MAY 2024

Beyond Economics

How U.S. Policies Can Undermine National Security Goals

By Thibault Denamiel, Taylar Rajic, William A. Reinsch, James A. Lewis, and Julia Brock

Introduction

Gaining and maintaining leadership in technology and innovation is set to be a key feature of global competition throughout the twenty-first century. With today's intermingling of economic competitiveness and defense, staying ahead of the technology curve is a cornerstone of national security. The United States, to further its geopolitical interests and maintain a strong domestic economy, must approach every aspect of economic and trade policy through the lens of global technology competition.

U.S. secretary of state Antony Blinken stated that the administration under President Joe Biden has **recognized** that technology "is profoundly a source of national strength." Renewed government investment and tightening rules around cross-border technology transfers reflect an understanding of the sector's significance to global competition. Nevertheless, while the administration has promoted large-scale investments in U.S. critical and emerging technology (CET) capabilities, some of its current economic and trade policies are undercutting the U.S. technology sector's potential and undermining the country's long-term national security interests. The administration's current approach to antitrust also discounts the landscape of competition between China and the United States and may jeopardize U.S. advancements in emerging technologies, which could cede the advantage to China and other foreign competitors.

In this paper, the authors aim to shed light on the principal policy shortcomings that hobble the United States' ability to remain a leader in technology innovation and production. The paper highlights several areas of improvement, including ongoing antitrust cases, digital trade and competition policy, industrial policy guardrails, and novel economic security measures around CETs. It also identifies concrete pathways to address these issues.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

How the U.S. Tech Ecosystem Supports the Country's National Security Apparatus

U.S. technological leadership is an essential element of the nation's superpower status. The country's ability to remain ahead of the global race for scientific and industrial advancements is a cornerstone of its national security. **Semiconductors**, along with a range of other cutting-edge technologies, are the crucial drivers of every major U.S. defense system or platform. The **2022 National Defense Strategy** recognizes that expeditious and widespread adoption of commercial technologies by the military is paramount and the Defense Innovation Unit (DIU) stated in a **2022 report** that it is critical "to gain and maintain operational advantage over competitors," and the DIU has recently adopted commercial solutions for everything from satellite maneuverability to pilot simulation training. As with many elements of the defense industrial base, the government relies on private businesses to develop and manufacture these critical technologies. For example, **Advanced Micro Devices** and **Intel** lead the world in producing field-programmable gate arrays (FPGAs)—circuit technologies with a wide range of defense applications in sensing, electronic warfare, and data security. Semiconductors for F-35 fighter jets are produced by BAE Systems in New Hampshire, the recent recipient of a **$35 million** CHIPS and Science Act grant.

The United States maintains its leadership through robust research and development (R&D) efforts in both the public and private sectors. Prominent rankings show the United States is home to three of the top five globally renowned **research universities** and approximately 1,000 **venture capital firms**. In addition, the Department of Energy operates 17 **national laboratories**. Another ranking shows 81 of the world's largest **technology companies** are based in the United States, far outpacing any other nation, with China having only one company (Tencent Holdings) in the top 20. In the race for tech innovation, the United States has clearly maintained its position as the global leader. But with technological advancements and increased competition with China in emerging tech, such as quantum and artificial intelligence (AI), federal policy must be assessed regularly to ensure the United States can spur the entrepreneurship and R&D efforts foundational to the strength of the country's tech sector. Since the 1990s, the private sector has been the primary driver of this innovation, **surpassing** federal investments in technology. In 2021, U.S. businesses invested **$591 billion** in R&D, accounting for 74.9 percent of the national total investment in R&D for that year. The federal government's share of national R&D investment for 2021 was just $147.5 billion, or 18.7 percent of the national total.

Advancements in technology have helped the United States become a superpower. Investments in aerospace and defense technologies have established superior U.S. military capabilities and have underpinned U.S. power globally for decades. Technological advancements made before the Persian Gulf War had a **transformative** impact on the use of technology in warfare, including satellite surveillance systems, the Global Positioning System (GPS), and information technology for reconnaissance, surveillance, and intelligence gathering. Deployment of these technologies transcended their use on the battlefield to become essential in everyday life both in the United States and abroad.

