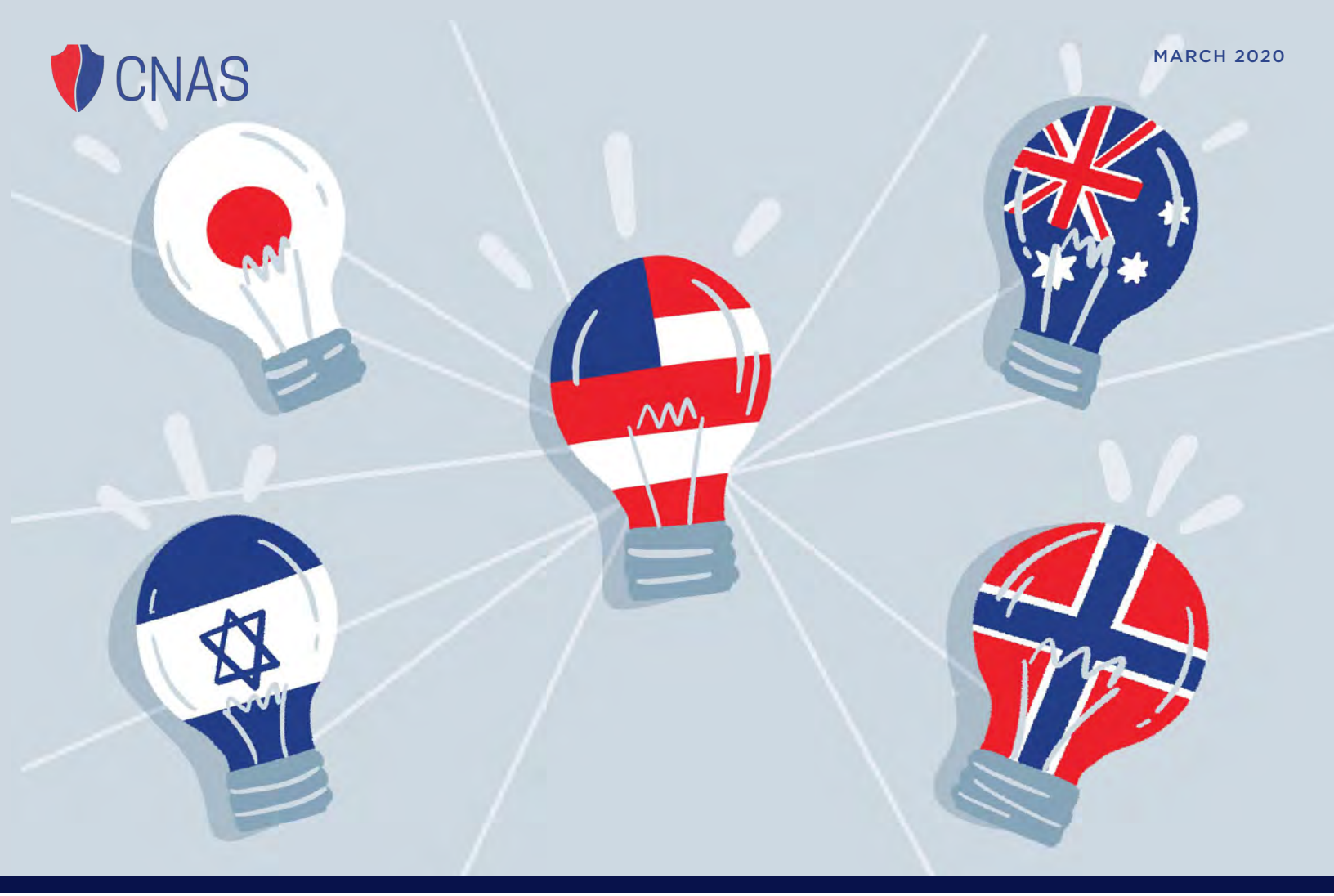
CNAS

MARCH 2020



Forging an Alliance Innovation Base

Daniel Kliman, Ben FitzGerald, Kristine Lee, and Joshua Fitt

America 2020 Competes

About the Author

Daniel Kliman is the Senior Fellow and Director of the Asia-Pacific Security Program at the Center for a New American Security (CNAS). He focuses on U.S. strategy toward China and on the future of U.S. alliances and partnerships in the Indo-Pacific. Before joining CNAS, Kliman worked in the U.S. Department of Defense, where he served as Senior Advisor for Asia Integration. His most recent book is *Fateful Transitions: How Democracies Manage Rising Powers, from the Eve of World War I to China's Ascendance* (University of Pennsylvania Press, 2014).

Ben FitzGerald is an Adjunct Senior Fellow with the Defense Program at the Center for a New American Security and a partner at Lupa, a private investment firm. Prior to these roles, FitzGerald was the Executive Director—Strategy, Data, and Design in the Pentagon's Office of the Undersecretary of Defense for Acquisition and Sustainment. Before the Pentagon, FitzGerald was a Professional Staff Member on the Senate Armed Services Committee.

Kristine Lee is an Associate Fellow for the Asia-Pacific Security Program at the Center for a New American Security. She received her BA from Harvard College, where she was editor-in-chief of the *Harvard International Review* and was awarded a Fulbright fellowship. She earned her Master in Public Policy from the Harvard Kennedy School, with a focus on international relations and security studies in the Asia-Pacific region.

Joshua Fitt is a Research Assistant for the Asia-Pacific Security Program at CNAS. He focuses on U.S. East Asian security strategy and specializes in Japanese and Korean Peninsular affairs. Before joining CNAS, Fitt was a campaign field organizer during the 2018 midterm elections in the Upper Midwest, an earthquake and tsunami disaster relief volunteer with IsraAID in Japan, and the Council on Foreign Relations' Japan Program Intern. He earned his BA in East Asian Studies from Yale University.

Acknowledgments

This report was made possible by the generous funding of the Government of Japan. The authors are grateful to the many officials and experts—both in the United States and elsewhere—who shared their perspectives during the course of the project. This report would not have been possible without assistance from a variety of current and former CNAS colleagues, including Karina Barbesino, Melody Cook, David Dee, Ashley Feng, Allison Francis, Ilan Goldenberg, Maura McCarthy, Martijn Rasser, Ely Ratner, Elizabeth Rosenberg, and Loren DeJonge Schulman. In addition, the authors would like to thank Eric Chewning, Martijn Rasser, and Anja Manuel for reviewing full drafts of this report, and James Schoff and Bill Greenwalt for reviewing smaller segments. Lastly, the authors are grateful to the Government of Norway for arranging a study tour in support of this report.

The views presented here are the authors' alone and do not represent those of CNAS or any other organization. The authors are solely responsible for any errors in fact, analysis, or omission.

About the Asia-Pacific Security Program

The CNAS Asia-Pacific Security Program addresses opportunities and challenges in the region for the United States, with a growing focus on issues that originate in the Asia-Pacific but have global implications. It draws on a team with deep government and nongovernment expertise in regional studies, U.S. foreign policy, international security, and economic statecraft. The Asia-Pacific Security Program analyzes trends and generates practical and implementable policy solutions around three main research priorities: U.S. strategic competition with China, American alliances and partnerships, and the North Korean threat.

America Competes

2020

America Competes 2020

America Competes 2020 is a Center-wide initiative featuring cutting-edge CNAS research, publications, events, and multimedia aimed at strengthening the United States' strategic advantages at home and abroad.

FORGING AN ALLIANCE INNOVATION BASE

Executive Summary

This report presents a blueprint for a community of technology innovation and protection anchored by America and its allies. Unless the United States builds this community—an "alliance innovation base"—it will steadily lose ground in the contest with China to ascend the commanding technological heights of the 21st century. Given that technology will increasingly determine future military advantage, underpin economic prosperity, and function as a tool for promoting liberal and illiberal visions of domestic governance, the stakes could not be higher.

To compete, China is leveraging its formidable scale—whether measured in terms of research and development (R&D) expenditures, data sets, scientists and engineers, venture capital, or the reach of its leading technology companies. The only way for the United States to tip the scale back in its favor is to deepen cooperation with allies. The global diffusion of innovation also places a premium on aligning U.S. and ally efforts to protect technology. Unless coordinated with allies, tougher U.S. investment screening and export control policies, for example, will feature major seams that Beijing can exploit.

America's current approach to allies on technology innovation and protection remains a work in progress. In recent years, animated by concerns about China, the United States has made a concerted effort to step up engagement with allies in both areas. Existing mechanisms for deepening innovation with allies include technology scouting programs, multilateral cooperative frameworks, rapid innovation initiatives, and bilateral projects. However, these mechanisms at times lack sufficient resourcing, move too slowly, or feature rigid constraints on participation. U.S. instruments for working with allies on technology protection also contain major points of weakness. Multilateral export control regimes, though inclusive, are ponderous. The extraterritorial reach of U.S. export control laws can generate unintended obstacles to technology collaboration with allies. Bilateral and minilateral consultations on protection lack positive incentives to motivate allies to incur immediate costs such as forgoing technology sector investments from China.

Design Principles

The strengths and weaknesses of the current American approach inform this report's blueprint for an alliance innovation base. So do the aspirations and potential contributions of individual U.S. allies. The report focuses in particular on Japan, given its deep-seated concerns about China's technology ascendance, intense interest in protection, and enduring strengths in certain types of technology development. Recognizing that these qualities also render Japan unrepresentative, this report further examines three additional U.S. allies—Australia, Israel, and Norway—countries that collectively feature significant diversity in their perceptions of China and approaches to technology innovation and protection.

The following design principles for an alliance innovation base reflect a detailed examination of these four countries as well as lessons learned from best practices and pitfalls of current U.S. engagement with allies on technology innovation and protection.

1. Adopt a flexible architecture for an alliance innovation base that can accommodate countries with variable threat perceptions and distinct capabilities.
2. Create tangible economic benefits to incentivize allies to adopt tougher technology protection measures.
3. Focus technology cooperation on solving narrowly scoped problems in order to manage divergent views on the nature of the international threat environment.
4. Foster a "benefit together" ethos that chips away at deeply rooted preferences for spending and procuring domestically.
5. Incorporate politicians, publics, and the private sector from the outset to build critical momentum in support of an alliance innovation base.

A BLUEPRINT FOR MOVING FORWARD

No single action by the United States will galvanize an alliance innovation base. Rather, the task for Washington is to construct a community of technology innovation and protection link by link, proceeding along five main lines of effort:

Strengthen America's Toolkit for Technology Engagement

- *Increase resources for major technology scouting programs.* For example, Congress in the next National Defense Authorization Act (NDAA) and defense appropriation should expand funding for the Office of Naval Research Global and the Foreign Comparative Testing Program.
- *Leverage U.S. Defense Attaché Offices.* The Defense Department should add technology scouting to the responsibilities of Defense Attachés posted to U.S. embassies in allies with robust innovation ecosystems.
- *Internationalize startup-focused engagements.* The Defense Innovation Unit, which today has a primarily domestic mandate, should over time go global, beginning with roadshows to allies, and culminating with a permanent presence overseas.

Build Ally Awareness and Capacity

- *Upgrade information sharing with ally governments.* Making releasable to allies the most granular list of critical technologies the U.S. government has compiled would help to align protection measures.
- *Promote broad-based awareness of China's actions.* The United States should undertake a comprehensive public diplomacy campaign to highlight China's pursuit of technology within the innovation ecosystems of allies.
- *Build ally capacity to protect technology.* Where possible, Washington should help ally intelligence and law enforcement agencies to retool for tracking and countering Beijing's technology acquisition efforts.

Launch New Collaborative Platforms

- *Establish bilateral national security innovation funds.* These funds could support a range of initiatives, from quickfire seed projects to road test high-risk ideas to incubators for startups innovating at the nexus of defense and commercial applications.
- *Form a military test facility consortium.* Participating governments would pool access to high-demand, low-availability equipment and ranges in exchange for the sharing of test results with other members of the consortium.
- *Launch a cross-national platform to build new companies.* This platform would bring together innovators and entrepreneurs from the United States and participating allies to develop new businesses around specific national security themes.

Create Positive Incentives for Technology Protection

- *Reduce barriers to investment in the United States for allies committed to technology protection.* As an initial step, the Treasury Department should make explicit what investment screening and export control standards allies must meet to qualify as "excepted states" under current regulation governing U.S. national security review of foreign investments.
- *Invite U.S. allies to join an "ITAR Free Zone."* Washington should announce its intent to eliminate onerous licenses controlling the bilateral flow of U.S. defense goods, services, and knowledge with and among allies that meet concrete technology protection standards.

Leverage the U.S.-Japan Alliance

- *Announce a government data pooling partnership.* The United States and Japan should unveil an initiative to pool select, curated datasets held by each government for use by companies and innovators in each country.
- *Spearhead export controls on semiconductor manufacturing equipment.* To extend their current advantage in this critical technology area, the United States and Japan should work with the Netherlands – the other market leader – to impose new restrictions on sales to China.
- *Initiate a bilateral dialogue on research integrity.* Washington and Tokyo should convene a regular dialogue of administrators from their top technology universities to develop best practices for managing risks posed by Chinese researchers and institutional partnerships.

Chapter 1: Introduction

The United States is steadily losing ground in the race against China to pioneer the most important technologies of the 21st century. With technology a critical determinant of future military advantage, a key ingredient of economic prosperity, and a potent tool for the promotion of different models of governance, the stakes could not be higher for Washington.

America's eroding technological edge stems from multiple causes. China has vastly increased domestic research and development (R&D) expenditures and supported the growth of new cutting-edge industries. It has also invested in fostering science and engineering talent, taking advantage of its much larger population.[1] By contrast, the United States has failed to undertake a comparable effort domestically. Moreover, Washington for decades largely overlooked Beijing's systematic effort to acquire technology from U.S. companies and research institutions through tactics ranging from legal investments to cyber-enabled economic espionage.[2]

As the scope and scale of the technology challenge posed by China has become evident, politicians, business leaders, government agencies, and think tanks in the United States have called for a renewed commitment to sustaining America's innovation leadership.[3] Domestically, the path forward for the United States is clear but politically fraught. Washington remains mired in a seemingly endless debate over the merits of greater government R&D funding; enhanced science, technology, engineering, and mathematics (STEM) education; and an immigration system optimized to attract and retain foreign talent.

Protecting technology has proved an easier political lift in Washington than advancing a pro-innovation agenda. Congress and the executive branch have come together to support tightened investment screening procedures and more rigorous export controls.[4] Yet such measures do nothing to grow America's capacity to innovate and, if poorly implemented, could have a constricting effect.

Until recently, the U.S. approach to technology innovation and protection treated allies as a relative afterthought, when they should be at the center of any strategy to secure America's technological advantage. In fact, Washington's global network of alliances represents a unique asset in the technology competition with Beijing.

To compete with the United States, China is leveraging its formidable scale—whether measured in terms of R&D expenditures, data sets, scientists and engineers, venture capital, or the reach of its leading technology companies. The only way for the United States to tip the scale back in its favor is to deepen innovation linkages with its allies. America's global portfolio of alliances encompasses most of the world's economically advanced nations.[5] But U.S. allies provide more than just scale. In today's new era of strategic competition, American allies have emerged as leaders in specific technology areas that are core to future U.S. prosperity and military advantage, such as 5G next generation wireless networks, autonomy, and microelectronics.[6] Closer cooperation with allies will enable the United States to tap into pockets of technological expertise it now lacks domestically.

The only way for the United States to tip the scale back in its favor is to deepen innovation linkages with its allies.

The diffusion of innovation also places a premium on aligning U.S. and ally efforts to protect technology. Through more rigorous investment screening, updated export controls, and closer scrutiny of research collaborations involving China, the United States can unilaterally become a harder target. However, unless coordinated with allies, such policies will feature major seams that Beijing can exploit: China will acquire technology from American allies that it can no longer easily extract from the United States. For Washington, the net result will be barriers to innovation and forgone economic opportunities with little to show in terms of technology secured.[7]

Toward a Community of Innovation and Protection

Galvanized by the China challenge, the United States has started to deepen engagement with allies around innovation and protection. For example, on the innovation side, the U.S. Department of Defense in January 2020 launched the Allied Prototyping Initiative (API), which aims to "co-develop leapahead capabilities through cooperation with trusted allies whose industrial capacity, capability and workforce strategically complement those of the United States."[8] This is a promising step, but the larger set of mechanisms for technology collaboration with U.S. allies in the national security domain generally reflects an earlier era of unchallenged American preeminence in which concerns about China and the imperative to move quickly or risk falling behind did not exist.

Through separate policy channels, Washington has made a concerted push to get its allies to sharpen their

investment screening and export controls and apply more scrutiny to research involving Chinese institutions and nationals.[9] Yet the potential economic costs of such measures—and for some, fear of Beijing's retaliation—renders progress slow and uneven. Where U.S. allies share American concerns about China's geopolitical ambitions, efforts to align approaches to protection have moved forward quickly. However, this overlap of threat perceptions largely exists in the Indo-Pacific (and not even uniformly there), rendering key innovation hubs in Europe and elsewhere vulnerable to China's continued efforts to obtain technology abroad through any means possible.

When engaging with allies, the United States has largely separated innovation from protection. This reflects organizational and cultural inertia rather than a strategic choice. Within the executive branch, different offices typically manage each issue set: U.S. officials can spend their entire career in one area or the other, given the level of expertise required to oversee collaborative technology programs or master the intricacies of export control regulatory requirements. Outside the U.S. government, distinct expert communities work on technology innovation and protection, and rarely converge. More broadly, the principles that animate the two—openness versus closure—exist in tension.

American efforts to promote technology protection will progress slowly, if at all, unless paired with a positive vision of an innovation community.

