 1, 2019, <https://www.militaryaerospace.com/computers/article/14067743/artificial-intelligence-computer-hardware-algorithms>.
- 113 Saif M. Khan and Alexander Mann, *AI Chips: What They Are and Why They Matter* (Washington, DC: Center for Security and Emerging Technology, 2020), <https://cset.georgetown.edu/publication/ai-chips-what-they-are-and-why-they-matter/>.

- 114 “arXiv,” Cornell University, <https://arxiv.org>.
- 115 “Industry Officials, Advocates Warn BIS against BCI Tech Export Controls,” *Export Compliance Daily*, February 21, 2023, https://exportcompliancedaily.com/article/view?search_id=679445&p=1&id=1511325&BC=bc_646cc89a9c014.
- 116 Olcott, Sevastopulo, and Liu, “Chinese AI Groups Use Cloud Services to Evade US Chip Export Controls.”
- 117 Margot Putnam and Emily Benson, “Export Controls and Intangible Goods,” CSIS, *CSIS Critical Questions*, April 11, 2023, <https://www.csis.org/analysis/export-controls-and-intangible-goods>.
- 118 Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit,” The White House.
- 119 “Executive Order on Advancing Biotechnology and Biomanufacturing Innovation for a Sustainable, Safe, and Secure American Bioeconomy,” The White House, September 12, 2022, <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/12/executive-order-on-advancing-biotechnology-and-biomanufacturing-innovation-for-a-sustainable-safe-and-secure-american-bioeconomy/>.
- 120 CSIS interview conducted on a non-attribution basis. Spring 2023.
- 121 Ibid.
- 122 The BIS Unverified List is a list of entities for which BIS could not verify the entities’ bona fides. According to BIS, “No license exceptions may be used for exports, reexports, or transfers (in-country) to Unverified parties. A statement must be obtained from such parties prior to shipping items not subject to a license requirement.” See: “Lists of Parties of Concern,” Bureau of Industry and Security, Department of Commerce, <https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern#:~:text=Unverified%20List,subject%20to%20a%20license%20requirement..>
- 123 “China’s Collection of Genomic and Other Healthcare Data from America: Risks to Privacy and U.S. Economic and National Security,” The National Counterintelligence and Security Center, February 2021, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf; and Marianne Kolbasuk McGee, “NCSC Warns of China’s Efforts to Collect US DNA Data,” *Data Breach Today*, February 3, 2021, <https://www.databreachtoday.com/ncsc-warns-chinas-efforts-to-collect-us-dna-data-a-15920>.
- 124 Ian Cohen, “Industry Officials, Advocates Warn BIS Against BCI Tech Export Controls,” *Export Compliance Daily*, February 3, 2021, <https://exportcompliancedaily.com/article/2023/02/21/industry-officials-advocates-warn-bis-against-bci-tech-export-controls-2302170030>.
- 125 Ibid.
- 126 Ibid.
- 127 Julian E. Barnes, “U.S. Warns of Efforts by China to Collect Genetic Data,” *New York Times*, October 22, 2021, <https://www.nytimes.com/2021/10/22/us/politics/china-genetic-data-collection.html>.
- 128 Sui-Lee Wee, “China Uses DNA to Track Its People, With the Help of American Expertise,” *New York Times*, February 21, 2019, <https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html>.
- 129 The White House, *National Security Strategy*.
- 130 Mark Scott, “Cambridge Analytica Helped ‘Cheat’ Brexit Vote and US Election, Claims Whistleblower,” *Politico*, March 27, 2018, <https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump>

- britain-data-protection-privacy-facebook/; and Philip N. Howard, Samuel Woolley, and Ryan Calo, “Algorithms, Bots, and Political Communication in the US 2016 Election: The Challenge of Automated Political Communication for Election Law and Administration,” *Journal of Information Technology & Politics* 15, no. 2 (2018): 81-93, <https://www.tandfonline.com/doi/full/10.1080/19331681.2018.1448735>.
- 131 Ronen Bergman and Mark Mazzetti, “The Battle for the World’s Most Powerful Cyberweapon,” *New York Times*, January 28, 2022, <https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html>.
- 132 Jon Allsop, “Around the World in (at Least) Eight Court Cases Involving Pegasus and the Press,” *Columbia Journalism Review*, February 14, 2023, https://www.cjr.org/the_media_today/pegasus_spyware_court_cases.php.
- 133 Bergman and Mazzetti, “The Battle for the World’s Most Powerful Cyberweapon.”
- 134 Stephen Shankland, “Pegasus Spyware and Citizen Surveillance: Here’s What You Should Know,” CNET, July 19, 2022, <https://www.cnet.com/tech/mobile/pegasus-spyware-and-citizen-surveillance-what-you-need-to-know/>.
- 135 Ottavio Marzocchi and Martina Mazzini, *Pegasus and Surveillance Spyware* (Strasbourg, France: European Parliament, May 2022), [https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA\(2022\)732268_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf).
- 136 Bureau of Industry and Security, “Implementation of Certain New Controls on Emerging Technologies Agreed at Wassenaar Arrangement 2019 Plenary.”
- 137 Ibid.
- 138 “FACT SHEET: President Biden Signs Executive Order to Prohibit U.S. Government Use of Commercial Spyware that Poses Risks to National Security,” The White House, March 27, 2023, <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/>.
- 139 The U.S. Department of the Treasury defines sensitive personal data by identifying 10 categories of data that might pose national security threats. These categories include data which has the capacity to impact certain groups of people, is bulk collected on at least one million people, or is collected on greater than a million people for the purposes of a U.S. business’ primary financial objectives. See: “Fact Sheet: Final CFIUS Regulations Implementing FIRRMA,” Office of Public Affairs, Department of Treasury, January 13, 2020, <https://home.treasury.gov/system/files/206/Final-FIRRMA-Regulations-FACT-SHEET.pdf>.
- 140 Office of Investment Security, “Provisions Pertaining to Certain Investments in the United States by Foreign Persons,” Federal Register, January 17, 2020, <https://home.treasury.gov/system/files/206/Part-800-Final-Rule-Jan-17-2020.pdf>.
- 141 Putnam and Benson, “Export Controls and Intangible Goods.”
- 142 Gregory C. Allen, Emily Benson, and William A. Reinsch, “Improved Export Controls Enforcement Technology Needed for U.S. National Security,” CSIS, *CSIS White Paper*, November 30, 2022, <https://www.csis.org/analysis/improved-export-controls-enforcement-technology-needed-us-national-security>.

COVER PHOTO MANDEL NGAN/AFP/GETTY IMAGES

CSIS | CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW

Washington, DC 20036

202 887 0200 | www.csis.org