Now, CETs are becoming a focus for foreign policy because they promise to transform both how economies grow and how nations defend themselves. The U.S. technology sector's ability to innovate and flourish is directly tied to the country's ability to ensure its national security. The U.S. technology sector plays an essential role in providing both hardware and software to the national security

community. Tech giants like Amazon, Microsoft, and Google provide digital infrastructure such as cloud security and updates to legacy federal systems to promote a safe and secure online environment. Amazon Web Services (AWS) offers cloud computing services, such as **GovCloud**, designed to meet strict security thresholds to national security agencies that need to host sensitive data and applications in the cloud. **IBM** also provides a cyber response training facility in Washington, D.C., aimed to improve incident response capabilities to protect federal systems. Federal civilian networks require secure and reliable information technology systems to safeguard data that ensure national security and contain the private information of millions of U.S. citizens. Critical infrastructure, another key component of safeguarding national security, relies heavily on a robust digital infrastructure to protect the daily functioning of key critical sectors.

Policy Areas

ANTITRUST

The United States, to preserve its edge in the current technology competition with China, needs to maintain its strong innovation ecosystem. The question of antitrust is at the center of the policy debate over how to encourage innovation. Now there are growing **concerns** that overregulating U.S. tech companies will stifle the innovative culture that makes the United States a global technology leader.

> *Now, CETs are becoming a focus for foreign policy because they promise to transform both how economies grow and how nations defend themselves. The U.S. technology sector's ability to innovate and flourish is directly tied to the country's ability to ensure its national security.*

The **Sherman Act**, **Federal Trade Commission Act**, and **Clayton Act**—the core U.S. antitrust statutes intended to regulate business practices to promote competition and protect consumers—are enforced by the Federal Trade Commission (FTC) and Department of Justice (DOJ). Recent antitrust lawsuits by the **DOJ** and **FTC** reflect growing concern in those agencies and among some analysts about monopolization in the U.S. technology industry and the potential effects this could have on innovation.

Through recent **lawsuits**, the FTC is attempting to address alleged illegal monopolies and companies' desire to harness emerging technologies solely to their benefit. The FTC argues that issues around **self-preferencing** of products and applications, for example, have allegedly blocked competitors from entering the digital services market. FTC chair Lina Khan **expressed** her skepticism at the concept of tech "national champions," citing the failures of Boeing as an example where lack of competition disincentivized the company to spend on improving safety and innovation. She has also cited the FTC's **blocking** of Lockheed Martin's acquisition of Aerojet Rocketdyne as a strategy to maintain fair competition in a sector critical to national security and defense. These concerns are now being aimed at the tech sector for its role in maintaining a critical line of defense in national security and ensuring an environment of competition remains to promote innovation and enrich the market. Khan's critiques, however, have also been brought into **question** for their validity and whether they demonstrate lack of

understanding of national security considerations and market dynamics. Her efforts are part of a larger antitrust effort by the Biden administration to mitigate what it sees as regulators' **failure** to reign in the rise of Big Tech.

DOJ has raised similar concerns in its investigations of **Apple**, aimed at the company's market control in both its software and hardware, which DOJ views as anticompetitive. Apple controls approximately **58 percent** of U.S. smartphone sales and has a significant share of the mobile app market. The mobile app market is effectively a duopoly between Apple and Google, which have dominated by defaulting their app stores to their respective smartphones. These issues were highlighted in the **European Union's actions** to fine Apple for banning app developers from offering cheaper subscriptions to customers who want to use their services outside Apple's App Store. Japan's antitrust regulators have also maintained that there is a **clear duopoly** of the mobile app market, that developers can create iOS apps only by selling them through the App Store, and that consumers rarely switch platforms due to familiarization and self-preferencing. Efforts by Apple's competitors and **lawsuits** in the United States also emphasize the concern that the App Store is designed to completely shut out competition.

As high tech becomes an increasingly important part of U.S. national defense and as China's competitive challenges grow, it is important to take a close look at how other federal government efforts impact U.S. national security, including attempts by the FTC and DOJ to regulate Big Tech. Although in the past these national giants have been at the forefront of U.S. technological innovation, greater scrutiny of their R&D spending and practice surrounding patent numbers, and whether this is reflected in product advancement and output, is needed to ensure the market remains competitive—an instrumental part of keeping the U.S. tech sector a step ahead. The most common metrics for measuring the success of innovation are patent holdings and R&D spending; Big Tech generally leads the pack in both.