In an era of strategic competition with China, this policy separation is counterproductive. Outside a handful of U.S. allies in the Indo-Pacific, American efforts to promote technology protection will progress slowly, if at all, unless paired with a positive vision of an innovation community spanning the United States and its allies that delivers significant benefits to all involved. These benefits, when linked to concrete steps to elevate technology protection, would help to incentivize ally governments to enact measures that carry an up-front economic cost, such as adopting tougher investment screening procedures or enhancing export controls. Moreover, embedding protection within a larger context of deepening innovation is likely to resonate far more with ally publics than the current U.S. approach, in which American demands to take action against China make the front-page local press, while technology cooperation involving the United States occurs in the background, with little popular fanfare.[10]

Now is the time to move beyond this flawed approach. This report advances a blueprint for building a new community that would bring together the United States and its allies around innovation and technology protection. The new community—an "alliance innovation base"—would feature a web of cooperative connections and incentivize technology protection through mutual benefits.

Scoping the Alliance Innovation Base

This report reflects several analytic choices by the authors that are worth illuminating. The first choice pertains to scoping cross-national innovation. The report does not attempt to cover all forms of technology collaboration among the United States and its allies—a topic so vast that it would be impossible to adequately explore here. At the same time, the report takes a more expansive approach than joint military R&D or prototyping. It examines cross-national innovation through the lens of using technology to address shared national security concerns, broadly defined. This reflects the authors' assessment that many of the most pressing challenges confronting the United States and its allies are not purely military and that significant opportunity exists for cooperative technology solutions to yield commercial benefits that could in turn incentivize closer alignment on technology protection.

The second analytical choice shaping this report is its detailed focus on a handful of U.S. allies, starting with Japan. Among America's allies, Japan is best positioned to amplify U.S. efforts to forge an alliance innovation base. Tokyo and Washington share similar concerns about China's bid for technology supremacy. Japan has taken an intense interest in technology protection. Although it lags in startup creation, Japan remains a world leader in select technologies.[11] Yet for all the same reasons, Japan is not representative of America's allies as a whole.

Indeed, U.S. allies run the gamut in their perceptions of Beijing, with some regarding China almost entirely as an economic opportunity. Likewise, approaches to technology protection differ substantially across U.S. allies. So does the type of innovation and technological expertise that allies might contribute. To design for this diversity, the report also contains in-depth case studies on Australia, Israel, and Norway. These three allies provide

significant variation in the attributes described above. A few additional considerations behind this case selection include Australia's membership in the Five Eyes intelligence alliance, Israel's density of startups with dual civilian-military use technology, and Norway's disproportionate defense technology contributions to U.S. and ally militaries. An alliance innovation base that can serve as a community for these three nations plus Japan is scalable to a much wider set of countries.

The Way Forward

The remainder of this report lays out a blueprint for an alliance innovation base. Chapter 2 makes the case for why America must enhance cooperation with its allies around technology innovation and protection. Chapter 3 reviews the strengths and weaknesses of the current U.S. approach in both areas. Chapter 4 draws out the perspective of American allies—starting with Japan, and then turning to Australia, Israel, and Norway—with a focus on what each might contribute to an alliance innovation base and expect in return. Lastly, Chapter 5 advances design principles and concrete policy recommendations for forging an alliance innovation base.

Chapter 2: The Case for an Alliance Innovation Base

In technology, as in most other domains of strategic competition, the United States can rise to the China challenge only in concert with allies. This chapter makes the case why. It starts by documenting China's growing scale advantage over the United States in critical inputs of innovation, then demonstrates how allies can help tip the scale back in America's favor. Next, this chapter explores how the global diffusion of innovation creates a new imperative for the United States to cooperate with its allies. Lastly, this chapter discusses some of the general limitations of America's current approach toward allies, and points to the need for the types of positive incentives that an alliance innovation base could generate.

China's Scale Advantage

Innovation has emerged as a key pillar of China's national power. President Xi Jinping made clear in his 19th Party Congress address in 2017 that national rejuvenation requires cementing China's standing as a "country of innovators" and implementing an "innovation-driven development strategy."[12] This has involved the pursuit of grand strategic policies such as Made in China 2025,[13] which seeks to upgrade China's placement in global production and innovation networks through government subsidies, the mobilization of state-owned enterprises, and forced transfer of technologies.[14] Beijing's bid for technology supremacy benefits from scale, due to the size of China's population and its economy—now the world's largest by some measures.[15] As the 2020s begin, China is poised to outmatch the United States in many of the raw inputs that fuel technology innovation.

China's R&D efforts overwhelmingly focus on experimental development, enabling Chinese companies like Huawei to quickly adapt products and scale up engineering output across critical technology areas. (Kevin Frayer/Getty Images)

First, China's total R&D expenditure is positioned to overtake combined U.S. government and corporate R&D before the end of the decade, enabled by a combination of concerted government planning and rapid economic growth.[16] In 2019, Beijing's R&D spending surged past 2.19 percent of its gross domestic product (GDP), compared with a mere 0.72 percent of its GDP in 1991, setting China on track to meet its R&D expenditure-to-GDP ratio of 2.5 percent by 2020 as delineated in its 13th Five-Year Plan.[17]

Although the United States still spends more on R&D than any other country at about half a trillion dollars a year, China has quickly pulled to second place.[18] China's gross R&D expenditure now exceeds that of Japan, Germany, and South Korea combined.[19] Notably, China's R&D efforts today overwhelmingly focus on experimental development—at about 80 percent of overall spending, compared with 60 percent to 65 percent in the United States.[20] This comparative emphasis on experimental research has enabled China to quickly adapt products and services and scale up engineering output across critical technology areas, including quantum communications, artificial intelligence (AI), and 5G.

Second, China's level of venture capital funding, though in flux, has recently caught up to and, by some metrics, even briefly surpassed that of the United States. In 2005, the totality of China's venture capital hovered at a mere $4.8 billion.[21] But in the second quarter of 2018, companies based in China secured nearly $3 billion more in venture capital funding than their American counterparts for the first time in history.[22] The trajectory of venture investment in China is far from stable.[23] Nonetheless, the perhaps fleeting uptick in funding provided a boost to a diverse set of Chinese industries, including transportation, logistics, financial technology, and biotechnology. The government of China has, meanwhile, touted its deepening well of venture capital funds as a vehicle for achieving its goal of technological leadership by 2025.[24]

Third, China's technology giants are operating at an increasingly global scale. Just a decade ago, the largest U.S. technology companies, including Facebook, Amazon, Netflix, and Google (colloquially known as "FANGs"), were largely unrivaled. But in recent years, Beijing's technology champions—Baidu, Alibaba, and Tencent (known as "BATs")—have experienced outsized growth. In 2019, American companies in the FANGs group still maintained a substantial lead in stock market value over China's BATs, with respective market capitalizations at around $2.3 trillion[25] and $950 billion.[26] This measure notwithstanding, many of China's technology companies have led a concerted effort to penetrate global markets and are able to design and sell innovative products in larger quantities than leading U.S. firms. For example, Huawei surpassed Apple in 2018 as the world's second-largest smartphone vendor.[27] Tencent has also led a sustained push in the past several years to expand its international user base by launching English and other non-Chinese language versions of WeChat, its central platform.[28] In the realm of e-commerce, Alibaba

Jack Ma of Alibaba and Pony Ma of Tencent, standing at center of the first row, at the 40th Anniversary of Reform and Opening Up at The Great Hall of The People in December 2018. Their companies are among the "BATs," Beijing's technology champions with an increasingly global reach. (Andrea Verdelli/Getty Images)

overshadows Amazon in terms of global gross merchandise, with Alibaba raking in $765 billion in 2019, compared with Amazon's $239 billion.[29]

Fourth, China is systematically hoarding data for commercial advantage. These practices have been enabled by its online population of more than 800 million and lack of privacy protection, which stands in stark contrast to the United States' stronger regulations and fewer than 300 million internet users.[30] And while U.S. technology giants have faced growing domestic political resistance due to privacy concerns over their extensive data gathering, the Chinese Communist Party (CCP) enjoys a symbiotic relationship with China's major technology companies, leveraging them to collect data, expand and optimize its political controls, and ultimately shape its global operating environment.[31] The CCP in fact directly supervises certain Chinese state-owned enterprises, such as the Global Tone Communication Technology Co. Ltd., which gathers massive amounts of consumer data through its own platforms and through cooperation with other national champions such as Huawei and Alibaba Cloud.[32] Chinese city governments have also initiated dozens of partnerships with these technology companies on "smart city" projects[33] to streamline data collection in support of the country's national surveillance system.[34]

Fifth, China is investing heavily in its homegrown talent. According to the National Science Foundation, China has almost caught up to the United States in its annual number of doctoral degrees in science and engineering, with 34,000 compared to the United States' 40,000 in 2014.[35] In 2016, China produced 4.7 million STEM graduates across the board, compared with 569,000 in the United States, though the quality of these degrees is not necessarily comparable.[36] Through its aggressive Thousand Talents recruiting program, Beijing has enticed an elite group of foreign-born scientists as well as Chinese citizens who have studied at elite international universities to China with lucrative offers and promises of multiyear research funding.[37] The volume of China's output of intellectual property has also surged in equal measure. In 2017, China's State Intellectual Property (IP) Office received 1.2 million applications—more than double the number the United States' IP office received.[38] Similarly, in 2016, annual scientific publications from China surpassed those from the United States for the first time, with Chinese contributions accounting for 36 percent of global publications.[39] Along metrics of quality, however, China lags the United States. Scientific papers published by American scientists are still more frequently cited than those published by their Chinese counterparts, particularly as publication fraud has roiled the Chinese academic community.[40] Similarly, although the quantity of Chinese patent filings has ticked upward in recent years, the quality of these applications has not necessarily increased commensurately.[41]

Sixth and finally, China's military-civil fusion framework has enabled advancements made in its commercial sector to broadly drive forward the modernization of the People's Liberation Army (PLA).[42] Beijing mandates synergies between industry and its national defense apparatus. Commercial companies are expected to share technology with the PLA and incentivized to turn first to it with their innovations.[43] Moreover, the PLA can embed its officers in research universities and even corporations.[44] While the PLA is well positioned to benefit from China's growing technological prowess, the U.S. Department of Defense operates in a radically different domestic environment. Elements of the technology industry, particularly in Silicon Valley, remain reluctant to cooperate with the U.S. military due to normative concerns and frustrations about the pace of government contracting.[45]

Allies Tip the Scale Back in America's Favor

Despite China's technology ascendancy, the United States and its allies together retain a commanding—and in some cases, probably insurmountable—lead in key drivers of innovation. For example, in R&D, the Organisation for Economic Co-Operation and Development (OECD), which comprises the United States, most of NATO, American allies in the Indo-Pacific, and a handful of other developed economies, collectively outspends China by more than 250 percent.[46]

Although China's production of PhDs in science and technology rivals the output of U.S. doctoral programs (notwithstanding questions of comparability), the pool of doctoral candidates across U.S. and ally countries is more than double that of China.[48] Venture capital is another area where allies can keep scale in America's favor. The United States and China are clear leaders in this field, with venture capital deals in each reaching more than $100 billion in recent years. Venture capital investments in U.S. allies, though much smaller in scale, still add up to substantial totals. For example, in 2018, venture capital deals in Europe and Israel combined approached $30 billion.[49]

Finally, the collective online population of the United States and its allies towers over that of China at 1.5 billion active users, compared with China's approximately 840 million internet users.[50] Although data usage and online privacy regulations are fragmented across OECD countries, the much larger pool of online users across U.S.

allies offers opportunities to reinforce shared values and norms around privacy protection and freedom of expression online.

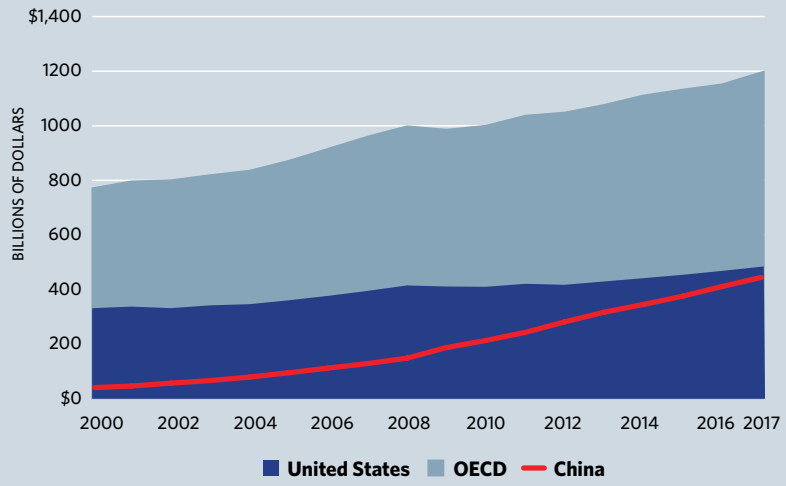
Technology Protection Requires a Collective Effort

The U.S. government, as part of a coordinated, interagency response to what FBI Director Christopher Wray described in 2018 as a "whole-of-society" threat emanating from China, has taken steps to become a harder target for Beijing's technology acquisition strategy.[51] In 2018, the U.S. Congress passed the Foreign Investment Risk Review Modernization Act (FIRRMA). This landmark legislation substantially broadened the scope and authorities of the Committee on Foreign Investment in the United States (CFIUS) to conduct national security reviews. In parallel, the United States has moved to strengthen export controls, with a greater focus on critical emerging technologies.[52]

Beijing has responded to U.S. efforts to protect critical technology by shifting its focus to American allies that it perceives as easier targets. Just as China has made a concerted effort to acquire technology from the United States using both licit and illicit means, it is seeking to extract value from the innovation ecosystems of American allies using the following mechanisms:

- *Mergers and acquisitions:* Beijing has funneled significant capital toward direct investments and investment funds overseas with the aim of acquiring critical technologies from foreign competitors. Guangdong-based Midea Group's acquisition of a leading German robotics company[53] and the takeover of a British digital radio producer by Shenzhen-based Hytera Communications are but two examples of China acquiring cutting-edge technology companies outside the United States.[54]
- *Forced tech transfer for market access*: A 2019 survey conducted by the European Union (EU) Chamber of Commerce showed that about 20 percent of respondents from European firms felt compelled to transfer technology to maintain access to Chinese markets, a 10 percent increase since 2017.[55] In Asia, Japan has also bristled at China's efforts to extract critical technology. One particularly high-profile spat involved accusations in 2011 by Kawasaki Heavy Industries Ltd., maker of Japan's Shinkansen bullet train, that China had leveraged Japanese technology to construct its own high-speed rail network after Shinkansen had set up a joint venture with local Chinese manufacturers in 2004.[56]
- *Cybertheft:* The threat from Chinese cyberespionage and cybertheft has raised alarm bells among the Five Eyes—the United States, the United Kingdom (UK), Canada, New Zealand, and Australia—as well as U.S. allies in Asia such as Japan. In 2018, a coalition of countries, including the Five Eyes, Japan, Germany, and Norway, publicly decried a 12-year Chinese campaign of cyberattacks to steal technology and trade secrets from corporate computers in more than 12 countries.[57]
- Research partnerships and *overseas researchers:* The PLA and PLA-affiliated institutes have also stood up research partnerships with and sent researchers to prominent U.S. ally universities around the world to acquire cutting-edge technology. For example, in 2018, the People's Daily—which is part of the CCP's propaganda apparatus—claimed that the PLA's National University of Defense Technology (NUDT) was establishing "overseas study bases" at academic institutions including Oxford, Cambridge, and Harvard.[58] Since 2007, the PLA has quietly and at times covertly sent more than 2,500 military scientists to institutions around the world, including in Australia, Canada, Germany, Japan, Singapore, and the United

Total Gross Research and Development Expenditures of the OECD and China



China's gross R&D spending has caught up to the United States, but the OECD as a whole—which includes the United States—significantly outspends China by more than 250 percent.

Source: OECD Gross Domestic R&D Spending statistics[47]

States, for the express purpose of exfiltrating sensitive information that could facilitate the development of new Chinese military technologies.

The U.S. government's protection measures will do little to slow China's technology acquisition strategy without parallel actions by allies. Through a range of legal, policy, societal, and cyber-enabled tools, Beijing is systematically exploiting weak links in the innovation ecosystems of American allies to acquire technology that it is increasingly being denied within U.S. borders. Technology protection is an inherently collective endeavor.

American Allies Require Positive Incentives

For American allies, most steps to reduce their vulnerability to China's technology acquisition strategy will incur an economic cost. Short-term pain points might include relinquishing export opportunities to China; turning down investment from China, when alternative sources of financing may or may not exist; forgoing the financial benefits to domestic universities that research partnerships with China might provide; and risking broader Chinese economic retaliation, including a curtailing of the flow of Chinese students and tourists or boycotting of a country's exports.

In recent years, U.S. efforts to convince allies to adopt new technology protection measures have yielded some fruit. After pressure from the United States, for example, Israel's security cabinet decided in 2019 to establish a mechanism to monitor Chinese investments into businesses designated as critical to the economy or to national security.[59] Also in 2019, after sustained outreach from and consultation with senior U.S. government officials, the European Union—led by Germany and France—declared China a "strategic rival" in high-level strategy documents, adopted a series of new rules to enable closer scrutiny of Chinese investments in Europe,[60] and launched a review of the EU's industrial and procurement policies to ensure Beijing is not unfairly advantaged.[61]

With the handful of U.S. allies that share America's view of China as a leading competitor, these conversations can be productive and yield rapid results. However, most American allies do not fully share U.S. concerns about the challenge posed by China. Allies across Europe, for example, are reluctant to adopt technology protection measures that impose an immediate short-term cost on their economies. As U.S. leaders concerned about China's technological ambitions honed in on 5G wireless networks,[62] Berlin, for example, has remained reluctant to apply its sharper approach toward Beijing to this critical domain, despite considerable opposition to the use of Huawei telecommunications equipment among some German legislators.[63] At the beginning of 2020, the UK, much to the consternation of the United States, also approved the use of Huawei technology in its new 5G network, notwithstanding significant pushback from some members of Parliament and pleas from the U.S. government that doing so could compromise the two nations' close intelligence-sharing relationship.[64]

To present a compelling case for technology protection, the United States needs to offer a series of positive benefits that offset some of the short-term costs allies will incur. Absent this affirmative agenda, U.S. efforts to reduce China's access to the innovation ecosystems of its allies will fall short. An alliance innovation base could provide a platform for incentivizing enhanced technology protection, while broadening the public conversation with allies from countering China to capitalizing on shared technology opportunities.

