Countering Chinese Engagement with Israel: *A Comprehensive and Cooperative U.S.-Israeli Strategy*

JINSA's Gemunder Center Israel-China Policy Project - *February 2021*

Co-Chairs: ADM Jonathan W. Greenert, USN (ret.) and VADM John M. Bird, USN (ret.)

JINSA
The Jewish Institute for National Security of America

DISCLAIMER

The findings and recommendations contained in this publication are solely those of the authors.
Cover image credit: JINSA

Policy Project Staff and Contributors

Co-Chairs

Admiral Jonathan W. Greenert, USN (ret.)
Co-Chair, JINSA Israel-China Policy Project; Former Chief, Naval Operations (CNO, 2011-2015)

Vice Admiral John M. Bird, USN (ret.)
Co-Chair, JINSA Israel-China Policy Project; Former Commander, U.S. Seventh Fleet

JINSA Staff & Contributors

Michael Makovsky, PhD
President & CEO

IDF MG (ret.) Yaacov Ayish
Senior Vice President for Israeli Affairs, Former Israeli Defense Attaché to the United States and Canada, and former Head of the IDF General Staff Operations Branch

Blaise Misztal
Vice President for Policy

Charles B. Perkins
Director for U.S.-Israel Security Policy

Jonathan Ruhe
Director of Foreign Policy

Ari Cicurel
Senior Policy Analyst

Erielle Davidson
Senior Policy Analyst

Shiri Moshe
Senior Policy Analyst

Table of Contents

I. Executive Summary

China seeks to expand its influence around the globe while weakening the U.S.-led, rules-based international order that aims at the freedom, security, and prosperity of all. In pursuit of this objective, Beijing has launched a sophisticated, disciplined, and calculated whole-of-government effort that combines economic, psychological, informational, and legal warfare. Ostensibly benign trade and investment, undertaken in the guise of the Belt and Road Initiative (BRI), are key tools in this Chinese strategy, allowing Beijing to gain access to vital infrastructure, dual-use technology, and intellectual property (IP) with which to grow its own geopolitical power and military capabilities while simultaneously undermining its competitors' economic vitality.

Perhaps belatedly, the United States has realized that protecting its national security against Chinese threats also requires protecting its economic vitality, particularly in the form of its IP. Thus, U.S. policymakers have begun to scrutinize or even, in some instances, block Chinese investments in strategically important U.S. infrastructure projects and sensitive technologies. Meanwhile, business leaders have called on Washington to do more "to renew American competitiveness and sustain critical U.S. technological advantages" in order to "out-compete China."[1] With broad and bipartisan recognition of the challenge that China poses to the rules-based international order, this task of managing China's presence in U.S. markets and industries will remain central to the emerging 21st century U.S. national security and economic strategy. But, to protect itself, it is not enough for the United States to undertake this task alone. Washington must also work closely with and assist its allies to adjust their economic—especially investment and trade—policies to address China's expansionist ambitions.

As a close U.S. partner, on which Washington increasingly leans to protect its interests in the Middle East, a "start-up nation" on the frontlines of technological breakthroughs, and a target of Chinese economic exploitation, Israel can and should more fully join U.S. efforts to protect against Chinese penetration. That means creating a comprehensive whole-of-government strategy for assessing and responding to Chinese activities in and around Israel. In particular, in the economic sphere, this will require regular and systematic interagency processes to review foreign infrastructure investments and exports of dual-use technologies, as well as joining relevant multilateral export control regimes. The United States, meanwhile, should not merely demand and expect cooperation, but recognize the economic pain that excluding China from the Israeli economy might entail and offer assistance in making the transition, including by promoting greater investment in, and commerce with, Israel and by elevating its security and intelligence relationship with Israel.

By working together, the United States and Israel can protect themselves from Chinese economic exploitation, build deeper strategic and economic ties, and, perhaps most importantly, develop a model of democratic economic governance that can serve as the foundation for a new, broader international coalition against authoritarian great powers.

A. China's Strategy

China's geo-economic strategy involves acquiring and controlling the key drivers of the global economy: the infrastructure that enables international commerce and the technological

breakthroughs, most developed by the United States and its allies, that will fuel future growth. Beijing's strategy seeks to turn economic power into geopolitical dominance and civilian technology into a military advantage.

Part of this strategy is pursued through illegal and covert gray zone operations short of warfare, often involving hacking and espionage. An interconnected combination of lawfare, cyber operations, and coercive Chinese market influence seeks not only to benefit China economically but also to intimidate the United States and its partners so that they fear taking action against Beijing.[2] Just as damaging, however, are overt Chinese actions that are, on the surface, legal, yet are designed to subvert and undermine the open global economic order that they exploit. In particular, three Chinese activities should be understood as part of its comprehensive and global geo-economics strategy of civil-military fusion: (1) provision of critical civilian infrastructure services; (2) investment in and purchase of commercial dual-use technology; and (3) participation in research and development (R&D). These activities not only allow China to gain controlling interest in key infrastructure assets or access to intellectual property but also enable further illegal activities that have become part of China's global BRI strategy, from Islamabad to Athens.

B. U.S. Response

The United States has slowly woken to the threat of Chinese economic exploitation but only after it already suffered significant military and economic damage. "Every year," according to the 2017 *National Security Strategy*, "competitors such as China steal U.S. intellectual property valued at hundreds of billions of dollars. …In addition to these illegal means, some actors use largely legitimate, legal transfers and relationships to gain access to fields, experts, and trusted foundries that fill their capability gaps and erode America's long-term competitive advantages."[3] In February 2018, the White House approved a strategy for competing with China in the Indo-Pacific that elevates blocking China's acquisition of innovative and dual-use technologies and unfair trading practices to a major U.S. objective.[4] This objective, however, applies not only to the United States but also to its regional partners, not just in Asia but in the Middle East as well.