Some **argue** that these FTC and DOJ actions are targeting the wrong industries and that Big Tech is both competitive and innovative. Amazon spent the most of any U.S. company on R&D (**$73.2 billion**) in 2022, followed by Alphabet, which spent $35.9 billion. Big Tech also has a commanding lead when it comes to new patents. IBM holds the most **patents** in the United States. Other companies, such as Amazon, Google, Apple, and Microsoft, also promote innovation by rewarding employees with in-house **patent recognition programs**, regardless of whether the patents are approved or not.

Despite Big Tech clearly leading the U.S. government in both R&D spending and patent holdings, there is some **concern** this could be stifling innovation. **One study** suggests that when start-ups see the prospect of acquisition from larger firms, their innovation decreases despite having more access to funding, which could be stifling bolder ideas in order to take a safer approach that appears more profitable to potential investors and start-ups hoping to be bought out. However, breaking up Big Tech through an antitrust approach raises the question of whether the United States has the potential to innovate more than under its current model, which has so far proved very strong. It remains to be seen what effects of pending litigation and mixed public opinion on these issues have on efforts to break up Big Tech and if decades of technological innovation amount to less than hypothetically what could have been achieved with more domestic competition.

COMPETITION WITH CHINA

China, the primary U.S. competitor, directly supports its national giants and has helped them become globally competitive. China began **strengthening** its defense technology base in the 1980s and 1990s by investing in research and technology firms, investing in its tech workforce, and engaging in commercial espionage and **intellectual property (IP) theft**. These strategies continue to mark how China conducts business with Western commercial firms. Today, despite the United States maintaining an established global position in technology development, an Australian think tank claims (using debatable data) that China **leads** the world in developing 37 out of 44 CETs and has promoted policies to drive further innovation and promote technology i**ndependence** from the West. Despite these claims, the United States is clearly established as a global leader in technological innovation; what remains to be seen is how treatment of the U.S. domestic technology base and national giants will affect this position with China's approach to subsidizing its tech industry.

China's government supports its technology giants—including Huawei, SMIC, Alibaba, Tencent, and ZTE—to modernize and strengthen its commercial and defense sectors. China's **New Generation AI Development Plan** and its **Made in China 2025** plan are part of China's goal to invest in domestic innovation to develop technological self-reliance and compete with Western tech industries. In 2019, China **supported** Huawei through loans from national banks, and in 2022, China's estimated state financial support for Huawei alone was **$75 billion**. The Chinese government also **invested** $40 billion in state funds to boost the country's domestic semiconductor market in 2023.

In addition to government funding, China has used regulatory tools to promote independence from Western services and strengthen its tech companies. In 2021, for instance, Beijing issued new rules **regulating** internet platforms after China's State Administration for Market Regulation (SAMR) fined Alibaba **$2.8 billion** or anticompetitive behavior, and it **updated its Anti-Monopoly Law in 2022**. China's antitrust regulatory body is starkly **different** from that of the United States. Antitrust regulators in China are rarely challenged in their rulings. Further, antitrust agencies often follow the directives of the central government, and regulatory authorities are afforded a greater deal of flexibility. By contrast, any U.S. antitrust ruling would likely take several years to litigate. The long-term effect of China's antitrust policies on Chinese tech innovation remains to be seen, and increasing political strictures by the Chinese Communist Party may hamper innovation in China. Nevertheless, thus far, its approach has helped strengthen the country's technology innovation ecosystem vis-à-vis the United States.

Breaking up U.S. national champions—large companies that have become synonymous with U.S. know-how and support the country's greater national security interests—or unnecessarily limiting their ability to invest and innovate could limit U.S. ability to lead globally in emerging technologies like AI and quantum tech, leaving the country at risk of ceding this leadership position to China. Currently, the seven largest **AI companies** by market share are U.S. companies, including Alphabet, Microsoft, and Meta. The four leading global **quantum companies** are also U.S. national giants, including Google, Microsoft, and Amazon. The United States is leaning on national champion tech companies to pioneer development and commercialization of these technologies. Given China's increasing **competitiveness** in the tech sector, hobbling or breaking up these companies could set the United States back in its tech development competition with China.