U.S. Secretary of State Mike Pompeo meets British Prime Minister Boris Johnson in January 2020 to discuss the role of Huawei in the UK's 5G networks. The UK approved the use of Huawei technology in its 5G networks over American protests and concern over future intelligence sharing. (Tolga Akmen/WPA Pool/Getty Images)

Chapter 3: Evaluating America's Current Approach

At present, U.S. engagement with allies falls well short of a community that pairs technology innovation and protection. This chapter examines America's current approach to allies in both areas, with a focus on highlighting points of strength and weakness. It concludes by evaluating the degree to which the instruments Washington now employs could serve as a model for an alliance innovation base.

Cooperation on Technology Innovation

The United States has an array of mechanisms for collaborating with allies on technology in the pursuit of common national security objectives. Some mechanisms date back to the Cold War, while others are recent and reflect growing American recognition of the imperative to deepen innovation linkages with allies amid an accelerating U.S.-China technology competition. What follows is a curated survey of these mechanisms intended to highlight their diversity, rather than an exhaustive compilation of every international technological engagement undertaken by the U.S. national security establishment.[65]

TECHNOLOGY SCOUTING

Office of Naval Research Global (ONR Global)

Established in 1946, ONR Global is arguably the Defense Department's flagship technology scouting enterprise. It has physical offices in Asia, Europe, and Latin America. ONR Global arranges for foreign scientists to visit the United States, finances international workshops, and provides seed funding to international researchers—all with the aim of identifying technology relevant to addressing challenges confronted by the U.S. Navy and Marine Corps.[66]

Strengths

- *Globally oriented:* ONR Global's international reach and extensive program of activities facilitates connectivity between technical communities across a wide range of countries for long-term research and development. ONR projects encompass some of the United States' most innovative allies that are not a part of the Five Eyes.

Weaknesses

- *Narrowly scoped:* Despite its global reach and the wide-ranging scope of its activities, the thrust of ONR Global research and development programs largely remains limited to innovation in the naval domain.

Foreign Comparative Testing (FCT) Program

The FCT program, established in 1980, is primarily a procurement program that connects foreign technologies—ranging from artificial intelligence software to electromagnetic field sensors—to the Department of Defense by reducing acquisition costs and procedural hurdles between U.S. and ally industries.[67] Through the program, for example, the Department of Defense nominates foreign items to undergo an expedited testing and evaluation process to determine whether they fulfill U.S. military standards or address mission area shortcomings.[68] Since its establishment, the program has yielded procurements of more than 281 projects worth over $11 billion.[69]

Strengths

- *Structured efficiency:* The FCT creates a concrete point for trusted foreign vendors to enter the U.S. defense industrial base. Having a structured process in place enables significant cost and schedule savings to support the relatively quick fielding of capabilities.
- *Comprehensive:* The scope of technologies involved in the FCT cuts across areas prioritized by the Defense Department, including space, missile defense, hypersonics, artificial intelligence, and quantum technology.

Weaknesses

- *Near-term focus:* The FCT is primarily focused on procurement and acquisition that serve to fill present or near-term future gaps in U.S. military capability, rather than supporting cooperation around long-term innovation.[70]
- *Low profile:* The FCT maintains a relatively low profile, and opportunities are socialized by word of mouth. The absence of an effective data-sharing mechanism across U.S. allies leads to redundancies and missed opportunities in discovery and matchmaking.

MULTILATERAL COOPERATIVE FRAMEWORKS

The Technical Cooperation Program (TTCP)

The TTCP, a collaborative five-nation forum among the Five Eyes countries, provides opportunities for member nations to integrate their R&D capabilities at minimal cost.[71] The program today covers 11 major areas, including electronic warfare, aerospace, joint systems and analysis, and conventional weapons and materials processing, and involves more than a thousand scientists across the allied countries.[72] Each of the 11 focus areas features a

technical panel that monitors and identifies opportunities for collaboration, as well as an action group that executes discrete projects.[73]

Strengths

- *Trusted network:* The unique nature of Five Eyes enables cooperation across sensitive technology areas that might otherwise be challenging for countries that do not form an intelligence alliance with the United States.

Weaknesses

- *Limited scalability:* Expanding the program beyond the Five Eyes remains infeasible due to the exclusive military focus of technology collaboration, secrecy surrounding its activities, and the program's relative detachment from commercial sector innovation.

National Technology and Industrial Base (NTIB)

Mandated by the 1993 National Defense Authorization Act (NDAA) as Congress grappled with the prospect of significant cuts to U.S. defense spending at the end of the Cold War, NTIB sought to boost advanced R&D and systems development and industrial preparedness to sustain the technological superiority of the U.S. military—initially through closer U.S.-Canadian defense cooperation.[74] More than two decades later, the 2017 NDAA expanded the NTIB to include the UK and Australia, just as Congress directed the Department of Defense to work toward closer integration of the technology and industrial bases of the four NTIB member countries.[75]

Strengths

- *Involvement of key allies:* NTIB serves as the most coordinated and comprehensive framework for structured cooperation between U.S. allies to date, and the United States is able to play to its strength as a system integrator within the framework.

Weaknesses

- *Challenges to integration:* Despite this push for deeper integration, the U.S. export control system—including the State Department's International Traffic in Arms Regulations (ITAR)—remains a barrier to more seamless integration of the industrial bases of the United States, Canada, Australia, and the UK.[76] Additionally, the prospect of expanding the NTIB to include some of the United States' other technologically advanced allies remains uncertain, given the lack of continuity across their export control systems, threat perceptions, and other standards.

RAPID INNOVATION INITIATIVES

Defense Innovation Unit (DIU)

As the Defense Department's premier initiative to engage commercial technology startups, the DIU has an overwhelmingly domestic mandate. It leverages a formerly obscure contracting authority to rapidly award prototyping contracts to companies with technology relevant to challenges identified by the U.S. military. To date, the DIU has made only limited forays into engagements. For example, in 2018, the DIU welcomed a UK liaison officer, while also seeking greater connectivity with its UK counterpart, the Joint Forces Command's jHub.[77]

Strengths

- *Attractive power:* The DIU's model of fast prototype projects leveraging commercial sector technology remains of interest to many U.S. allies, which are keen to replicate it.

Weaknesses

- *Constrained bandwidth:* Limited staffing and pressures to show quick results within the United States have held back the DIU from undertaking major initiatives with U.S. allies.

The Defense Innovation Unit (DIU) met with Indian Minister of Defence Manohar Parrikar on August 29, 2016. The DIU is the Department of Defense' premier initiative to engage commercial technology startups and has made only limited forays into international engagements. (Tim D. Godbee/DoD)

Allied Prototyping Initiative

In January 2020, the Department of Defense launched the API, which aims to "co-develop leap-ahead capabilities through cooperation with trusted allies whose

industrial capacity, capability and workforce strategically complement those of the United States."[78] The initiative—housed within the Under Secretary of Defense for Research and Engineering—focuses on coordinating innovation around a set of discrete projects in priority technology areas, including hypersonic weapons, artificial intelligence, and cybersecurity.

Strengths

- Discrete scope: The API supports innovation over a medium-term time horizon, rather than simply acquisition or long-term R&D without concrete deliverables. This scoping facilitates rapid prototyping across priority technology areas, broadly supporting alliance interoperability in emerging technologies.

Weaknesses

- Lack of strategic focus: While the initiative is well positioned to deliver a discrete set of projects, it lacks a broader framework for technology cooperation with U.S. allies that is galvanized by a common strategic imperative.

BILATERAL PROJECTS

There are also numerous bilateral projects and dialogues underway between the United States and its allies to apply technology against shared national security challenges. Standout projects include long-running collaboration between the United States and Japan on the Standard Missile-3 Block 2A interceptor[79] and the United States and Israel on the Arrow family of missile defense systems.[80] An example of ongoing bilateral dialogues is the Science and Technology Forum (S&TF), which is held once a year by the U.S. Department of Defense and Japan's Ministry of Defense.[81]

Strengths

- *Streamlined management:* Bilateral projects with allies, though by no means straightforward, are generally easier to manage than multicountry collaborations.
- *Maximizing shared resources:* With some allies, bilateral cooperation is the optimal or only avenue to solicit burden-sharing with the United States on technology innovation.

Weaknesses

- *Uneven results:* Some projects and dialogues can yield significant real-world outcomes while others can be more formulaic than substantive, absent a clear and present threat or political pressure for rapid deliverables.
- *Fragmented:* Engaging individual U.S. allies creates bilateral silos of cooperation that in turn impose barriers on realizing potential economies of scale or collective shared interest across American alliances.

Aligning Technology Protection With Allies

The United States has a long history of working with its allies to secure technology from strategic competitors. For example, during the Cold War, Washington used the Coordinating Committee for Multilateral Export Controls (CoCom), which encompassed most members of NATO plus Australia and Japan, to deny the Communist bloc access to critical technologies.[82] Today, American engagement with allies on protection employs multiple instruments, including multilateral regimes, the extraterritorial reach of U.S. law, and bilateral and minilateral consultations.

MULTILATERAL EXPORT CONTROL REGIMES

The United States participates in four multilateral export control regimes. The first, the Nuclear Suppliers Group, seeks to limit the proliferation of nuclear weapons. The second, the Australia Group, aims to restrict the spread of chemical and biological weapons. The third, the Missile Technology Control Regime, endeavors to prevent the diffusion of medium- and long-range unmanned delivery systems. The fourth, the Wassenaar Arrangement, has a more expansive mandate and is therefore the primary focus here.[83]

Wassenaar Arrangement

The Wassenaar Arrangement is the direct successor to CoCom, which was eliminated after the end of the Cold War. Wassenaar covers the export of conventional arms and dual-use goods and technologies. The 42 states participating in it include most of the world's technologically advanced democracies, developing economies such as India, as well as a nondemocracy: Russia. Members agree to incorporate the export control lists maintained by Wassenaar into their national policies. Members are also expected to share information on exports of controlled items to nonparticipating states. Whereas CoCom had an explicit target—the Communist bloc—Wassenaar avoids specifying particular threat countries, simply differentiating between members and nonmembers. Unlike its Cold War-era predecessor, Wassenaar does not contain an institutional mechanism to veto potential exports of concern by participating states.[84]

Strengths

- *Inclusivity:* Compared with any other international instrument for technology protection, Wassenaar brings together the largest number of American allies. Its control lists have the potential to influence the export policies of most of NATO as well as American allies in the Indo-Pacific.
- *Expansive coverage:* Among the four multilateral export control regimes, Wassenaar, with its broad mandate, is best positioned to address emerging technologies.[85] Often developed for commercial purposes but carrying significant military potential, these technologies—such as artificial intelligence—are central to the strategic competition between the United States and China.

Weaknesses

- *Voluntary implementation:* Wassenaar gives participating states significant latitude over whether and how they limit the export of items on its control lists. In practice, this "national discretion" means that some members take a rigorous approach to implementing export controls while others allow their companies to freely export sensitive goods and technologies.[86]
- *Consensus driven:* Decisions within Wassenaar require a consensus among its disparate membership.[87] This constrains its ability to rapidly update control lists as technologies evolve and precludes a focus on China, which though outside Wassenaar has friends within.

The Wassenaar Arrangement met for its 20th Plenary session in December of 2014. Wassenaar covers the export of conventional arms and dual-use goods and technologies. (Katharina Schiffl, Estonian Foreign Ministry)

EXTRATERRITORIAL REACH OF U.S. LAW

American domestic laws and regulations directly shape how allies protect technology. This is deliberate and compulsory in the case of the U.S. export control system: A prime example is the International Traffic in Arms Regulations, which controls how allies (and other countries) use select U.S. origin defense-related goods, services, and knowledge. At the same time, American legislation can have a powerful signaling effect. A number of American allies have paid close attention to the Foreign Investment Risk Review Modernization Act of 2018, which strengthened U.S. investment screening procedures with a particular emphasis on the technology sector.

International Traffic in Arms Regulations

The Arms Export Control Act of 1976 set in motion ITAR, a regulatory regime governing U.S. exports of defense-related technology. The U.S. State Department manages the granting of licenses to export under ITAR. Over time, ITAR has evolved to provide the United States with an unprecedented level of control over technology outflows to allies. As one observer notes, "the system has moved from controlling tangible end items of military equipment, to components, to technology, to knowledge of that technology, to any service done to that equipment."[88]

Strengths

- *Comprehensive:* A holistic approach to securing U.S. technology exports is well warranted in today's era of strategic competition with China. Simply protecting major U.S. defense platforms or components would be insufficient.

Weaknesses

- *Lack of differentiation:* With the exception of Canada, the ITAR regime as currently structured fails to differentiate between U.S. allies and other countries. Among its allies, and again excluding Canada as well as the United Kingdom and Australia, the United States applies the same treatment under ITAR regardless of demonstrated commitment to protecting technology.
- *Perverse incentives:* ITAR's lack of differentiation coupled with its comprehensive reach has generated major obstacles to technology cooperation between the United States and its allies. The reporting burdens associated with ITAR disincentivize collaborations involving U.S. technology and persons: Ally companies fear becoming caught up in American export control regulations that would jeopardize commercial

business opportunities. When collaboration occurs, these companies have a strong incentive to keep their best technology at home, lest American modifications to their technology render it subject to ITAR.[89]

The strengths and weaknesses of ITAR are generally replicated across the U.S. export control system, including the Export Administration Regulations (EAR) maintained by the Department of Commerce, which perform a similar function with respect to commercial and dual-use technology and items.

Foreign Investment Risk Review Modernization Act

In 2018, the United States enacted landmark legislation to strengthen its foreign investment screening procedures. Titled the Foreign Investment Risk Review Modernization Act, this legislation was primarily motivated by mounting concerns in Congress and the executive branch regarding China's acquisition of U.S. technology through legal means.[90] FIRRMA expands the type of transactions subject to national security review by the Committee on Foreign Investment in the United States, an interagency body. The new law also creates a mandatory filing requirement in some cases and opens the door to differential treatment of certain countries and investors.[91] From its introduction as a bill in 2017 to its passage in 2018 to its subsequent implementation by the Treasury Department, FIRRMA has attracted considerable interest from American allies.

Strengths

- *Signaling effect:* Through FIRRMA, Washington has conveyed an unmistakable message to allies: Take technology protection seriously. Coinciding with the debate, passage, and implementation of FIRRMA, a number of U.S. allies either blocked individual Chinese transactions or moved to put in place tougher investment screening procedures.[92] In at least one U.S. ally, Israel, FIRRMA has also signaled to technology startups that bringing on Chinese investors carries considerable risk if they seek to enter the American market.[93]

Weaknesses

- *Inadequate discrimination:* FIRRMA as implemented by the Treasury Department carves out a potential exit lane for U.S. allies. This exit lane is confined to "excepted foreign states," a category that currently includes Australia, Canada, and the United Kingdom. The selection of these three allies is predicated on their existing investment screening processes and willingness to cooperate with the United States in this area. However, to qualify for exemption from U.S. national security review, transactions involving these allies must fulfill a second criteria: The individual investor is deemed low-risk and will not possess a controlling stake.[94] Motivated by genuine concerns about opaque ownership structures, this narrow offramp prioritizes maximum risk mitigation over lowering barriers to capital inflows from allies that could benefit America's technology sector and broader economy.
- *Limited replicability:* The policy tools strengthened by FIRRMA are rooted in America's system for national security review of foreign investments. These tools are not necessarily replicable in other national contexts. Rather than serve as an exact model for allies to emulate, FIRRMA is more suitable as a jumping off point for discussions with allies on how to close off points of technology leakage using their own domestic policy mechanisms.

BILATERAL AND MINILATERAL CONSULTATIONS

To align technology protection with allies, Washington also leverages bilateral and minilateral consultations. Some of these are long-standing—for example, since 2007, the United States and Japan have held regular talks under the umbrella of the Bilateral Information Security Consultations (BISC), with the aim of safeguarding advanced defense systems and technology, as well as general classified information.[95] More recently, the United States has refocused dozens of bilateral counterproliferation dialogues to address China's global pursuit of cutting-edge technologies with military application.[96] In parallel, Washington has sought to promote the sharing of threat information and best practices across a group of 15 advanced industrial nations through the Multilateral Action on Sensitive Technologies (MAST) process.[97] Going forward, U.S. consultations with allies appear set to take on a capacity-building function in order to ensure that convergent threat perceptions—if achieved—can translate into effective action to stem technology loss to China.

Strengths

- *Speed:* U.S. action through large-scale international groupings is generally slow and cumbersome. By contrast, working bilaterally with allies can yield rapid results, in part by leveraging existing mechanisms for alliance management designed to translate policy dialogue into concrete outcomes. Minilateral consultations, though less conducive to swift action than bilateral discussions, remain agile compared with multilateral export control regimes like Wassenaar.

- *Disproportionate impact:* Leadership in some critical technologies such as semiconductor manufacturing equipment (SME) is concentrated among a small number of U.S. allies.[98] In these instances, minilateral and even bilateral consultations can have an outsized impact in denying China access to technologies that could underpin its future commercial prowess and military effectiveness.

Weaknesses

- *Absent incentives:* Bilateral and minilateral consultations with allies on technology protection can help close gaps in threat perceptions. However, these dialogues lack positive incentives for allies to take economically painful steps involving China, such as forgoing technology investment, limiting exports, and reducing research collaborations. The absence of positive incentives remains a major impediment to aligning protection policies with U.S. allies, even when threat assessments converge.