Digital Policy

COMPETITION POLICY

The United States, unlike many economic partners and competitors, has not defined a clear policy on digital competition. The most assertive push from Congress in addressing the issue came after a **16-month investigation** by the House Judiciary Committee's Subcommittee on Antitrust, Commercial and Administrative Law, which ended in 2020. The investigation yielded five bills aimed narrowly at regulating technology companies, none of which became law. Several like-minded bills were introduced in the Senate, yielding similar results. The Klobuchar-Grassley **American Innovation and Choice Online Act**, for instance, would give federal antitrust agencies the authority to issue civil penalties and injunctions against online platforms ("covered platforms") (1) with at least 50 million monthly active users (or 100,000 business users), (2) with an annual market capitalization or U.S. net sales exceeding $550 billion, and (3) serving as a "critical trading partner" for its business users.

> *Breaking up U.S. national champions or unnecessarily limiting their ability to innovate could limit U.S. ability to lead globally in emerging technologies like AI and quantum tech, leaving the country at risk of ceding this leadership position to China.*

As Congress has been unable to pass meaningful legislation on digital competition, federal agencies have begun to chart their own path. Defining a U.S. approach that would adequately protect consumers at home and abroad while ensuring fair treatment for providers has therefore been problematic. The absence of a clear policy slows the development of a stable digital ecosystem in the United States.

This gap in policymaking creates two issues that speak to the importance of U.S. leadership in this space. First, it cedes first-mover advantage to other governments around the world that are free to decide the rules of a sector, which inherently have extraterritorial implications. Chief among them is the European Union's Digital Markets Act (DMA). The act identifies digital services that fall under its purview, defines characteristics that make a service provider a gatekeeper, creates rules and ex ante obligations for those gatekeepers, and establishes punishments if those obligations are not met. A previous **CSIS study** showed that EU regulations in the tech sector, such as the DMA and Digital Services Act, among others, would cost U.S. service providers an estimated $22–$50 billion in compliance.

Secondly, the absence of congressional action leaves U.S. states to chart their own path in this sector. In 2023 alone, seven state legislatures introduced competition-related legislation, continuing the trend of states attempting to tighten regulation in the digital space. These state-level efforts, in turn, may present additional challenges to ensuring federal leadership on the issue, which is necessary to guarantee that policies supporting the homegrown tech sector are designed and implemented with a whole-of-nation approach. A consortium of subnational policies, moreover, may increase the **regulatory burden** for tech actors, which, instead of abiding by a single law at the federal level, must simultaneously meet various sets of standards across states—not all of which are compatible.

Given the lack of direction, some parts of the Biden administration have pursued policies that undercut the interests of U.S. champions, while others have risen to these champions' defense. In December 2021, U.S. Secretary of Commerce Gina Raimondo **expressed** "serious concerns that these proposals will [the DMA would] disproportionately impact U.S.-based tech firms." Later, the Department of Commerce **formally lobbied** the EU Parliament in a letter sent in February 2022, calling on lawmakers to "use scoping criteria that do not discriminate against U.S. firms." In the 2023 National Trade Estimate (NTE), U.S. trade representative (USTR) Katherine Tai **classified** the DMA as a barrier to digital trade. Administration officials even sent a **letter of protest** to Brussels in early 2022, objecting to the DMA's targeting of U.S. companies and potential effect on technological innovation.

Despite these condemnations, the FTC and DOJ have worked closely with the European Commission via the **U.S.-EU Joint Technology Competition Policy Dialogue** (TCPD) on DMA implementation. Both agencies have sent officials to the European Union to assist with the process. This support from parts of the Biden administration is encouraging the implementation and enforcement of digital competition policies that disadvantage U.S. providers by imposing discriminatory compliance requirements.

Altogether, it appears the administration's progressive wing has taken the reins on digital competition policy. Secretary Raimondo, after becoming isolated over her opposition to the DMA, **fell silent** on the issue. This shift has been most evident in USTR's 2024 NTE, which **narrows the definition** of trade barriers by defining them as "government measures that unduly impede the international exchange of goods and services," instead of the previous year's broader definition, which characterized any government action that restricts trade, U.S. investment, or cross-border data flows as a barrier. In addition, the new NTE drops several restrictions on the cross-border transfer of data present in the previous year's estimate and makes no mention of the DMA, which was included in earlier versions.

TRADE

Digital trade is another area where the administration's internal disputes have put the United States at a disadvantage in plurilateral negotiations. In late October 2023, USTR suddenly **withdrew U.S. support** for digital trade negotiating objectives in a meeting of the Joint Statement Initiative (JSI) on Electronic Commerce at the World Trade Organization (WTO). These objectives include protection of cross-border data flows, prohibition of data localization mandates, and safeguarding of source code from forced disclosure to foreign governments. Given the importance of the WTO JSI in safeguarding U.S. interests in this sector and the negotiation's significance to economic allies and partners, USTR's withdrawal represents a significant setback in establishing rules in the e-commerce space, which will likely incur significant costs to U.S. tech firms aiming to grow abroad.