America's current approach to allies around innovation and technology protection features points of strength and weakness. What most stands out is that no mechanism for engaging U.S. allies can singularly serve as a foundation for an alliance innovation base. Highly developed frameworks intended to backstop cooperation with allies on innovation—the TTCP and NTIB—lack scalability. They function relatively well precisely because membership remains strictly limited. No comprehensive model emerges from American engagement with allies on technology protection either. The most promising U.S. instruments—bilateral and minilateral consultations—remain devoid of the types of positive incentives central to an alliance innovation base. To build a community of technology innovation and protection in concert with its allies, the United States will need a more expansive toolkit. Identifying new instruments for engaging allies requires an in-depth understanding of their perspectives—the focus of the next chapter of this report.

Chapter 4: The View From America's Allies

By definition, an alliance innovation base requires the energetic participation of America's allies. It is critical to take ally perspectives into account from the outset—otherwise the United States risks putting forward a vision for a community of technology innovation and protection that will fail to resonate outside Washington. Specifically, American policymakers should make an effort to understand what allies want, what allies can provide, and the state of existing allies' technology protection mechanisms.

The following findings focus on four U.S. allies: Japan, Australia, Israel, and Norway. These four countries provide a basis for developing an approach that accounts for a wide spectrum of ally external threat perceptions, approaches to technology protection, approaches to technology innovation and national security, and potential contributions to and desired

American policymakers should make an effort to understand what allies want.

benefits from an alliance innovation base. Of the four countries surveyed, the authors visited three: Japan, Israel, and Norway. These research trips provided unique insight through interviews with government officials, military officers, business representatives, investors, think tank experts, and academics. The analysis in this section captures information gathered from nearly 40 off-the-record interviews.

Japan

EXTERNAL THREAT PERCEPTIONS

Tokyo is, in many respects, at the geographic and economic frontline of competition with China. The Japanese government is closely aligned with Washington's threat perception. In particular, Japan has identified Beijing's military-civil fusion framework, lack of data privacy, digital repression, and unfair economic competition as areas of concern. After the 2010 Chinese embargo of rare earth mineral exports to Japan, Tokyo also became acutely aware of the need for supply chain integrity and insulation from coercive economic power.[99] More generally, Japan sees maintaining its technological supremacy as essential to its position vis-à-vis China.[100]

APPROACH TO TECHNOLOGY PROTECTION

Investment screening

There is no exact CFIUS counterpart in Japan, but both the Ministry of Economy, Trade, and Industry (METI) and the Ministry of Finance have high visibility on the issue of Chinese investment in sensitive Japanese commercial sectors. Tokyo has been heavily influenced by the recent FIRRMA legislation and a 2018 DIU report on how China uses investments to steal innovative technology.[101] Japan's parliament, the Diet, recently lowered the ownership stake threshold required to trigger foreign investment screening from 10 percent to 1 percent in 12 strategic sectors.[102]

Export controls

Japan has recently developed a new approach to securing critical technology. This approach expands the scope of Japanese export controlled technology to largely mirror the 14 categories of crucial emerging technology listed in the U.S. Export Control Reform Act (ECRA).[103] In addition to traditional military and select dual-use items, the Japanese government is expanding coverage to technology that is fundamental to the defense industrial base, including products developed by startups and universities. Moreover, Tokyo appears open to leveraging its critical role in certain supply chains—particularly semiconductor manufacturing equipment—to slow China's technology ascent.

Research integrity

As in the United States, foreign researchers in Japan are a potential weak link in technology protection. Chinese students are the largest group of foreign researchers at universities.[104] METI and the Ministry of Justice have begun to address the risks associated with foreign researchers, mainly drawing from the processes in place in American universities. However, there are major obstacles to implementing an effective vetting system in Japan. For example, since Japan's foreign intelligence apparatus is less robust than that of the United States, Tokyo has less capacity to vet incoming researchers. Labs often delegate the management of confidential data to researchers even if they are foreign, seriously increasing the risk of intellectual property and data theft.[105] Universities in Japan tend to lack an accurate threat perception and are reluctant to move aggressively on this issue.

APPROACH TO TECHNOLOGY INNOVATION AND NATIONAL SECURITY

Because of Imperial Japan's actions before and during World War II and the subsequent demilitarization of Japan under U.S. occupation, Japanese companies and research labs generally do not want to be perceived as cooperating with the Ministry of Defense or working on military-related issues. The only reliable exceptions are heavy-industry subsections of large Japanese conglomerates. Therefore, Japan's technology cooperation with the United States on defense has been almost

As the world's third largest spender on R&D, Japan is an important counterweight to China's scale advantage.

entirely focused on big-ticket joint R&D projects, such as codeveloping the SM-3 Block IIA Interceptor[106] and maintenance, repair, overhaul, and upgrade support for F-35s delivered to Japan.[107] The Ministry of Defense is often unable to leverage cutting-edge commercial sector technology in the way that some of its ally counterparts can. Many Japanese small and medium enterprises reportedly possess technology that would be useful for national security purposes but find that their own scale and compliance issues limit the profitability of the domestic defense market.[108]

The U.S. Navy successfully tested an SM-3 Block IIA Interceptor in December 2018. Japan's technology cooperation with the United States on defense has been largely focused on big-ticket joint R&D projects, such as codeveloping the SM-3 Block IIA Interceptor. (U.S. Army)

POTENTIAL CONTRIBUTIONS TO AN ALLIANCE INNOVATION BASE

Because of Japan's high standing with many U.S. allies, its involvement would help lend credibility to an alliance innovation base. A validating voice from Japan in parallel with the United States would also help to promote tougher technology protection across American alliances.

As the world's third largest spender on R&D, Japan is an important counterweight to China's scale advantage.[109] Even though it has some challenges with information security writ large, Japan has made improvements to its oversight of industrial security and can still maximize its pockets of excellence to leverage comparative technological advantages. Japanese companies are already working on technology that would be useful to an alliance innovation base, including select hypersonic capabilities and 5G network virtualization.[110] Japan has trusted cutting-edge facilities capable of coproduction and maintenance on the SM-2, SM-3, and Patriot missile systems.[111]

DESIRED BENEFITS FROM AN ALLIANCE INNOVATION BASE

Japan is looking for increased market opportunities in the United States as well as in the markets of allies where there is not yet a large Japanese presence. It is also looking for the next marquee collaboration with the United States in the national security domain after the SM-3 Block IIA project. Possible projects of interest to Tokyo could include hypersonic defense, the replacement for the F-2 fighter jet, and counter unmanned aerial and undersea vehicle capabilities. On technology protection, Japan regards an alliance innovation base as a vehicle to advance new multilateral export controls against China in targeted areas.

Australia

EXTERNAL THREAT PERCEPTIONS

Both Australia's 2016 Defence White Paper and 2017 Foreign Policy White Paper identify China as a destabilizing force in the Indo-Pacific and the primary international challenge for Australian policymakers over the next several decades.[112] Recent high-profile news stories about China seeking to co-opt, install, and censor Australian members of Parliament have further exacerbated domestic political concerns about Chinese influence in Australia.[113]

APPROACH TO TECHNOLOGY PROTECTION

Investment screening

Australia's primary investment screening body is the Foreign Investment Review Board (FIRB). Established one year after the creation of CFIUS in the United States, FIRB considers national security concerns as one of multiple criteria when determining whether foreign investments are in the Australian national interest.[114] Though FIRB increased the threshold of state ownership necessary to be considered a foreign government investor from 15 percent to 20 percent in 2015, it is clearly attentive toward Chinese investment. In response to China's 2017 National Intelligence Law, FIRB declared that Chinese companies are inherently not private.[115] Still, while FIRB automatically reviews investment by all foreign state-owned enterprises (SOEs), the terms of the 2014 Australia-China free trade agreement provide FIRB screening exemptions for the first $730 million of investment from private Chinese companies into "non-sensitive sectors."[116]

Export controls

In Australia, the Defence and Strategic Goods List, which includes both military goods and several categories of dual-use technologies, governs export controls.[117] In 2012, the Defence Trade Controls Act updated Australia's export control regime to include the prohibition of intangible supply of controlled technology, for example, digital transfer of a photograph with controlled information. In 2017, research collaborations between prominent Australian universities and Chinese SOEs with links to the PLA came to light.[118] A subsequent independent review of Australia's export control system in 2018 acknowledged gaps in the Defence Trade Controls Act.[119] Notably, Australia's defense export controls remain technology based, as opposed to targeting specific entities—a major difference from the U.S. system.[120]

Australia's defense export controls remain technology based, as opposed to targeting specific entities—a major difference from the U.S. system.

Research integrity

Because of the blurred lines caused by China's military-civil fusion framework, Australian universities have a difficult time evaluating the threats posed by institutions in China that are affiliated with the PLA.[121]

In addition to the often obscured nature of connections between the PLA and universities in China, the economic opportunities presented by Chinese-funded research partnerships are difficult for Australian universities to resist. Researchers sponsored by the PLA often conceal their affiliation and work on sensitive research projects such as hypersonic technology and then return to China with the data.[122] While all Five Eyes countries have hosted a surprising number of PLA-affiliated researchers, Australia in particular has had the most.[123] Leveraging both government and university expertise, the University Foreign Interference Taskforce released a comprehensive set of guidelines at the end of 2019 to safeguard against foreign interference without weakening the contributions of Chinese researchers to Australia's economy.[124] The task force made an explicit decision to frame the initiative as protecting research integrity instead of explicitly countering a threat from China.

APPROACH TO TECHNOLOGY INNOVATION AND NATIONAL SECURITY

Similar to the United States, Australia has a growing appreciation for the role of commercial technology in addressing national security challenges. The new approach to defense innovation laid out in the 2016 Defence White Paper is focused on using collaboration with cutting-edge companies, particularly SMEs, to maintain Australia's regional technological advantages.[125] Australia has put this into practice by standing up the Next Generation Technologies Fund, which offers flexible funding open to companies of all sizes, and creating a Defence Innovation Hub, which is designed to assist companies working on specific defense innovation priorities at the prototyping phase.[126] Australia also collaborates with the United States on basic research through its Defence Science and Technology organization and with Five Eyes through the Technical Cooperation Program.[127]

POTENTIAL CONTRIBUTIONS TO AN ALLIANCE INNOVATION BASE

Australia is well regarded by a broad set of U.S. allies, which makes it an effective diplomatic voice to amplify the benefits of an alliance innovation base to an expansive network of countries. Australia's participation would improve threat intelligence-sharing, especially on Chinese academic espionage, given its depth of experience on this issue. Exercises like Talisman Sabre showcase Australia's strengths in the development of operational concepts, wargaming, and joint testing,[128] in addition to collaborative platform development like the MQ-4C Triton.[129] Additionally, the Australian defense industry has important pockets of excellence that would make it a pillar of an alliance innovation base. Australia has large testing ranges for weapon systems and vast quantities of rare earth minerals essential to the production of critical defense hardware, and is seeking to grow its defense exports in areas of critical technology including phased array radars, niche space capabilities, and quantum computing.[130]

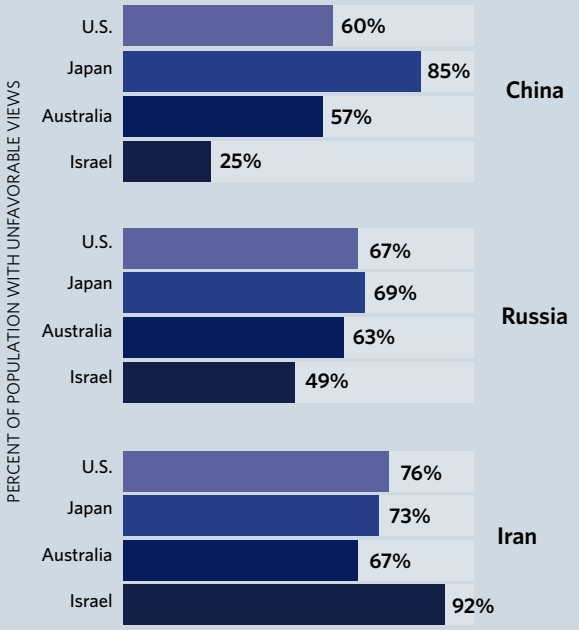
DESIRED BENEFITS FROM AN ALLIANCE INNOVATION BASE

Australia may initially see limited incentive to participate in an alliance innovation base given its membership in the NTIB. But given the Australian government's aspiration to become one of the top 10 global defense exporters, more open access to U.S. and allied defense markets is a major impetus for Australia to join the United States in building this new community of technology innovation and protection.[131] So is the prospect of privileged treatment for meeting defined technology

An experimental supersonic aircraft test is conducted in October 2005 at the Woomera Test Range in Southern Australia, the world's largest testing range. Australia's large testing ranges for weapon systems and aircraft would be a unique contribution to an alliance innovation base. (Japan Aerospace Exploration Agency via Getty Images)

protection standards. Although the new CFIUS reform gave Australia "excepted state" status,[132] Canberra is still unclear on whether this truly translates into more privileged access given the multitude of additional regulatory hurdles to exiting U.S. national security review. Lastly, an alliance innovation base would provide a pathway to accelerate the process of solidifying the Australian technology sector and enable Canberra to gain insight from the United States and other allies on how to reframe existing military problems with commercial technology solutions.

Public Perception in the United States and Allies of China, Russia, and Iran



Just as threat perceptions among U.S. and ally governments diverge, so does public opinion regarding potential countries of concern.

Source: Pew Research Global Indicators. The data for views toward China and Russia is from 2019, while the latest available survey data on views of Iran is from 2015.[133]

Israel

EXTERNAL THREAT PERCEPTIONS

Israel's main defense focus is on existential threats, including Iran and Iranian proxies in Lebanon and Syria, and terror groups in Gaza and the West Bank. The immediacy of these threats largely precludes a focus on potential challenges emanating from China. In fact, Israel views China as an economic opportunity, not a military threat. While there is slowly growing recognition that the China-Iran relationship is detrimental to Israel and that economic entanglement with China renders Israel vulnerable to new coercive pressure, the Israeli government generally discounts the strategic threat from China. Accordingly, Israel's intelligence and law enforcement agencies, though highly capable, are not optimized to address Beijing's pursuit of technology within its borders.

APPROACH TO TECHNOLOGY PROTECTION

Investment screening

After the uproar surrounding China's winning bid to construct and operate Haifa Port's new container terminal, Israel has decided to move forward with creating an investment screening mechanism.[134] How this new mechanism will function remains unclear, but currently, the regulatory body will not cover Israel's dynamic commercial technology sector, in which China has a sizable investment presence.[135] Israel has a strong and natural aversion to regulating what it regards as an economic cornerstone. However, this is problematic given the military application of many commercial technologies pioneered by Israeli startups.

Export controls

Israel does not sell military equipment to China because of backlash from the United States at Israel's attempt to refurbish and sell the Phalcon and Harpy platforms to China in the mid-2000s.[136] However, the export of dual-use technology—a broad and growing category—is far less regulated. International political considerations also have an outsized role in the imposition of export controls due to Israel's sensitive position, so the application of regulations can sometimes be the result of complex political calculus.

Research integrity

Chinese partnerships with Israeli universities are thus far relatively limited. The existing partnership between the Technion—Israel's MIT—and a Chinese university appears to steer clear of technology areas that touch

While there is slowly growing recognition that the China-Iran relationship is detrimental to Israel and that economic entanglement with China renders Israel vulnerable to new coercive pressure, the Israeli government generally discounts the strategic threat from China.

on national security, though funding shortages always elevate the appeal of taking Chinese money.[137] The number of Chinese students in Israel is still relatively low but is growing rapidly.[138]

APPROACH TO TECHNOLOGY INNOVATION AND NATIONAL SECURITY

Israel is a small country that has had to innovate to survive. Nearly the entire country is well aware that its defense cannot be taken for granted, in part because of mandatory national service. Each year, the Israel Defense Forces (IDF) handpicks the nation's sharpest minds and places them in its prestigious signals intelligence and cyber unit. Between reservists and new recruits, highly trained talent is always flowing between the private sector and military. Israel's primary defense science and technology administrative body, Maf'at, coordinates with the larger defense companies, but there is an almost nonexistent barrier between Israel's national security apparatus and commercial sector technology due to the human networks created by mandatory service in the IDF.[139]

POTENTIAL CONTRIBUTIONS TO AN ALLIANCE INNOVATION BASE

Between the IDF's unique function as a tech talent incubator and Israel's density of startups, it has a disproportionate amount to offer to an alliance innovation base. Particular Israeli strengths include autonomous vehicles, missile defense, and countertunnel capabilities. Israel is also an easy place to road test U.S.-promoted initiatives. It has relatively little bureaucracy as a small country used to dealing with emergencies. And singular dependence on the United States inclines Israel to collaborate with Washington wherever possible. Finally, Israel's security realities provide tactical opportunities to test new technology in active operational environments.

DESIRED BENEFITS FROM AN ALLIANCE INNOVATION BASE

Israel remains broadly skeptical of multilateral arrangements and has complicated political relationships with some U.S. allies. It is most likely to be interested in an alliance innovation base as a mechanism to widen security cooperation with Washington. Given the importance of the United States to its security, Israel always looks for opportunities to strengthen the defense elements of the alliance. Beyond defense, Israel might also look for an alliance innovation base to deliver a 5G alternative to Huawei, as some Israeli policy circles remain skeptical about the long-term viability of Nokia and Ericsson.

Norway

EXTERNAL THREAT PERCEPTIONS

Norway's primary security objective is to defend against Russian incursions on its territory and exclusive economic zone—an area approximately the size of western Europe.[140] Oslo has a growing awareness of threats emanating from China. Although Norway has little firsthand experience of China's technology transfer strategy, it is concerned about losing its competitive edge through intellectual property theft and sees China's tactics in action against other countries. Notably, Norway experienced Chinese economic coercion when Beijing boycotted the Norwegian salmon industry for nearly seven years after Liu Xiaobo was awarded the Nobel Peace Prize in 2010.[141] China only normalized relations with Norway after the Dalai Lama visited Oslo and no government officials would meet with him.[142]

APPROACH TO TECHNOLOGY PROTECTION

Investment screening

To date, investment from China in Norway's technology sector has been relatively minimal. Even so, in January 2019, Norway implemented a new regime for reviewing foreign investments based on potential risk to national security. The law defines security broadly, to include financial stability and autonomy.[143] In addition to the regulatory process, as the Norwegian defense industry is extremely export-oriented, companies are much more inclined to welcome foreign investment from other democracies because these countries are more likely to be purchasers of its products.

Export controls

Norway's defense sector is highly export-focused and selective about which countries may receive its products.

Relatedly, Oslo has a sophisticated understanding of U.S. export control regimes, the details of which directly inform Norwegian industry decisions ranging from technology development to compliance systems. When assessing whether to sell equipment, Norway evaluates the abilities of the proposed end-country and its close allies or partners to copy the technology or develop countermeasures. To address the increasingly large portion of military technology that comes from the commercial sector, Norway's export control regime uses the EU's list of what is considered a dual-use item.[144]

Research integrity

At present, security standards at university research labs in Norway appear to vary from lab to lab, but the recent case of two Iranians arrested at the Norwegian University of Science and Technology for leaking weapons of mass destruction-related information to Tehran may catalyze a policy response to standardize protection.[145]

APPROACH TO TECHNOLOGY INNOVATION AND NATIONAL SECURITY

As a small country, Norway focuses on developing niche capabilities. The military, government organizations that fund research, and industry intentionally coordinate to maximize Norway's defense technology capabilities in select areas. In contrast to the U.S. approach, the Norwegian government's emphasis is on building sustainable defense businesses, rather than simply executing project requirements or creating Norwegian jobs. The scale of demand from the Norwegian military is too small to support the domestic defense industry, so the Ministry of Defense is uninterested in funding technology projects that lack export potential. The compact Norwegian defense community leads to close military-industry relationships, shortening the time required to bring technology solutions to the battlefield.

POTENTIAL CONTRIBUTIONS TO AN ALLIANCE INNOVATION BASE

Norway provides disproportionately large contributions to the United States and allies in terms of military technical innovation, including micro unmanned aerial vehicles (UAVs), remote weapons stations, and precision munitions, all of which are currently used by U.S. forces. The Norwegian government plays a major role in cultivating its domestic innovation ecosystem and is well positioned to curate local startups and traditional defense firms in order to develop innovative technology with military utility for the United States and other American allies. Norway is also competitive in niche but important technologies such as autonomous undersea vehicles and missile development. Lastly, Norway's cold-weather environment provides unique conditions for weapons field testing.

DESIRED BENEFITS FROM AN ALLIANCE INNOVATION BASE

The principal benefit Norway would seek to derive from an alliance innovation base would be expanded markets for its defense exports, both in the United States and in other American allies. In addition to market access, Norway would benefit from streamlined compliance regimes to improve the ease of collaboration with allies, including with the United States. Oslo would also use an alliance innovation base as a vehicle to promote and strengthen its commercial technology sector.

SNAPSHOT: POTENTIAL CONTRIBUTIONS AND DESIRED BENEFITS FROM AN ALLIANCE INNOVATION BASE

Country	Potential Contributions	Desired Benefits
Japan	▪ Credibility due to Japan's high standing with other U.S. allies ▪ Validating voice on technology protection ▪ Sizeable counterweight to China's scale advantage in R&D ▪ Expertise in select areas of technology development	▪ Increased opportunities in U.S. and allied markets ▪ New marquee collaboration with United States after SM-3 Block IIA project ▪ Vehicle to advance multilateral export control against China in targeted areas
Australia	▪ Threat intelligence sharing, especially on Chinese academic espionage ▪ Large testing ranges ▪ Significant quantities of rare earth minerals ▪ Niche areas of technology expertise	▪ Access to U.S. and allied defense markets ▪ Privileged treatment for meeting defined technology protection standards ▪ Accelerated solidification of Australian technology sector
Israel	▪ Strength as a technology talent and startup incubator ▪ Leader in cutting-edge dual-use technologies ▪ Low bureaucratic barriers to road-testing U.S.-promoted initiatives ▪ Opportunities to test new technology in an active operational environment	▪ Widened security cooperation with Washington ▪ Non-defense technology solutions, such as a viable 5G alternative to Huawei
Norway	▪ Disproportionately large contribution to military technology innovation ▪ Coordinated curation of domestic startups and defense firms ▪ Strength in select defense technologies ▪ Cold-weather field environment for testing weapons	▪ Expanded opportunities for defense exports in U.S. and allied markets ▪ Streamlined compliance regimes to ease collaboration ▪ Strengthened domestic commercial technology sector

Chapter 5: A Blueprint for an Alliance Innovation Base

Now is the moment for the United States to forge an alliance innovation base. This chapter presents a blueprint for constructing a new community pairing technology innovation and protection. It starts by outlining design principles for an alliance innovation base, then identifies substantive areas for collaboration. The rest of this chapter lays out concrete and actionable recommendations spanning five major lines of effort: strengthening America's toolkit for technology engagement; building ally awareness and capacity; launching new collaborative platforms; creating positive incentives for technology protection; and leveraging the U.S.-Japan alliance.

Design Principles

In previous chapters, this report evaluated America's engagement with allies on technology innovation and protection and conducted in-depth studies of Japan, Israel, Australia, and Norway. Lessons learned regarding the strengths and weaknesses of existing U.S. policy, and the expectations and potential contributions of a diverse set of countries, inform the following design principles for an alliance innovation base.

1. *Adopt a flexible architecture for an alliance innovation base that can accommodate countries with variable threat perceptions and distinct capabilities.* The United States should advance cooperation through a substantial number of bilateral and minilateral mechanisms. Some will operate in parallel while others will intersect. Washington does not need to be at the center of every grouping and should encourage its allies to work together independently as well.
2. *Create tangible economic benefits to incentivize allies to adopt tougher technology protection measures.* The United States should put in place a series of benefits accessible to allies as they take discrete steps to tighten investment screening, strengthen export controls, and enhance scrutiny of academic research involving China.
3. *Focus technology cooperation on solving narrowly scoped problems in order to manage divergent views on the nature of the international threat environment*. With the right scoping, U.S. allies can collaborate to address shared military-operational and technical challenges absent a consensus on whether China, Russia, or Iran constitutes the primary threat to their future security.
4. *Foster a "benefit together" ethos that chips away at deeply rooted preferences for spending and procuring domestically.* This home bias—evident in the United States and many of its allies—constitutes a major impediment to deepening technology cooperation. It will be essential for collaboration under the umbrella of an alliance innovation base to deliver rapid and broad-based gains; otherwise, achieving buy-in within the United States and among America's allies will prove difficult.
5. *Incorporate politicians, publics, and the private sector from the outset to build critical momentum in support of an alliance innovation base.* Moving beyond long-standing preferences for domestic industry and shouldering the short-term costs of technology protection are choices that implicate multiple societal stakeholders. The U.S. executive branch will need to engage these stakeholders early and often, both at home and abroad, in order to successfully advance an alliance innovation base. With protectionism rising at home, American policymakers should in particular emphasize the benefits to U.S. industry: fewer barriers to inbound investment from allies, improved access to ally technology, and reduced compliance burdens—all contributing to enhanced innovation and profitability.

Promising Areas for Cooperation

New alliance collaboration efforts will struggle to gain momentum without specific areas to address. A number of shared national security needs stand out as focal points for initial collaboration. These include:

- *Developing New Approaches to Intelligence, Surveillance, and Reconnaissance (ISR):* In the Indo-Pacific, the Atlantic, and the Middle East, the United States and its allies seek to track the movements of competitors across vast geographic areas. The demand for existing assets will invariably outstrip supply, given the expense and finite number of major ISR platforms.[146] Likewise, collection inputs will continue to overwhelm traditional processing techniques.[147]
- *Diversifying Options for 5G:* Huawei's investment in R&D and its cut-rate pricing[148] have positioned it to dominate the global market in 5G hardware. Yet reliance on a single supplier—particularly one beholden to an autocratic regime, the CCP—risks exposing the United States and its allies to disruption of critical infrastructure, as well as espionage and data exfiltration.[149]

- *Expanding Rare Earth Supply Chains:* With China dominating the production and refinement of rare earth minerals, the United States and its allies remain highly susceptible to disruptions of supply, whether due to Beijing's deliberate policy choices[150] or destabilizing developments within China, such as the coronavirus.[151]
- *Promoting Trusted Sources of Semiconductors:* The United States and its allies have special security needs for the semiconductors used by their militaries and intelligence communities. Yet trusted semiconductor foundries are scarce given that commercial demands vastly outpace boutique government purchases. Constructing new chip factories costs billions of dollars,[152] rendering trusted foundries beyond the reach of many allies.
- *Addressing Digital Disinformation:* The software tools required to generate and promote digital disinformation have rapidly become widely available and relatively easy to use.[153] Online disinformation campaigns targeting the United States and its allies can discredit democratic governance and accentuate polarization.[154]
- *Building Military Network Resiliency:* U.S. and ally combat effectiveness hinges on seamless flows of information for rapid maneuver and precise targeting. However, multiple competitors have invested heavily in tools to attrit the networks that have underpinned the battlefield edge the United States and its allies have long enjoyed.[155]
- *Pooling Cross-National Data Sets:* Large volumes of data provide advantage for advanced analytics, artificial intelligence, and machine learning.[156] Collectively, the United States and its allies possess unmatched reservoirs of data. Today, however, platforms that allow for secure sharing of appropriately curated data between governments do not exist.

Recommendations for Galvanizing an Alliance Innovation Base

No single action by the United States will summon an alliance innovation base into existence. Rather, the task for Washington is to construct this community of technology innovation and protection link by link. The following recommendations advance a blueprint for moving forward, structured around five main lines of effort: strengthening America's toolkit for technology engagement; building ally awareness and capacity; launching new collaborative platforms; creating positive incentives and removing barriers to cooperation; and leveraging the U.S.-Japan alliance.

STRENGTHEN AMERICA'S TOOLKIT FOR TECHNOLOGY ENGAGEMENT

- Increase resources for major technology scouting programs
- Leverage U.S. Defense Attaché Offices
- Internationalize startup-focused engagements

Existing U.S. mechanisms for technology engagement with allies remain inadequate. To strengthen its toolkit, Washington should:

- *Increase resources for major technology scouting programs.* Inside the Defense Department, the Office of Naval Research Global and the Foreign Comparative Testing Program could, with additional staff and funding, ramp up cooperative activities with American allies. These organizations have demonstrated their effectiveness over a sustained period, ensuring that extra resourcing would enhance U.S. access to ally technology. Defense Department leadership should work with Congress to plus up these two organizations in the next National Defense Authorization Act and defense appropriation.
- *Leverage U.S. Defense Attaché Offices.* The United States maintains Defense Attaché Offices at most embassies overseas. Traditionally, these offices have functioned as points of liaison with host country militaries. However, they could be used to augment programs such as ONR Global and FCT. To this end, the Defense Department should add technology scouting to the responsibilities of defense attachés at U.S. embassies in allies with robust innovation ecosystems. In turn, the uniformed services should encourage officers with significant R&D or acquisition backgrounds to consider a tour as defense attachés, generate training programs for them in advance of these assignments, and cue tasks for them once posted to U.S. embassies.
- *Internationalize startup-focused engagements.* Since 2015, the Defense Department has made a sustained effort to encourage U.S. startups to develop solutions to military challenges. Examples include the establishment of the Defense Innovation Unit, new platforms for engaging startups around the requirements of a particular service or combatant command,[157] and pitch days.[158] This effort should become increasingly internationalized over time. The recent launch of an Allied Space Accelerator in partnership with the Netherlands and Norway[159] is a promising step and, if successful, will serve as a model for working with ally startups

in other technology areas. Beyond this, the Defense Department should gradually take DIU global—beginning with regular DIU road shows to allies and culminating with one or more DIU outposts in ally innovation hubs overseas.[160]

BUILD ALLY AWARENESS AND CAPACITY

- Upgrade information sharing with ally governments
- Promote broad-based awareness of China's actions
- Build ally capacity to protect technology

U.S. cooperation with allies to protect technology has made important strides in recent years, but significant obstacles remain to aligning policy measures in this area. To overcome existing obstacles, the United States should:

- *Upgrade information-sharing with ally governments.* Across America's allies, the United States has broadly improved awareness of Beijing's technology ambitions through the Multilateral Action on Sensitive Technologies process and numerous bilateral dialogues. What allies lack today is a granular understanding of the exact technologies Washington seeks to deny China. As the U.S. government as a whole continues to grapple with this thorny question, it should make releasable to allies a more targeted list compiled by the Defense Department's Protecting Critical Technology Task Force.[161] Another area where allies would benefit from improved information-sharing is addressing academic espionage. The State Department should work with the intelligence community to develop a database of high-risk institutions and researchers in China and make this resource available to U.S. allies. The database would help ally governments to scrutinize existing partnerships with Chinese academic institutions and backstop tighter visa screening.
- *Promote broad-based awareness of China's actions.* Expanding information-sharing with ally governments is necessary but insufficient, as some policies to protect technology will require support from ally politicians, publics, and the private sector. The United States should undertake a comprehensive public diplomacy campaign to highlight China's pursuit of technology within the innovation ecosystems of its allies. Key elements of this campaign would include declassifying U.S. intelligence and providing it to ally media in order to showcase Beijing's activities; encouraging ally governments to conduct or sponsor unclassified studies of how China's technology transfer strategy plays out within their economies;[162] and funding globally oriented, open source research on Chinese academic espionage to complement information flows through government channels.[163]
- *Build ally capacity to protect technology.* China's global pursuit of technology differs sharply from traditional external threats such as terrorism and narrowly scoped espionage. In many U.S. allies, intelligence and law enforcement agencies remain ill-equipped to track and counter Beijing's ever-shifting attempts to acquire technology within their jurisdictions. The United States is now retooling its domestic security apparatus to meet this challenge[164] and should help allies do the same, where possible. Washington can build ally capacity to mitigate the risk of academic espionage through a hybrid approach that incorporates nongovernmental actors. Specifically, the State Department should organize visits by American academic administrators to the top technology universities located in U.S. allies. The visits would allow for dialogue on the risks posed by China to the integrity of the research enterprise and how to move forward while upholding academic norms of open exchange as much as possible.

LAUNCH NEW COLLABORATIVE PLATFORMS

- Establish bilateral national security innovation funds
- Form a military test facility consortium
- Launch a cross-national platform to build new companies

The United States should expand the set of national security-related platforms by which it collaborates with allies on technology. To build out the architecture for an alliance innovation base, Washington should:

- *Establish bilateral national security innovation funds.* The Department of Defense should work with ally ministries of defense to stand up bilateral funds that would support rapid technology development and prototyping in mutually prioritized areas. This could take multiple forms—from quick-fire seed projects to road test promising but high-risk ideas to opening incubators for startups innovating at the nexus of defense and commercial applications.[165] Resourcing for these bilateral funds could originate from defense sale offset obligations, incremental increases in host nation support, or multiyear military aid packages, depending on the ally involved. At a time when burden-sharing has emerged as a point of contention between the United States and some of its allies, American requests

for additional contributions could become more palatable to allies if channeled into bilateral national security innovation funds.

- *Form a military test facility consortium.* A critical step in developing technology for defense applications is testing. Compact or crowded geographies constrain the domestic test options of some U.S. allies. Others possess unique facilities. For example, Australia's remote and vast Woomera Range Complex is well suited for hypersonics,[166] while Norway's Andøya Test Center offers real-world arctic conditions.[167] American military test ranges, though unmatched in number and sophistication by any ally, must handle a much higher workload. Accordingly, the United States and its allies would collectively benefit from forming a new test facility consortium. Participating governments would pool access to high-demand, low-availability equipment and ranges in exchange for the sharing of test results with other members of the consortium. Ultimately, the consortium would serve to accelerate the fielding of technologies essential to the security of America and its allies.
- *Launch a cross-national platform to build new companies.* The United States and select ally governments should bring together innovators and entrepreneurs from participating countries to develop new businesses around specific national security themes. Cross-national teams physically located at the platform, or foundry, would receive public and private sector funding. Investors would encourage business models that straddle national security and commercial markets. The United States should host this foundry in a major American innovation hub, taking advantage of existing international academic partnerships with U.S. allies, such as the joint Cornell-Technion (Israel) venture in New York City. Although the membership of the platform could grow over time, starting with a limited group of U.S. allies would maximize success. Japan and Israel are two strong candidates, as both seek to deepen technology cooperation with the United States, and each other.[168]

CREATE POSITIVE INCENTIVES FOR TECHNOLOGY PROTECTION

- Reduce barriers to investment in the United States for allies committed to technology protection
- Invite U.S. allies to join an "ITAR Free Zone"
- Amend the Buy American Act

A critical function of an alliance innovation base is to generate benefits that offset the immediate costs of technology protection. Many of these benefits would have the dual advantage of lowering barriers to collaboration between the United States and its allies. To create well-defined incentives, Washington should:

- *Reduce barriers to investment in the United States for allies committed to technology protection.* The United States should make clear what technology protection standards its allies must meet to qualify as "excepted states" in the future. The information-sharing and capacity-building efforts discussed above should explicitly aim to help allies cross this threshold. However, under the current Treasury Department regulation, even becoming an "excepted state" carries limited benefit, as any controlling stake investment in the United States still triggers an interagency review. Starting with the current "excepted states," the Treasury Department, working with the intelligence community, should compile a "white list" of major investors that pose minimal risk to national security. Entities on this "white list" should be exempt from investment screening regardless of controlling stake. This "white list" would grow in tandem with the number of "excepted states."
- *Invite U.S. allies to join an "ITAR Free Zone."* Washington should announce its intent to eliminate ITAR licenses for allies that meet concrete technology protection standards. Qualifying allies would receive an ITAR waiver covering not only bilateral transfers of defense-related goods, services, technology, and knowledge, but also retransfers to other qualifying American allies. This "ITAR Free Zone" would require wrenching bureaucratic changes in the United States but generate strong incentives for allies to elevate technology protection—and have the ancillary advantage of reducing a major impediment to technology cooperation. An "ITAR Free Zone" could also pave the way for an analogous effort focused on other elements of the U.S. export control system that impose significant reporting burdens on U.S. allies.