Digital trade negotiations have also suffered setbacks in U.S.-led forums. In November 2023, following the WTO JSI withdrawal, USTR **suspended talks** on some key digital trade aspects of its Indo-Pacific Economic Framework (IPEF) initiative. As with the WTO talks, the suspensions conflict with previous digital trade accomplishments enshrined in the United States-Mexico-Canada Agreement on trade, as well as the more recent U.S.-Japan Digital Trade Agreement, supporting the aforementioned U.S. policy objectives on data flows, localization mandates, and source codes disclosures. These failures in negotiating digital trade rules create an uneven terrain in which U.S. tech champions will need to abide by different—and potentially protectionist—standards of e-commerce that will limit their ability to conduct business.

INDUSTRIAL POLICY

The Biden administration's championing of industrial policy to spur technological advancements and support production of CETs represents a monumental shift in U.S. economic policy. The semiconductor sector exemplifies the U.S. government's turn to state-led investments. The CHIPS and Science Act allocates roughly **$200 billion** for public sector entities like the National Science Foundation and Department of Energy. On the private side, the CHIPS for America fund alone will provide roughly $50 billion over five fiscal years to **subsidize** investments in semiconductors using a competitive grant process. Under the fund, $39 billion **will go toward** general subsidization of investments that develop domestic manufacturing capability, and the remaining $11 billion will go toward advanced semiconductor R&D. Likewise, an advanced manufacturing investment tax credit **creates** a 25 percent investment tax credit for investments in semiconductor manufacturing and includes incentives for the manufacturing of semiconductors, as well as for manufacturing of the specialized tooling equipment required in the semiconductor manufacturing process. In addition to the federal government's efforts, several states have created analogous incentive programs for drawing investment. For instance, Ohio has **announced** "$2 billion of state grants, credits, and incentives to construct a new semiconductor manufacturing plant in Ohio."

> *These failures in negotiating digital trade rules create an uneven terrain in which U.S. tech champions will need to abide by different—and potentially protectionist—standards of e-commerce that will limit their ability to conduct business.*

The new U.S. turn to industrial policy to support critical sectors, including technology, could unlock capital to ensure the country remains ahead of the global competition, but it also creates novel roadblocks. For one, large industrial policy packages risk fraying relationships with allies and economic partners who believe the United States may be breaking the rules governing world trade to give domestic champions unfair advantages. Related to this issue is the potential for a spiraling subsidy war: as with other government-led investments, large U.S. government packages in the tech sector threaten to provoke a global subsidy race making nations' cash infusions in the relevant sectors increasingly inefficient. The European Union has already responded to the United States with its own **European Chips Act**, a piece of legislation that aims to boost the continent's semiconductor production from 10 percent to 20 percent of global capacity by 2030 and will allocate over €43 billion ($45.9 billion) toward chips until 2030. Moreover, aside from trade rules considerations, U.S. incentives may also run counter to other types of U.S. multilateral engagement. For instance, **global minimum taxation standards enshrined in Pillar Two** of the Organization for Economic Cooperation and Development (OECD) currently expose companies aiming to take advantage of the R&D tax credit to a top-up tax equal to the difference between Pillar Two's threshold and their tax rate—partially negating the incentive's ability to spur innovation.

Another hurdle to effective industrial policy is current local and federal environmental regulations that hinder building manufacturing centers critical to emerging technologies—such as semiconductor fabrication plants, or fabs. While these regulations may be necessary to lower the environmental impact

of proposed facilities—semiconductor facilities require large amounts of energy and fresh water and can produce several tons of hazardous waste every year—processes to secure governmental permits are both time-consuming and expensive. The President's Council of Advisors on Science and Technology **found** that the permitting process can take 12–18 months for large fab projects. Semiconductor fabs are also required to undergo an environmental assessment under the National Environmental Policy Act. If the assessment determines the project will have a significant environmental impact, then it must also go through an impact statement process. According to the **Council on Environmental Quality**, these take an average of 4.5 years to complete. These potential delays, which China's authoritarian system can avoid, hinder the United States' ability to undertake large-scale projects to enhance the production of CETs. The tech sector moves at a brisk pace, and lengthy timelines can have profound security and economic implications. Responsible acceleration of the permitting process for goods critical to national security through the creation of a dedicated fast-track process would mitigate issues associated with lengthy timelines and allow the United States to ensure its position as a leader in tech manufacturing.

> *The new U.S. turn to industrial policy to support critical sectors, including technology, could unlock capital to ensure the country remains ahead of the global competition, but it also creates novel roadblocks.*

Lastly, the U.S. turn to industrial policy exacerbates a problem that has already been a barrier to long-term U.S. economic growth—namely, worker shortages. Sustained government spending significantly increases demand for labor in targeted sectors, creating jobs the country simply does not have enough people to fill. A **recent study** by Deloitte revealed the labor shortage in the U.S. semiconductor industry could reach up to 90,000 workers over the next few years. Issues arising from a lack of specialized workers have already been evident from Taiwan Semiconductor Manufacturing Company's (TSMC) **difficulties** in building a **$40 billion fab** in Arizona. Industrial policy packages promoting the U.S. tech sector can work only if there are enough workers to support them. Barring stark changes in U.S. workforce development capabilities or immigration policy, labor is set to remain **insufficient**.

ECONOMIC SECURITY MEASURES

The Biden administration has also had to confront the increasing intermingling of economics and national security in its policy development. Once two parallel tracks, they now complement each other in the eyes of the U.S. government: economic statecraft tools support national security measures, and prosperity is defined by resilience. This turn has led to a significant expansion in tools at the disposal of the U.S. government, which, whether warranted by rising geopolitical tensions or not, are set to curb U.S. companies' ability to grow. Expanded export control rules, outbound investment screening mechanism proposals, and an executive order on data flows will transform the U.S. tech sector, building up barriers and limiting firms' ability to access the foreign markets they need to continue to grow.

EXPORT CONTROLS

Recognizing the national security threats posed by China's access to advanced technologies, including chips and the AI capabilities they support, the Biden administration has significantly expanded export control rules on semiconductors. On October 7, 2022, the Bureau of Industry and Security (BIS) issued rules meant to curtail the sale of chips and certain related technologies to Chinese firms. The rules spell out **nine new actions**, including the addition of advanced chips and manufacturing equipment items to the Commerce Control List (CCL) and the restriction of U.S. persons' ability to support the development or production of integrated circuits at certain semiconductor fabrication facilities located in China. On October 17, 2023, BIS **announced** revisions meant to address gaps in the previous year's controls. The revisions change the thresholds for which chips are covered by making performance density the primary parameter of interest, subject **43 additional countries** to expanded licensing requirements to combat circumvention via third-party nations, include additional manufacturing tools to the list of controlled equipment, and blacklist 13 Chinese AI firms deemed to threaten U.S. national security. An initial issue with the expanded controls lies in the Department of Commerce's limited enforcement capacity. The significant expansion of control rules without the commensurate expansion of BIS enforcement capabilities threatens pervasive circumvention, putting legitimate U.S. firms that abide by the new rules at a disadvantage. While BIS has already expanded its enforcement capabilities, with a fiscal year 2023 budget that increased by $50 million over the previous year, additional rules and personnel should be accompanied by increased investment in the agency. CSIS has already **argued** that data-driven digital technologies using AI and machine learning can and should play an integral role in enhancing BIS export control enforcement capabilities.

Expansion of semiconductor export controls presents a central dilemma for U.S. economic security policymaking: China is both the greatest long-term threat to national security and the largest customer for U.S. businesses. Depending on how the Department of Commerce handles licensing, U.S. and allied chipmakers are set to forgo a large amount of revenue by having their access to the Chinese market curtailed. From 2016 to 2020, financial filings of top U.S. chip companies show they derived roughly a third of their net revenue from sales to China. Lam Research, Applied Materials, and KLA have **provided** negative growth guidance for the quarter ending in June 2023 after warning they could stand to lose up to $5 billion worth of revenue from China in 2023 from the chip controls.

Aside from potential revenue losses, U.S. and allied chip firms also face the threat of being designed out of the semiconductor supply chain by China's homegrown champions, as well as third-country firms. Beijing has responded to sweeping U.S.-led semiconductor export curbs against China by seeking to "**de-Americanize**" its chip sector. One such design-out pathway China is pursuing includes leveraging advanced packaging techniques to develop chiplets, which may offer a route for producing high-performance chips not dependent on the astronomical investment to produce smaller chips. In addition, other countries may soon be able to fill the gaps left by U.S. and allied semiconductor firms.