- *Amend the Buy American Act*. Enacted in 1933 and updated many times since, the Buy American Act encourages the U.S. government to favor domestic over foreign producers. Although allowing for exceptions based on factors such as cost,[169] the Buy American Act generally serves as an obstacle to U.S. allies seeking to sell into the American defense market. Congress should enact legislation amending the Buy American Act that would extend less discriminatory treatment to U.S. allies that meet enhanced technology protection standards. Today such legislation would confront formidable domestic political headwinds and almost certainly fail. But as the U.S.-China technology competition continues to heat up, Washington will be increasingly tempted—if not compelled—to use the potential inducement of its defense market to motivate allies to its side. One additional benefit of amending the Buy American Act would be to inject greater competition into the market for U.S. defense procurement, which would enhance incentives to innovate and create downward pressure on prices.

LEVERAGE THE U.S.-JAPAN ALLIANCE

- Convene a "Hard Problems Seminar"
- Launch a U.S.-Japan national security innovation fund
- Announce a government data pooling partnership
- Spearhead multilateral export controls on semiconductor manufacturing equipment
- Initiate a bilateral dialogue on research integrity

Japan is uniquely positioned to work with the United States to advance an alliance innovation base given its deep-seated concerns about China's technology ascendance, intense interest in technology protection, and enduring strengths in incremental types of innovation. Washington and Tokyo should leverage their alliance to launch a series of new initiatives, including cooperative efforts the United States could subsequently replicate with other allies. In practice, the United States and Japan should:

- *Convene a "Hard Problems Seminar."* This seminar would bring together officials from each side's national security, diplomatic, technology, and commercial communities to identify and refine shared alliance challenges such as limited 5G options and vulnerable rare earth supply chains. Although the United States and Japan have numerous bureaucratic touch points, this type of convening would take a step back from the daily work of alliance management and provide a forum for a diversity of perspectives rarely represented at bilateral meetings. The seminar would also depart from the scripted format of most official gatherings and employ design thinking methodologies common in the private sector.
- *Launch a U.S.-Japan national security innovation fund.* This fund could support bilateral projects using technology to address the alliance challenges framed by the "Hard Problems Seminar." The current host nation support agreement between Washington and Tokyo expires in March 2021.[170] The United States and Japan should commit to channel a major portion of any increase into a new bilateral national security innovation fund. This could help to diminish pushback within Japan against a higher level of financial support for U.S. forces stationed within its borders.
- *Announce a government data pooling partnership.* The United States and Japan should unveil an initiative to pool anonymized data sets held by each government. Companies and researchers from both countries could tap into the resulting bilateral reservoir of data, which would help to partially offset China's scale advantage in this area. A government data pooling partnership would be high-profile and could become the next marquee U.S.-Japan technology project now that cooperation to develop a joint missile interceptor has come to fruition.[171]
- *Spearhead multilateral export controls on semiconductor manufacturing equipment*. A critical bottleneck in China's bid for technology supremacy is its domestic semiconductor industry, which remains "years behind"[172] global pacesetters. To leap from laggard to leader, Beijing will need to import semiconductor manufacturing equipment from overseas. The United States and Japan, along with the Netherlands, comprise 90 percent of the market for the tools and equipment that go into chip fabrication facilities. This concentration of market share creates an opportunity for Washington and Tokyo to spearhead new export restrictions on the sale of SME to China.[173] Working with Japan from the outset, the United States is more likely to convince the Netherlands to implement such restrictions.
- *Initiate a bilateral dialogue on research integrity.* In Japan as in the United States, how to address China's academic espionage remains an outstanding question, with concerns about infringing on norms of open exchange complicating potential government responses. Washington and Tokyo should convene

a regular dialogue of administrators from their top technology universities to discuss the thorny problem of Chinese researchers and institutional partnerships. Over time, this dialogue could develop a set of best practices and feed into ongoing discussions among international research universities on how to uphold research integrity.

The United States is well positioned to execute some of these recommendations today. Others will require a level of coordinated economic statecraft across the executive branch that is currently lacking. Washington should move forward where it can now, recognizing that it will have to create new interagency processes and bureaucratic constructs as it builds a new community of technology innovation and protection with its allies.

Chapter 6: Conclusion

In the contest with China to scale the commanding technological heights of the 21st century, the United States benefits from a unique asset: its allies. Now is the moment for Washington to translate this asset into an enduring technological advantage by standing up an alliance innovation base. Combining technology innovation and protection will create a community that appeals to allies with diverse threat perceptions, capabilities, and needs.

An alliance innovation base by necessity will involve disparate activities and a multitude of structures. An interesting parallel is the networked security architecture that America has long promoted in the Indo-Pacific. What began as small-scale and often trilateral meetings among the United States and its allies and partners has since blossomed into a much more robust set of cooperative arrangements. Increasingly, American allies and partners network with each other, independent of the United States. This security architecture has empowered U.S. allies and partners, concerned about blowback from China, to move forward at their own pace.[174]

An alliance innovation base could evolve along a similar trajectory as a thickening web of cooperation spanning the United States and its allies. Over time, for Washington and some allies, it could serve as a proving ground for something more: a technology alliance.[175]

Endnotes

1. China Power Team, "Is China a global leader in research and development?," Center for Strategic and International Studies, January 31, 2018, https://chinapower.csis.org/china-research-and-development-rnd/.

2. Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation" (Defense Innovation Unit Experimental (DIUx), January 2018), https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf.

3. Fred Strasser, "Senator Mark Warner: Meeting the Challenge of China," U.S. Institute of Peace, September 26, 2019, https://www.usip.org/publications/2019/09/senator-mark-warner-meeting-challenge-china; Jeffrey Dastin and Nandita Bose, "U.S. urged to invest more in AI; ex-Google CEO warns of China's progress," Reuters, November 4, 2019, https://www.reuters.com/article/us-usa-artificial-intelligence/u-s-urged-to-invest-more-in-ai-ex-google-ceo-warns-of-chinas-progress-idUSKBN1XE1UD; "Biennial Report Shows US at Risk of Losing Global R&D Leadership to China," American Institute of Physics, January 23, 2018, https://www.aip.org/fyi/2018/biennial-report-shows-us-risk-losing-global-rd-leadership-china; and Ratner, Kliman, Blume, Doshi, Dougherty, Fontaine, Harrell, Rasser, Rosenberg, Sayers, Singh, Scharre, and DeJonge Schulman, "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific."

4. Alan Rappeport, "In New Slap at China, U.S. Expands Power to Block Foreign Investments," *The New York Times*, October 10, 2018, https://www.nytimes.com/2018/10/10/business/us-china-investment-cfius.html.

5. Advanced economy here is defined as membership in the Organisation for Economic Co-Operation and Development (OECD). Of the 35 other OECD members, 27 have a formal treaty alliance with the United States. A handful of others such as Israel and Sweden have defense partnerships with the United States that amount to de facto alliances.

6. For example, Japan, Europe (primarily the Netherlands), and South Korea together make up roughly 42 percent of global semiconductor sales and pour 7 percent to 14 percent back into R&D, while Germany, France, and the UK together hold about 10 percent of autonomous maritime patents, and Korea and Japan each hold roughly 5 percent putting all of them in the top 10 globally. "Beyond Borders: The Global Semiconductor Value Chain" (Semiconductor Industry Association, May 2016), https://www.semiconductors.org/wp-content/uploads/2018/06/SIA-Beyond-Borders-Report-FINAL-June-7.pdf; and Bradley Martin, Danielle C. Tarraf, Thomas C. Whitmore, Jacob DeWeese, Cedric Kenney, Jon Schmid, Paul DeLuca, "Advancing Autonomous Systems: An Analysis of Current and Future Technology for Unmanned Maritime Vehicles" (RAND Corp., 2019), https://www.rand.org/pubs/research_reports/RR2751.html.

7. Anja Manuel, Pavneet Singh, and Thompson Paine, "Compete, Contest, and Collaborate: How to Win the Technology Race with China" (Freeman Spogli Institute for International Studies, October 17, 2019), https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/manuel_et_al_china_tech_race_101619_final_updated_0.pdf; and Charles W. Boustany Jr. and Aaron L. Friedberg, "Partial Disengagement: A New U.S. Strategy for Economic Competition with China," NBR Special Report #82 (The National Bureau of Asian Research, November 2019), https://www.nbr.org/wp-content/uploads/pdfs/publications/sr82_china-task-force-report-final.pdf.

8. Michael Griffin quoted in "Department of Defense Launches Allied Prototype Initiative," Office of the Under Secretary of Defense for Research and Engineering, press release, January 13, 2020, https://www.cto.mil/wp-content/uploads/2020/01/allied-prototype-initiative.pdf.

9. Noa Landau, "Israel Panel to Monitor Chinese Investments Following U.S. Pressure," *Haaretz*, October 30, 2019, https://www.haaretz.com/israel-news/.premium-israel-to-form-committee-to-monitor-chinese-investments-following-u-s-pressure-1.8058754; and Matthew P. Goodman and Stephanie Segal, "With or Without Them," Center for Strategic and International Studies, December 18, 2018, https://www.csis.org/analysis/or-without-them.

10. For example, Huawei/5G debate in the UK and Australia, U.S. pressure on Israel to screen People's Republic of China investment, even as significant tech cooperation occurs; Daniel Estrin and Emily Feng, "There's A Growing Sore Spot in Israeli-U.S. Relations: China," NPR, September 11, 2019, https://www.npr.org/2019/09/11/757290503/theres-a-growing-sore-spot-in-israeli-u-s-relations-china; and Julian E. Barnes and Adam Satariano, "U.S. Campaign to Ban Huawei Overseas Stumbles as Allies Resist," *The New York Times*, March 17, 2019, https://www.nytimes.com/2019/03/17/us/politics/huawei-ban.html.

11. For example, materials and robotics; B.S. Kademani, Ganesh Surwase, Angil Sagar, K. Bhanumurthy, "Publication trends in materials science: A global perspective," *Scientometrics* (March 2013), https://www.researchgate.net/publication/257663225_Publication_trends_in_materials_science_A_global_perspective; and "Executive Summary World Robotics 2019 Industrial Robots," International Federation of Robotics, 2019, https://ifr.org/downloads/press2018/Executive%20Summary%20WR%202019%20Industrial%20Robots.pdf.

12. Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era" (19th National Congress of the Communist Party of China, Beijing, October 18, 2017).

13. John Lee, "China's Economic Slowdown: Root Causes, Beijing's Response and Strategic Implications for the US and Allies" (Hudson Institute, December 2019), https://s3.amazonaws.com/media.hudson.org/Lee_Chinas_Economic_Slowdown_FINAL_WEB.pdf.

14. James McBride and Andrew Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?," Council on Foreign Relations, May 13, 2019, https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade.

15. Mike Bird, "China Just Overtook the US As The World's Largest Economy," BusinessInsider.com, October 8, 2014, https://www.businessinsider.com/china-overtakes-us-as-worlds-largest-economy-2014-10.

16. OECD.Stat, "Main Science and Technology Indicators (MSTI)," Organisation for Economic Co-Operation and Development, August 2019, http://www.oecd.org/sti/msti.htm.

17. China Power Team, "Is China a Global Leader in Research and Development?"

18. OECD.Stat, "Main Science and Technology Indicators (MSTI)."

19. OECD.Stat, "Main Science and Technology Indicators (MSTI)."

20. China Power Team, "Is China a Global Leader in Research and Development?"

21. Landy Huang and Edward Jiang, "Chinese venture capital and competition with the U.S.," Wharton Public Policy Initiative, May 12, 2019, https://publicpolicy.wharton.upenn.edu/live/news/2965-chinese-venture-capital-and-competition-with-the/for-students/blog/news#_edn7.

22. Huang and Jiang, "Chinese venture capital and competition with the U.S."

23. Jing Yang, "No More Easy Profits as China's Venture-Capital Boom Fizzles," *The Wall Street Journal*, November 14, 2019, https://www.wsj.com/articles/chinas-venture-capital-boom-is-over-leaving-investors-high-and-dry-11573727756.

24. Scott Kennedy, "Made in China 2025," Center for Strategic and International Studies, June 1, 2015, https://www.csis.org/analysis/made-china-2025.

25. Jeremy Bowman, "FANG Stocks: What to Expect in 2019," The Motley Fool, August 1, 2019, https://www.fool.com/investing/fang-stocks-what-to-expect-in-2019.aspx.

26. "Baidu, Alibaba and Tencent: BAT companies dominate Chinese VC," PitchBook Blog on PitchBook.com, April 29, 2019, https://pitchbook.com/blog/baidu-alibaba-and-tencent-bat-companies-dominate-chinese-vc.

27. Lisa Eadicicco, "Huawei, the Chinese tech giant embroiled in controversy, just overtook Apple to become the second-largest smartphone maker," BusinessInsider.com, May 3, 2019, https://www.businessinsider.com/huawei-surpasses-apple-as-second-largest-smartphone-maker-2019-5.

28. ESC Editorial Team, "A deep insight into WeChat Pay's global expansion strategy," EcommerceStrategyChina.com, May 2019, https://www.ecommercestrategychina.com/column/a-deep-insight-into-wechat-pays-global-expansion-strategy; and Preetam Kaushik, "The new frontier: Malaysia is WeChat's stepping stone to Southeast Asian markets," ASEANToday.com, April 6, 2019, https://www.aseantoday.com/2019/04/the-new-frontier-malaysia-is-wechats-stepping-stone-to-southeast-asian-markets/.

29. Jenny Chang, "74 Amazon Statistics You Must Know: 2019 & 2020 Market Share Analysis & Data," FinancesOnline.com, https://financesonline.com/amazon-statistics/.

30. "Statistics: China internet users," ChinaInternetWatch.com, https://www.chinainternetwatch.com/statistics/china-internet-users/.

31. Steven Russolillo, "Not Just the FANGs: China's Tech Rally Has More Bite," *The Wall Street Journal*, June 7, 2017, https://www.wsj.com/articles/not-just-the-fangs-chinas-tech-rally-has-more-bite-1496811330?mod=article_inline&ns=prod/accounts-wsj.

32. Samantha Hoffman, "Engineering global consent: The Chinese Communist Party's data-driven power expansion" (Australian Strategic Policy Institute, October 14, 2019), https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion.

33. Jonathan E. Hillman and Maesea McCalpin, "Watching Huawei's 'Safe Cities'" (Center for Strategic and International Studies, November 4, 2019), https://www.csis.org/analysis/watching-huaweis-safe-cities.

34. Hillman and McCalpin, "Watching Huawei's 'Safe Cities.'"

35. "Rapid Rise of China's STEM Workforce Charted by National Science Board Report," American Institute of Physics, January 31, 2018, https://www.aip.org/fyi/2018/rapid-rise-china%E2%80%99s-stem-workforce-charted-national-science-board-report.

36. "Measuring Human Capital," World Economic Forum, 2016, http://reports.weforum.org/human-capital-report-2016/measuring-human-capital/?doing_wp_cron=1486038808.8636078834533691406250.

37. "The Recruitment Program for Innovative Talents (Long Term)," The Thousand Talents Plan, http://www.1000plan.org.cn/en/.

38. Jane Croft, "China plays catch-up with Europe and US in patents filing race," *Financial Times*, July 8, 2019, https://www.ft.com/content/8ecf7464-8d05-11e9-b8cb-26a9caa9d67b.

39. Qingnan Xie and Richard B. Freeman, "Bigger Than You Thought: China's Contribution to Scientific Publications and Its Impact on the Global Economy," *China & World Economy*, 27 no. 1 (January-February 2019), https://economics.harvard.edu/files/economics/files/bigger_than_you_thought_chinas_contribution_journal_china_and_world_economy_xie-freeman_jan2019.pdf.

40. Dennis Normile, "China cracks down after investigation finds massive peer-reviewed fraud," *Science Magazine* (July 31, 2017), https://www.sciencemag.org/news/2017/07/china-cracks-down-after-investigation-finds-massive-peer-review-fraud.

41. Lulu Yilun Chen, "China Claims More Patents Than Any Country – Most Are Worthless," Bloomberg, September 26, 2018, https://www.bloomberg.com/news/articles/2018-09-26/china-claims-more-patents-than-any-country-most-are-worthless.

42. Marcel Angliviel de la Beaumelle, Benjamin Spevack, and Devin Thorne, "Open Arms: Evaluating Global Exposure to China's Defense-Industrial Base," C4ADS, October 17, 2019, https://www.c4reports.org/open-arms?mod=article_inline.

43. Examples here include Yunzhou Tech, a leader in unmanned surface vessels; Ziyan, a major player in drones and unmanned helicopters; and Kuang-Chi Technologies, which is applying machine learning to its research on military metamaterials. Liu Xuanzun, "China's first unmanned missile boat revealed at Airshow China 2018," *Global Times*, November 7, 2018, http://www.globaltimes.cn/content/1126362.shtml; Melissa K. Chan, "China and the U.S. Are Fighting a Major Battle Over Killer Robots and the Future of AI," *Time* (September 13, 2019), https://time.com/5673240/china-killer-robots-weapons/; and Tang Shihua, "Chinese Future Tech Firm Wins First Military Order to Make Ships Invisible," YicaiGlobal.com, January 14, 2019, https://www.yicaiglobal.com/news/chinese-future-tech-firm-wins-first-military-order-to-make-ships-invisible.

44. Lorand Laskai, "Civil-Military Fusion: The Missing Link Between China's Technological and Military Rise," Net Politics blog on CFR.org, January 29, 2018, https://www.cfr.org/blog/civil-military-fusion-missing-link-between-chinas-technological-and-military-rise; and Alex Joske, "The China Defence Universities Tracker" (Australian Strategic Policy Institute, November 25, 2019), https://www.aspi.org.au/report/china-defence-universities-tracker.

45. Scott Chandler, "Rethinking Defense Acquisition: Zero-Base the Regulations," WarOnTheRocks.com, January 6, 2017, https://warontherocks.com/2017/01/rethinking-defense-acquisition-zero-base-the-regulations/; see Google walking away from Project Maven, Daisuke Wakabayashi and Scott Shane, "Google Will Not Renew Pentagon Contract That Upset Employees," *The New York Times*, June 1, 2018, https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html.

46. OECD.Stat, "Main Science and Technology Indicators (MSTI)."

47. OECD, Gross domestic spending on R&D, OECD Science, Technology, and Innovation Statistics: Main Science and Technology Indicators, https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm.

48. "The Global Human Capital Report 2017: Preparing people for the future of work" (World Economic Forum, 2017), http://www3.weforum.org/docs/WEF_Global_Human_Capital_Report_2017.pdf.

49. Rebecca Fannin, "China Rises To 38% of Global Venture Spending In 2018, Nears US Levels," *Forbes* (January 14, 2019), https://www.forbes.com/sites/rebeccafannin/2019/01/14/china-rises-to-38-of-global-venture-spending-in-2018-nears-us-levels/#431d8e095a5c; Gil Press, "2018 Was A Record-Breaking Year For Israeli Startup Funding. What's Next?," *Forbes* (January 14, 2019), https://www.forbes.com/sites/gilpress/2019/01/14/2018-was-a-record-breaking-year-for-israeli-startup-funding-whats-next/#7966e97f500f; and Paul Sawers, "PitchBook: European VC investment rose 4.2% in 2018, but number of deals dropped 25.9%," VentureBeat.com, January 18, 2019, https://venturebeat.com/2019/01/18/pitchbook-european-vc-investment-rose-4-2-in-2018-but-number-of-deals-dropped-25-9/.

50. "OECD broadband statistics update," OECD, July 9, 2019, https://www.oecd.org/internet/broadband-statistics-update.htm.

51. Michal Kranz, "The director of the FBI says the whole of Chinese society is a threat to the US – and that Americans must step up to defend themselves," BusinessInsider.com, February 13, 2018, https://www.businessinsider.com/china-threat-to-america-fbi-director-warns-2018-2.

52. Ambassador Charlene Barshefsky, Ronald I. Meltzer, Barry J. Hurewitz, David J. Ross, David M. Horn, and Semira Nikou, "The US Tightens Export Controls, Targeting China," WilmerHale, August 2, 2018, https://www.wilmerhale.com/en/insights/client-alerts/20180802-the-us-tightens-export-controls-targeting-china.

53. Edward Taylor, "China's Midea receives U.S. green light for Kuka takeover," Reuters, December 30, 2016, https://www.reuters.com/article/us-kuka-m-a-mideamidea-group-idUSKBN14J0SP.

54. Alex Morales, "U.K. Widens Scope of M&A Probes on National Security Grounds," Bloomberg, July 24, 2018,

https://www.bloomberg.com/news/articles/2018-07-23/u-k-expects-50-fold-rise-in-interventions-on-company-takeovers.

55. Julie Wernau, "Forced Tech Transfers Are on the Rise in China, European Firms Say," *The Wall Street Journal*, May 20, 2019, https://www.wsj.com/articles/forced-tech-transfers-are-on-the-rise-in-china-european-firms-say-11558344240.

56. "China Says Its High-Speed Trains Are More Advanced Than Japan's," Bloomberg News, July 8, 2011, https://www.bloomberg.com/news/articles/2011-07-08/china-says-its-high-speed-trains-are-more-advanced-than-japan-s.

57. Ellen Nakashima and David J. Lynch, "U.S. charges Chinese hackers in alleged theft of vast trove of confidential data in 12 countries," *The Washington Post*, December 21, 2018, https://www.washingtonpost.com/world/national-security/us-and-more-than-a-dozen-allies-to-condemn-china-for-economic-espionage/2018/12/20/cdfd0338-0455-11e9-b5df-5d3874f1ac36_story.html.

58. Alex Joske, "Picking flowers, making honey. The Chinese military's collaboration with foreign universities." (Australian Strategy Policy Institute, October 30, 2018), https://www.aspi.org.au/report/picking-flowers-making-honey.

59. Landau, "Israel Panel to Monitor Chinese Investments Following U.S. Pressure."

60. "Foreign Investment Screening: new European framework to enter into force in April 2019," European Commission, press release, March 5, 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1532.

61. Noah Barkin, "The U.S. Is Losing Europe in Its Battle With China," *The Atlantic* (June 4, 2019), https://www.theatlantic.com/international/archive/2019/06/united-states-needs-europe-against-china/590887/.

62. David E. Sanger, "Trump Wants to Wall Off Huawei, but the Digital World Bridles at Barriers," *The New York Times*, May 27, 2019, https://www.nytimes.com/2019/05/27/us/politics/us-huawei-berlin-wall.html.

63. Tobias Buck, "German regulator says Huawei can stay in 5G race," *Financial Times*, April 14, 2019, https://www.ft.com/content/a7f5eba4-5d02-11e9-9dde-7aedca0a081a.

64. Max Colchester, "U.K. Allows Huawei to Build Parts of 5G Network, Defying Trump," *The Wall Street Journal*, January 29, 2020, https://www.wsj.com/articles/u-k-allows-huawei-to-build-parts-of-5g-network-11580213316.

65. For one such survey, see "Strategic Engagement in Global S&T: Opportunities for Defense Research Consensus Study Report" (National Research Council of the National Academies, 2014), https://www.nap.edu/catalog/18816/strategic-engagement-in-global-st-opportunities-for-defense-research.

66. "About ONR Global," Office of Naval Research (ONR), https://www.onr.navy.mil/Science-Technology/ONR-Global/About-ONR-Global.

67. "Foreign Comparative Testing Program," ONR, https://www.onr.navy.mil/en/Science-Technology/Directorates/Transition/Foreign-Comparative-Testing-FCT.

68. Argie R Sarantinos Perrin, "Blackwell receives OUSD award for Foreign Comparative Testing Program," U.S. Army, May 30, 2019, https://www.army.mil/article/222529/blackwell_receives_ousd_award_for_foreign_comparative_testing_program.

69. Stephen Kuper, "'We make the connections': US FCT opportunities for Aussie businesses," DefenseConnect.com, September 4, 2018, https://www.defenceconnect.com.au/key-enablers/2829-we-make-the-connections-us-foreign-comparative-testing-fct-opportunities-for-aussie-businesses.

70. "Foreign Comparative Testing Program."

71. Jim Bexfield and Ben Taylor, "Organization of Operations Research in the Five Eyes Countries," *Phalanx,* 45 no. 3 (September 2012), 20-22.

72. "The Technical Cooperation Program," Defence Science and Technology Group, https://www.dst.defence.gov.au/partnership/technical-cooperation-program.

73. "The Technical Cooperation Program."

74. Heidi M. Peters, "Defense Primer: The National Technology and Industrial Base" (Congressional Research Service, January 31, 2020), https://fas.org/sgp/crs/natsec/IF11311.pdf.

75. Peters, "Defense Primer: The National Technology and Industrial Base."

76. William Greenwalt, "Leveraging the National Technology Industrial Base to Address Great-Power Competition: The Imperative to Integrate Industrial Capabilities of Close Allies" (Atlantic Council, April 2019), https://www.atlanticcouncil.org/wp-content/uploads/2019/04/Leveraging_the_National_Technology_Industrial_Base_to_Address_Great-Power_Competition.pdf.

77. Daniel Kliman and Brendan Thomas-Noone, "Now is the time to take DIUx global," *Defense News* (May 24, 2018), https://www.defensenews.com/opinion/commentary/2018/05/23/now-is-the-time-to-take-diux-global/; and "Joint Forces Command seeks out innovation in Silicon Valley," Ministry of Defence and Joint Forces Command, April 10, 2018, https://www.gov.uk/government/news/joint-forces-command-seeks-out-innovation-in-silicon-valley.

78. "Department of Defense Launches Allied Prototype Initiative."

79. Jason Sherman, "Pentagon approves initial production for U.S.-Japan SM-3 Block IIA program," InsideDefense.com, October 8, 2019, https://insidedefense.com/daily-news/pentagon-approves-initial-production-us-japan-sm-3-block-iia-program.

80. "Arrow (Israel)," Missile Defense Advocacy Alliance, https://missiledefenseadvocacy.org/defense-systems/arrow-israel/; and "Arrow 3 (Israel)," *Missile Threat*, Center for Strategic and International Studies, August 11, 2016, https://missilethreat.csis.org/defsys/arrow-3/.

81. The S&TF promotes U.S.-Japan interoperability through cooperative technology-related R&D and strengthening the two countries' shared industrial base through lowering procurement barriers. Mutual Defense Assistance Office, *U.S.-J Systems & Technology Forum (S&TF) Briefing*, https://japan2.usembassy.gov/pdfs/wwwf-mdao-stf-brief.pdf; and Jeffrey W. Hornung, "Managing the U.S.-Japan Alliance: An Examination of Structural Linkages in the Security Relationship" (Sasakawa Peace Foundation USA, April 2017), https://spfusa.org/wp-content/uploads/2017/04/Managing-the-U.S.-Japan-Alliance.pdf.

82. For background on CoCom, see Richard F. Grimmett, "Military Techology and Conventional Weapons Export Controls: The Wassenaar Arrangement" (Congressional Research Service, September 29, 2006), https://fas.org/sgp/crs/weapons/RS20517.pdf; Office of Technology Assessment, *Technology and East-West Trade*, November 1979, 153-159, https://www.princeton.edu/~ota/disk3/1979/7918/791810.PDF; and Michael Lipson, "The Reincarnation of CoCom: Explaining Post-Cold War Export Controls," *The Nonproliferation Review*, 6 no. 2 (1999), 33-51, https://www.nonproliferation.org/wp-content/uploads/npr/lipson62.pdf.

83. Bureau of Industry and Security, "Multilateral Export Control Regimes," https://www.bis.doc.gov/index.php/policy-guidance/multilateral-export-control-regimes.

84. Daryl Kimball, "The Wassenaar Arrangement at a Glance," Arms Control Association, December 2017, https://www.armscontrol.org/factsheets/wassenaar; and Wassenaar Arrangement, "About Us," https://www.wassenaar.org/about-us/.

85. James Andrew Lewis, "Emerging Technologies and Managing the Risk of Tech Transfer to China" (Center for Strategic and International Studies, September 2019), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190904_Lewis_ChinaTechTransfer_WEB_v2_1.pdf.

86. Lewis, "Emerging Technologies and Managing the Risk of Tech Transfer to China."

87. Kimball, "The Wassenaar Arrangement at a Glance."

88. Greenwalt, "Leveraging the National Technology Industrial Base to Address Great-Power Competition: The Imperative to Integrate Industrial Capabilities of Close Allies."

89. For an exhaustive and compelling treatment of this, see Greenwalt, "Leveraging the National Technology Industrial Base to Address Great-Power Competition: The Imperative to Integrate Industrial Capabilities of Close Allies."

90. Robert Delaney, "China using 'tentacles' to erode US security, senator warns, urging passage of bill boosting scrutiny of deals," *South China Morning Post*, February 14, 2018, https://www.scmp.com/news/china/policies-politics/article/2133263/china-using-tentacles-erode-us-security-senator-warns.

91. U.S. Department of the Treasury, "Fact Sheet: Proposed CFIUS Regulations to Implement FIRRMA," September 17, 2019, https://home.treasury.gov/system/files/206/Proposed-FIRRMA-Regulations-FACT-SHEET.pdf; and James K. Jackson and Cathleen D. Cimino-Isaacs, "CFIUS Reform Under FIRRMA," IF 10952 (Congressional Research Service, January 14, 2020), https://fas.org/sgp/crs/natsec/IF10952.pdf.

92. These allies include the European Union (European Commission), Canada, the United Kingdom, and Germany; Jackson and Cimino-Isaacs, "CFIUS Reform Under FIRRMA." Japan has also watched FIRRMA implementation closely as it upgrades its investment screening procedures. Interviews in Tokyo, October 2019.

93. This was evident during a CNAS research trip to Israel in December 2019.

94. David R. Hanke, Marwa M. Hassoun, Aman Kakar, "CFIUS 2.0: Treasury Unveils Final Regulations to Govern Expanded Foreign Investment Screening," Arent Fox, January 16, 2020, https://www.arentfox.com/perspectives/alerts/cfius-20-treasury-unveils-final-regulations-govern-expanded-foreign-investment.

95. Arthur Herman, "Closing the Defense Industrial Security Gap with Japan" (Hudson Institute, July 2018), 11, https://s3.amazonaws.com/media.hudson.org/files/publications/HermanJapanFINAL.pdf.

96. See remarks by Assistant Secretary of State Christopher Ashley Ford, "Bureaucracy and Counterstrategy: Meeting the China Challenge" (Conference on Great Power Competition, U.S. Defense Threat Reduction Agency, Ft. Belvoir, VA, September 11, 2019), https://www.state.gov/bureaucracy-and-counterstrategy-meeting-the-china-challenge/.

97. The MAST process is described in Ford, "Bureaucracy and Counterstrategy: Meeting the China Challenge"; Christopher Ashley Ford, "Huawei and its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications" (Multilateral Action on Sensitive Technologies (MAST) Conference, U.S. Department of State, Washington, September 11, 2019), https://www.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/.

98. Ratner, Kliman, Blume, Doshi, Dougherty, Fontaine, Harrell, Rasser, Rosenberg, Sayers, Singh, Scharre, and DeJonge Schulman, "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific," 23.

99. Keith Bradsher, "Amid Tension, China Blocks Vital Exports to Japan," *The New York Times*, September 22, 2010, https://www.nytimes.com/2010/09/23/business/global/23rare.html.

100. Takeshi Iwaya, "Japan's National Defense Strategy" (Center for Strategic and International Studies, Washington, January 16, 2019), https://www.csis.org/analysis/japans-national-defense-strategy.

101. Brown and Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation"; and "Will tighter foreign exchange law make Japan secure?" *The Japan Times*, January 6, 2020, https://www.japantimes.co.jp/news/2020/01/06/business/financial-markets/foreign-exchange-law-japan/#.Xlf0tpJKii4.

102. "Japan passes bill to tighten rules on foreign investments related to national security," *The Japan Times*, November 22, 2019, https://www.japantimes.co.jp/news/2019/11/22/business/financial-markets/japan-passes-bill-tighten-rules-foreign-investment-related-national-security/; and Mariko Kodaki, "Japan tightens entry of foreign investors in 12 strategic sectors," *Nikkei Asian Review* (February 21, 2020), https://asia.nikkei.com/Economy/Japan-tightens-entry-of-foreign-investors-in-12-strategic-sectors.

103. U.S. Department of Commerce Bureau of Industry and Security, *Review of Controls for Certain Emerging Technologies*, 83 FR 58201 (November 19, 2018), 58201-58202 https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies.

104. "International Students in Japan 2017," Japanese Student Services Organization, December 27, 2017, https://www.jasso.go.jp/en/about/statistics/intl_student/__icsFiles/afieldfile/2017/12/25/data17_brief_e.pdf.

105. Hiroyuki Akiyama, "Japan borrows US playbook to prevent student espionage," *Nikkei Asian Review* (December 17, 2019), https://asia.nikkei.com/Politics/Japan-borrows-US-playbook-to-prevent-student-espionage.

106. Sherman, "Pentagon approves initial production for U.S.-Japan SM-3 Block IIA program."

107. Jon Grevatt, "Lockheed Martin to develop F-35 maintenance facility in Japan," Jane's, August 28, 2019, https://www.janes.com/article/90716/lockheed-martin-to-develop-f-35-maintenance-facility-in-japan.

108. We are indebted to James Schoff for making this point during his review.

109. "How much does your country invest in R&D?," UNESCO Institute for Statistics, http://uis.unesco.org/apps/visualisations/research-and-development-spending/.

110. Alina Ragge, "Japan: plans for electronic-warfare and hypersonic capabilities," Military Balance blog on iiss.org, December 3, 2018, https://www.iiss.org/blogs/military-balance/2018/12/japan-plans-hypersonic-capabilities; and Yoichiro Hiroi, "Japan's Rakuten and NEC to build own 5G network," *Nikkei Asian Review* (June 5, 2019), https://asia.nikkei.com/Spotlight/5G-networks/Japan-s-Rakuten-and-NEC-to-build-own-5G-network.

111. Riki Ellison and Ian Williams, "Japan: Priorities for Missile Defense Development and U.S. Partnership," Missile Defense Advocacy Alliance, April 2015, https://missiledefenseadvocacy.org/wp-content/uploads/2015/04/Japan-BMD-Report.pdf; "Japan – SM-2 Block IIIB Standard Missiles," Defense Security Cooperation Agency, press release, July 19, 2016, https://www.dsca.mil/major-arms-sales/japan-sm-2-block-iiib-standard-missiles-0; and "Standard Missile-3: Beating Ballistic Missiles on Land and at Sea," Raytheon, https://www.raytheon.com/capabilities/products/sm-3.

112. Australian Department of Defence, *2016 Defence White Paper* (2016), https://www.defence.gov.au/Whitepaper/AtAGlance/Strategic-Outlook.asp; and Australian Government, *2017 Foreign Policy White Paper*, https://www.fpwhitepaper.gov.au/foreign-policy-white-paper/chapter-two-contested-world/power-shifts-indo-pacific.