If the United States ignores the design-out developments resulting from U.S. export control policy, Washington may find its semiconductor curbs increasingly irrelevant and subject to circumvention. This threat risks undercutting U.S. innovation in semiconductors, diminishing U.S. alignment with allies and partners on high technology, and propelling China's chip ambitions. Both revenue and design-out should also be taken into consideration as the U.S. government evaluates other export curbs on CETs—

such as quantum technologies, in which China is already **out-investing** (and potentially out-competing) the United States.

OUTBOUND INVESTMENT

The Biden administration's economic security policies have led to development of a brand-new tool intended to protect long-term U.S. interests by curbing China's access to emerging dual-use technologies. In early August 2023, President Biden signed **Executive Order 14105** to address "U.S. investments in certain national security technologies and products in countries of concern." The order directs the Treasury secretary to establish an outbound investment screening program for three types of sensitive technologies: (1) semiconductors and microelectronics, (2) quantum information technologies, and (3) AI. In the order's annex, the president specifically identifies China, along with Hong Kong and Macau special administrative regions, as a country of concern—highlighting the idea that the mechanism is aimed squarely at tackling national security threats emanating from China.

The mechanism's implementation is still being developed. Per the Department of the Treasury's **advance notice of proposed rulemaking** (ANPRM), covered transactions—a blanket term that applies to both prohibited and notifiable transactions—would include large-scale investments such as mergers and acquisitions , private equity, venture capital, greenfield, joint ventures, and certain debt financing schemes. Within semiconductors, the Department of the Treasury is considering banning investments in Chinese entities engaged in advanced design or manufacturing while simply requiring notification for less sophisticated integrated circuits. When it comes to quantum technologies, the Department of the Treasury is also **considering** banning investments in all identified subsets: quantum computers and components, certain quantum sensors, and quantum networking and networking systems. The ANPRM outlines a notification requirement for investments in AI systems with national security applications and is requesting comments on how to shape prohibitions for certain AI systems whose sole use is for military, intelligence, or surveillance purposes.

Given China's civil-military fusion doctrine, better monitoring of U.S. investments in the country will likely support policies designed to promote national security. Despite geopolitical tensions exerting downward pressure on U.S. investors' enthusiasm for China, the country remains a top destination for U.S. capital. In 2022, U.S. venture capital firms were involved in almost **600 deals** in China, totaling roughly $14.5 billion in value. Given investors' declining yet certainly extant interest in China, the ability to ban transactions should be exercised lightly to avoid denying the private sector growth opportunities that do not adversely impact U.S. national security. In addition, detractors of an outbound investment screening regime argue that multilateralizing the instrument, a key step for effective economic security measures, would be an uphill battle—though the European Union has recently considered taking a similar step. Given the Chinese government's willingness to subsidize critical industries, a mechanism curbing U.S. investment could simply change Chinese firms' financing sources rather than diminish their ability to acquire funding altogether.

DATA SECURITY EXECUTIVE ORDER

On February 28, 2024, the White House issued an Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, which aims to curb cross-border transfers that pose "an unacceptable risk to the national security of the United States." The new Biden administration policy aims to **tackle** a gap in national security policy as

entities or countries of concern can use sensitive personal information to illicit ends, such as curbing dissidents, activists, and journalists abroad; targeting misinformation campaigns at certain population subgroups; and spying or even blackmailing government personnel.

This new executive order directs the DOJ to issue regulations limiting U.S. companies from transferring or selling bulk data sets to covered persons or entities subject to the jurisdiction of countries of concern—namely, China, Russia, Iran, North Korea, Venezuela, and Cuba. The executive order includes six categories of sensitive personal data to the impending curbs: biometric identifiers, genomic data, personal identifiers, personal health data, personal financial data, and precise geolocation data. For each of these categories, the incoming government program to regulate data transfers will establish certain volume thresholds. Some classes of transactions will face bans altogether, while others will be prohibited unless they comply with additional requirements. Three classes of data transactions fall into the latter: employment, investor, and third-party vendor agreements.