113. "Gladys Liu: The row over a trailblazing Chinese-Australian MP," BBC, September 16, 2019, https://www.bbc.com/news/world-australia-49712187; "Australia investigates alleged Chinese plot to install spy MP," BBC, November 25, 2019, https://www.bbc.com/news/world-australia-50541082; and Sarah Martin, "'I will not repent': Andrew Hastie refuses to back down on China," *The Guardian*, November 16, 2019, https://www.theguardian.com/world/2019/nov/17/china-calls-on-liberal-mps-to-repent-after-beijing-study-tour-ban.

114. David Irvine, "Address to the Australia-China Business Council" (Australia-China Business Council, Sydney, August 19, 2019), https://firb.gov.au/about-firb/news/address-mr-david-irvine-ao-firb-chair-australia-china-business-council.

115. Angus Grigg, "No such thing as a private company in China: FIRB," *Financial Review*, January 16, 2019, https://www.afr.com/policy/foreign-affairs/no-such-thing-as-a-private-company-in-china-firb-20190116-h1a4ut.

116. "Sensitive sectors" include "media, telecommunications, and defence-related industries." John Kehoe, "Foreign Investment Review Board flags more China takeover crackdowns," *Financial Review*, February 19, 2019, https://www.afr.com/policy/foreign-affairs/foreign-investment-review-board-flags-more-china-takeover-crackdowns-20190219-h1bfzr.

117. "The Defence and Strategic Goods List," Australian Department of Defence, https://www.defence.gov.au/ExportControls/DSGL.asp.

118. Naaman Zhou, "Calls for regulation of universities partnering with military-linked foreign companies," *The Guardian,* December 15, 2017, https://www.theguardian.com/australia-news/2017/dec/16/calls-for-regulation-of-universities-partnering-with-military-linked-foreign-companies.

119. Vivienne Thom, "Independent Review of the Defence Trade Controls Act 2012," October 19, 2018, https://www.defence.gov.au/publications/reviews/tradecontrols/Docs/DTC_Act_Review_Final_Report.pdf.

120. This point was made in an email exchange with a leading Australian defense expert on February 18, 2020.

121. Joske, "The China Defence Universities Tracker."

122. Joske, "The China Defence Universities Tracker."

123. Joske, "Picking flowers, making honey. The Chinese military's collaboration with foreign universities."

124. "Guidelines to Counter Foreign Interference in the Australian University Sector," University Foreign Interference Taskforce, November 2019, https://docs.education.gov.au/system/files/doc/other/ed19-0222_-_int_-_ufit_guidelines_acc.pdf.

125. Australian Department of Defence, *2016 Defence White Paper,* 108-110.

126. Business.gov.au, "Research Opportunities and Priorities," https://www.business.gov.au/CDIC/Innovate-in-defence/Research-opportunities-and-priorities; and Business.gov.au, "Innovation Opportunities and Priorities," https://www.business.gov.au/CDIC/Innovate-in-defence/Innovation-opportunities-and-priorities.

127. Defence Science and Technology, "Partner With Us: International Government Agencies," https://www.dst.defence.gov.au/partner-with-us/international-government-agencies.

128. "Talisman Sabre 2019, Largest Ever Bilateral Defense Exercise in Australia Opens," U.S. Indo-Pacific Command, July 9, 2019, https://www.pacom.mil/Media/News/News-Article-View/Article/1899433/talisman-sabre-2019-largest-ever-bilateral-defense-exercise-in-australia-opens/.

129. "U.S., Australia work side-by-side on Triton UAS development," AerotechNews.com, August 26, 2019, https://www.aerotechnews.com/blog/2019/08/26/u-s-australia-work-side-by-side-on-triton-uas-development/.

130. "Companies to exhibit space capabilities at SpaceFest in Australia," Air Force Technology, March 20, 2019, https://www.airforce-technology.com/news/space-capabilities-spacefest-australia/; "CEA Technologies secures loan from Australia to boost exports," Army Technology, August 13, 2019, https://www.army-technology.com/news/cea-technologies-loan-australia-exports/; Josh Taylor, "Quantum leap from Australian research promises super-fast computing power," *The Guardian*, July 18, 2019, https://www.theguardian.com/technology/2019/jul/19/quantum-leap-australian-researchers-could-lead-to-much-greater-computing-power; "About the Woomera Prohibited Area," Australian Department of Defence, https://www.defence.gov.au/woomera/about.htm; and Frank Holmes, "Australia May Be The Saving Grace For The Rare Earth Metals Market," *Forbes* (November 6, 2019), https://www.forbes.com/sites/greatspeculations/2019/11/06/australia-may-be-the-saving-grace-for-the-rare-earth-metals-market/#1b74e0b041cd?.

131. Kate Louis, "Exports critical for Australia's defence industry," Australian Strategic Policy Institute, October 19, 2018, https://www.aspistrategist.org.au/exports-critical-for-australias-defence-industry/; and Australian Department of Defence, *Defence Export Strategy – Fact Sheet*, https://www.defence.gov.au/Export/Strategy/documents/DefenceExportStrategy-FactSheet.pdf.

132. "CFIUS Excepted Foreign States," U.S. Department of the Treasury, February 13, 2020, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-excepted-foreign-states.

133. Pew Research Center bears no responsibility for the analyses or interpretations of the data presented here. The opinions expressed herein, including any implications for policy, are those of the author and not of Pew Research Center. "People around the globe are divided in their opinions of China," Pew Research Center, December 5, 2019, https://www.pewresearch.org/fact-tank/2019/12/05/people-around-the-globe-are-divided-in-their-opinions-of-china/, "Topline questionnaire," Pew Research Center, February 7, 2020, https://www.pewresearch.org/wp-content/uploads/2020/02/Views-of-Russia-Topline-for-Release_UPDATED.pdf, and "Iran's Global Image Mostly Negative: Israel, Arab States Share Unfavorable View of Middle East Neighbor," Pew Research Center, June 18, 2015, https://www.pewresearch.org/global/wp-content/uploads/sites/2/2015/06/Pew-Research-Center-Iran-Report-June-18-2015-FINAL.pdf.

134. Mordechai Chaziza, "Israel Agrees to Monitor Foreign Investment," BESA Center Perspectives Paper No. 1,340 (The Begin-Sadat Center for Strategic Studies, November 11, 2019), https://besacenter.org/perspectives-papers/israel-monitor-foreign-investment/.

135. Doron Ella, "A Regulatory Mechanism to Oversee Foreign Investment in Israel: Security Ramifications," The Institute for National Security Studies, November 19, 2019, https://www.inss.org.il/publication/a-regulatory-mechanism-to-oversee-foreign-investment-in-israel-security-ramifications/.

136. "Pentagon says Israel improves arms-export controls," YnetNews.com, June 6, 2007, https://www.ynetnews.com/articles/0,7340,L-3446607,00.html.

137. "Academic Programs of Study," Guangdong Technion Israel Institute of Technology, https://www.gtiit.edu.cn/en/programs-of-study.aspx.

138. Sarah Levi, "Chinese enrollment at Israeli universities skyrockets," *The Jerusalem Post*, August 14, 2017, https://www.jpost.com/Israel-News/Chinese-enrollment-at-Israeli-universities-skyrockets-502404.

139. Dan Senor and Saul Singer, *Start-Up Nation: The Story of Israel's Economic Miracle* (New York: Twelve Books, 2011).

140. "The place of the oceans in Norway's foreign and development policy" (Norwegian Ministry of Foreign Affairs, 2016-2017), 36-37, https://www.regjeringen.no/contentassets/1b21c0734b5042e489c24234e9927b73/en-gb/pdfs/stm201620170022000engpdfs.pdf; and Bård Glad Pedersen, "Security in the Arctic – a Norwegian perspective" (Arctic Circle Conference, Reykjavik, November 2, 2014), https://www.regjeringen.no/en/aktuelt/security-in-the-arctic--a-norwegian-perspective/id2351274/.

141. Echo Huang and Isabella Steger, "Norway wants China to forget about the human rights thing and eat salmon instead," Quartz, June 14, 2017, https://qz.com/1000541/norway-wants-china-to-forget-about-the-human-rights-thing-and-eat-salmon-instead/.

142. Huang and Steger, "Norway wants China to forget about the human rights thing and eat salmon instead."

143. Simen Klevstrand and Marianne Henne Møller, "Norway's new investment screening regime enters into force," Haavind, January 2, 2019, https://haavind.no/en/news/investment-screening-regime/.

144 Ministry of Foreign Affairs, *Regulations relating to the export of defence-related products, dual-use items, technology and services* (June 19, 2013), https://www.regjeringen.no/contentassets/e19e0d2f0fe74437897036c1ddaf45f6/the-export-control-regulations.pdf.

145. "Norwegian Police Investigating Academics for Exposing Technology to Iranian Visitors," Radio Farda, January 22, 2020, https://en.radiofarda.com/a/norwegian-police-investigating-academics-for-exposing-technology-to-iranian-visitors/30391282.html.

146. Sam Brannen, "The Gap Between Supply and Demand for Spy Planes Just Got Bigger," DefenseOne.com, May 29, 2014, https://www.defenseone.com/threats/2014/05/gap-between-supply-and-demand-spy-planes-just-got-bigger/85453/.

147. Zachery Tyson Brown, "The US Intelligence Community Is Caught in a Collector's Trap," DefenseOne.com, February 25, 2020, https://www.defenseone.com/ideas/2020/02/us-intelligence-community-caught-collectors-trap/163304/.

148. Elsa B. Kania and Lindsey R. Sheppard, "Why Huawei Isn't So Scary," *Foreign Policy* (October 12, 2019), https://foreignpolicy.com/2019/10/12/huawei-china-5g-race-technology/.

149. Elsa B. Kania, "Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy" (Center for a New American Security, November 2019), https://s3.amazonaws.com/files.cnas.org/documents/Kania-Securing-Our-5G-Future-2.pdf?mtime=20191029084132. One potential solution to expand 5G options is through network virtualization. For more on this, see Ratner, Kliman, Blume, Doshi, Dougherty, Fontaine, Harrell, Rasser, Rosenberg, Sayers, Singh, Scharre, and DeJonge Schulman, "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific."

150. Peter Harrell, Elizabeth Rosenberg, and Edoardo Saravalle, "China's Use of Coercive Economic Measures" (Center for a New American Security, June 2018), https://s3.amazonaws.com/files.cnas.org/documents/China_Use_FINAL-1.pdf?mtime=20180604161240; Eric Ng, "China's rare earth producers say they are ready to weaponise their supply stranglehold, pass any tariff as cost to US customers," *South China Morning Post*, August 8, 2019, https://www.scmp.com/business/commodities/article/3021947/chinas-rare-earth-producers-say-they-are-ready-weaponise-their; Peter Harrell, Elizabeth Rosenberger, and Edoardo Saravelle, "China's Use of Coercive Economic Measures," June 2018, https://s3.amazonaws.com/files.cnas.org/documents/China_Use_FINAL-1.pdf?mtime=20180604161240.

151. Steve Banker, "Global High-tech Supply Chains Disrupted By The Coronavirus," *Forbes* (February 10, 2020), https://www.forbes.com/sites/stevebanker/2020/02/10/global-high-tech-supply-chains-disrupted-by-the-coronavirus/#78cb31153eae.

152. Department of Defense, *Trusted Foundry Program Accredited Suppliers*, February 6, 2020, https://www.dmea.osd.mil/otherdocs/AccreditedSuppliers.pdf; and Ratner, Kliman, Blume, Doshi, Dougherty, Fontaine, Harrell, Rasser, Rosenberg, Sayers, Singh, Scharre, and DeJonge Schulman, "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific."

153. Giorgio Patrini, "Mapping the Deepfake Landscape," Deeptrace, July 10, 2019, https://deeptracelabs.com/mapping-the-deepfake-landscape/.

154. Joshua A. Tucker, Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan, "Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature" (Hewlett Foundation, March 2018), https://hewlett.org/wp-content/uploads/2018/03/Social-Media-Political-Polarization-and-Political-Disinformation-Literature-Review.pdf.

155. Robert O. Work and Greg Grant, "Beating the Americans at their Own Game: An Offset Strategy with Chinese Characteristics" (Center for a New American Security, June 2019), https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-Work-Offset-final-B.pdf?mtime=20190531090041; and Christopher M. Dougherty, "Why America Needs a New Way of War" (Center for a New American Security, June 2019), https://s3.amazonaws.com/files.cnas.org/CNAS+Report+-+ANAWOW+-+FINAL2.pdf.

156. For more on this, see Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order* (Boston: Houghton Mifflin Harcourt, 2018).

157. "Who We Are/Our Mission," Defense Innovation Unit (DIU), https://www.diu.mil/about; and "About Air Force Small Business," Air Force Small Business, https://www.airforcesmallbiz.af.mil/About-Us/.

158. "Air Force Space Pitch Day welcomes small businesses to pitch their 'BIG' ideas," Los Angeles Air Force Base, press release, November 5, 2019, http://spaceref.com/news/viewpr.html?pid=54893.

159. "Techstars Allied Space Accelerator," Techstars, https://www.techstars.com/programs/allied-space-program/.

160. Kliman and Thomas-Noone, "Now is the time to take DIUx global."

161. C. Todd Lopez, "Task Force Curbs Technology Theft to Keep Joint. Force Strong," Department of Defense News, November 26, 2019, https://www.defense.gov/Explore/News/Article/Article/2027555/task-force-curbs-technology-theft-to-keep-joint-force-strong/; and C. Todd Lopez, "Losing Technology to Competitors Threatens Force Lethality," Department of Defense News, October 31, 2019, https://www.defense.gov/Explore/News/Article/Article/2004140/losing-technology-to-competitors-threatens-force-lethality/.

162. The model here is the DIUx report on China's Technology Transfer, which served as a wake-up call for Silicon Valley and the U.S. technology industry as a whole. Brown and Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation."

163. This has been the subject of work by the Center for Security and Emerging Technologies at Georgetown University. The few open source studies conducted by nongovernmental research institutions have created an outsized impact. See Joske, "Picking flowers, making honey. The Chinese military's collaboration with foreign universities."

164. Christopher Wray, "Opening Remarks: China Initiative Conference" (Center for Strategic and International Studies, Washington, February 6, 2020), https://www.csis.org/analysis/fbi-director-christopher-wrays-opening-remarks-china-initiative-conference.

165. One model for government-supported incubators is from Israel. "Incubators Incentive Program," Israel Innovation Authority, https://innovationisrael.org.il/en/program/incubators-incentive-program.

166. "Woomera Range Complex," Royal Australian Air Force, https://www.airforce.gov.au/about-us/bases/sa/woomera; "Woomera Range Complex," South Australia The Defence State, https://www.defencesa.com/precincts/test-and-training-areas/woomera-range-complex; and "Woomera Upgrade," Raytheon, https://www.raytheon.com/sites/default/files/au/rtnwcm/groups/public/documents/document/rau_pac13_cap_mobilerange_pdf.pdf.

167. "About ATC," Andøya Test Center, https://www.testcenter.no/about-atc/; "Andøya Test Center," Andøya Space Center, https://www.andoyaspace.no/test-range/; and Eivind V. Thrane, "The history of Andøya Rocket Range," History of Geo- and Space Sciences, December 7, 2018, https://www.hist-geo-space-sci.net/9/141/2018/hgss-9-141-2018.pdf.

168. Kliman and Thomas-Noone, "How the Five Eyes Can Harness Commercial Innovation"; Ratner, Kliman, Blume, Doshi, Dougherty, Fontaine, Harrell, Rasser, Rosenberg, Sayers, Singh, Scharre, and DeJonge Schulman, "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific," 36; and Arthur Herman, "Israel and Japan Are Finally Becoming Friends. Why?" Hudson Institute, August 6, 2015, https://www.hudson.org/research/11519-israel-and-japan-are-finally-becoming-friends-why.

169. David Gallacher, "'Buy American' (Again): New Executive Order Requires Changes (By 2020)" Government Contracts & Investigations Blog, July 31, 2019, https://www.governmentcontractslawblog.com/2019/07/articles/baa-and-taa/baa-buy-american-again/.

170. Taketsugu Sato, "U.S. diplomat confident that U.S., Japan will contribute more to alliance," *The Asahi Shimbun*, January 31, 2020, http://www.asahi.com/ajw/articles/13083259.

171. The missile interceptor is now in production. Paul McLeary, "New US/Japanese Missile Readying for New Generation of Threats," BreakingDefense.com, August 1, 2019, https://breakingdefense.com/2019/08/new-missile-interceptor-striking-as-threats-grow/.

172. Edward White, "China's ability to make computer chips still 'years behind' industry leaders," *Financial Times*, January 21, 2019, https://www.ft.com/content/a002a9e4-1a42-11e9-b93e-f4351a53f1c3.

173. This recommendation was initially advanced in Ratner, Kliman, Blume, Doshi, Dougherty, Fontaine, Harrell, Rasser, Rosenberg, Sayers, Singh, Scharre, and DeJonge Schulman, "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific," 23.

174. For more on this networked architecture, see Richard Fontaine, Patrick M. Cronin, Mira Rapp-Hooper, and Harry Krejsa, "Networking Asian Security: An Integrated Approach to Order in the Pacific" (Center for a New American Security, June 19, 2017), https://www.cnas.org/publications/reports/networking-asian-security.

175. Martijn Rasser, Elizabeth Rosenberg, and Paul Scharre, "The China Challenge: Strategies for Recalibrating the U.S.-China Tech Relationship," Center for a New American Security, December 12, 2019, https://s3.amazonaws.com/files.cnas.org/documents/CNAS-US-China-Tech-Competition-formatted-for-pdf-download.pdf?mtime=20191217130551.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy.

CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

1152 15th Street, NW Suite 950 Washington, DC 20005
t. 202.457.9400 | f. 202.457.9401 | info@cnas.org | cnas.org


Center for a
New American
Security