Several concerns come with the new rules delineated in the ANPRM. For one, it remains unclear how the rules would cover third-country transfers. While the executive order classifies transactions based on their inherent characteristics and the threat of access by countries of concern or covered persons, their enforceability remains unclear. Although several U.S. technology companies transfer personal information across borders, the executive order would likely **affect** the business models of data brokers that profit from the bulk collection, aggregation, and sales of a wide spectrum of personal data. Lastly, prior to this action, U.S. firms had few restrictions hindering their data exports. So while the executive order is meant to minimize negative externalities, its effect depends on how the DOJ, along with other federal agencies, decides to implement and enforce its rules.

Recommendations and Conclusion

Maintaining the U.S. competitive edge in technology requires a whole-of-government approach to incentivizing innovation. Several adjustments may be made to current U.S. policy to ensure that the country's investments yield the most substantial results.

- **Move quickly to pass legislation on digital privacy and protecting the U.S. competition landscape, which must be considered through a national security lens.** Comprehensive legislation in these policy areas has so far failed to become law, ceding leadership to other economic blocs around the world. Failure to act is itself a national security problem.
- **Build a national security factor into antitrust analysis**. The DOJ and FTC should embed national security considerations into antitrust enforcement analytical models. In other words, the agencies should consider the effects on U.S. national security when proceeding with an antitrust complaint. Current dominant positions in the administration and Congress equate a tech company's size with the potential damage to competition and, therefore, the U.S. economy at large. Policymakers should reconsider whether that is the relevant criterion to estimate negative effects on consumers. Large companies that behave responsibly can enable the United States to meet its defense needs and national security priorities.
- **Establish fast-track processes to set up CET-related facilities**. Evaluating environmental impacts of new projects is a paramount consideration for activities related to the tech sector. However, given the urgency of scaling up U.S. capabilities in research and production of CETs,

review of projects related to sectors included in the White House CET list should receive its own fast-track process.

- **Continue exploring alternative pathways of multilateralizing economic security measures**. The Biden administration has rapidly expanded the U.S. economic security tool kit through new semiconductor export controls, a novel outbound investment mechanism, and the recent EO on data security. These measures require a multilateral approach to ensure their effectiveness and mitigate the design-out threat that unilateral action poses. Existing multilateral bodies, such as the Wassenaar Arrangement, were not made to confront today's challenges. Working with allies to find novel pathways of coordinating policy on both the promote and protect sides of the economic security coin, such as working together on CET supply chain diversification efforts or designing common outbound investment screening approaches, continues to be a critical consideration. Multilateralizing economic security measures would ensure the U.S. tech ecosystem is not further isolated by unilateral tools, which ultimately hobble their ability to grow.
- **Pursue a more ambitious trade agenda with economic partners, including a robust digital trade component**. U.S. digital trade engagement has been uneven and has led to a more challenging landscape where U.S. tech champions need to unilaterally abide by foreign e-commerce standards that may curtail their ability to conduct business effectively. Reaffirming a clear U.S. digital trade agenda and embedding it in future negotiations will enable U.S. companies to remain leaders in the sector, ensuring their ability to support national security.
- **Ensure industrial policy measures remain compliant with U.S. multilateral commitments such as WTO rules**. The aspiration to remain a tech leader comes with the responsibility to promote and abide by global norms around economic engagement. Some recent U.S. economic and trade policies have eroded the country's credibility as well as trust with its partners. The current U.S. policy direction is set to foster a more anarchic international economic landscape that will inevitably hinder homegrown companies' ability to conduct business abroad. This situation should be rectified.

Technology has played a central role in protecting the United States and will continue to do so throughout the twenty-first century. Recognizing its significance is key in today's landscape of global competition, and promoting policies to spur the sector's growth is a strategic imperative. The Biden administration must address several policy gaps to help the U.S. tech ecosystem better support national security. Resolving current shortcomings through effective approaches to antitrust, digital competition policy and trade, state-led investments, and economic security measures constitutes an important step in that direction. ■

Thibault Denamiel *is an associate fellow with the Scholl Chair in International Business at the Center for Strategic and International Studies (CSIS) in Washington, D.C.* ***Taylar Rajic*** *is a research associate with the Strategic Technologies Program at CSIS.* ***William A. Reinsch*** *holds the Scholl Chair in International Business at CSIS.* ***James A. Lewis*** *is a senior vice president and director of the Strategic Technologies Program at CSIS.* ***Julia Brock*** *is a program coordinator and research assistant with the Strategic Technologies Program at CSIS.*

The authors would like to thank ***John Strezewski*** *for his assistance in writing this paper.*

This report is made possible through generous support from the Software and Information Industry Association.