Indeed, a strong bipartisan consensus has emerged in Washington on the need to reexamine U.S. economic relations with China. This consensus has only been reinforced by the novel coronavirus pandemic, which has exposed both how critical supply chains, such as pharmaceuticals, are dependent on China as well as how Beijing has aggressively moved to exploit a global crisis to expand its power and influence. As a result, the United States has begun the complicated process of protecting itself from China's concerted, comprehensive, and systematic geo-economic strategy through a similarly formal, comprehensive, and systematic response.

The cornerstone of these new U.S. efforts has been the effort to prevent China from exploiting overt, commercial economic activities through two mutually reinforcing legal tools: review of foreign investments into critical areas of the U.S. economy, including infrastructure and emerging technologies; and control of exports of U.S. commercial technology that could be used for military or other means—so-called "dual-use" technologies. Existing U.S. measures in both these areas are being updated and strengthened; however, more remains to be done.

C. The Threat to Israel

Even as the United States seeks to better protect itself, however, China pursues the same strategy globally, threatening the prosperity and vitality of many U.S. allies and partners. Chinese outbound investment has grown over fifty times in the last two decades. Under the auspices of the BRI, China now explicitly seeks to build and develop infrastructure to link Western and emerging markets firmly to the Chinese economy. This Chinese use of legally permissible entry points into the economies of the United States, its allies, and its partners has led to significant access to cutting-edge Western technologies and global infrastructure.

A particularly important target of China's geo-economic exploitation is Israel, a high-technology powerhouse. It has the highest per-capita production of IP in the world. Israeli civil IP falls into critical dual-use areas: artificial intelligence algorithms; cyber-offense and -defense; quantum encryption; electromagnetic spectrum exploitation; nanotechnology; and autonomy. China is a significant participant in these Israeli sectors. Besides, Israel has pivotal geography: China has offered, as part of BRI, to modernize part of Haifa port, a harbor frequented by the U.S. Navy.

With the United States lessening its footprint in the Middle East, Washington will be increasingly looking to Israel to help secure its regional interests, rendering this already significant partnership even more strategically crucial. Simultaneously, however, China seeks to exploit the region for its own economic gains—from securing cheap Iranian oil to gaining access to Israeli infrastructure and technology. Going forward, Washington will be seeking Israeli assistance in thwarting China's Middle Eastern ambitions. Israel's ability to play that role, however, will be determined by the extent of its economic connections with China.

Given Israel's valuable civil IP and transportation facilities, it is a tempting target for Chinese economic penetration and one target that Beijing is already seeking to exploit. These pernicious Chinese activities, however, threaten to undermine both Israel's economic dynamism and its strategic partnership with the United States. Israeli technology stolen or acquired by China today could be sold for pennies tomorrow, depriving Israeli companies of profits. Or it could be used in weapons sold to Israeli adversaries, such as Iran, with which China reportedly has pursued a $400 billion deal that would include cooperation between the country's militaries through joint training, intelligence-sharing, and R&D.[5] As China's investments in Israel grow, so, too will the influence it can exert, allowing it to potentially demand difficult political and economic concessions. Meanwhile, with attitudes towards Beijing dimming in democratic nations around the world and a growing number of voices in Washington calling for an anti-China coalition, its continued economic relations with China could begin adversely affecting Israeli ties with partners.[6]

That is why the executive and legislative branches of the U.S. government have made it a priority to convince Israel to be among the first major U.S. partners to cut problematic economic ties with China. The Department of Defense has made the Haifa port issue a priority, stressing that U.S. naval vessels will not be able to dock at a harbor with nearby Chinese involvement. Last year, the Secretary of State made his first trip abroad since the outbreak of COVID-19, and the Sino-Israel challenge was among the three issues in his brief.[7]

Israel has taken these U.S. concerns seriously, taking some steps to address them. Yet, the extent of the threat, and of what the United States is asking for, exceeds the handful of

prominent and particularly troubling Chinese investments in Israel, like the Haifa port, that U.S. policymakers have tended to focus on, and that Israel has acknowledged. China's penetration of Israel's economy is systematic and far-reaching. Israel cannot simply count on the United States raising the occasional red flag.

D. Toward a Common Defense

To respond to China's growing presence in Israel and in the Middle East and the challenges this presence creates, Jerusalem needs a comprehensive, whole-of-government strategy. A major part of this strategy should be focused on protecting its economy. To do so, Israel requires a comprehensive and systematic legal framework to screen inbound investment and outbound exports.

Israel is not alone in confronting the daunting task of protecting its economy from Chinese penetration. Although some U.S. allies, such as Germany and Australia, have full-fledged foreign investment review processes, the United States is having immense difficulty getting key allies in Europe, the Middle East, and Asia to undertake similar measures. China has developed a competitive strategy that not only brings its economic gains, but also breeds dependency and foments dissension between the United States and its allies. Countries are loath to lose the Chinese capital flows that have enriched them in recent years without certainty that there are available substitutes for Chinese investment and commerce. An even greater worry might be that, even if they limit their exposure to China, their neighbors will not or the United States will change course, growing richer, at least in the near term, by remaining beholden to Beijing's investments.

This "substitute" dilemma is one that the United States is uniquely positioned to solve as the world's leading economy and most powerful nation. It already has been trying to address the issue domestically, with programs designed to supplant Chinese capital by spurring government funding and catalyzing vetted private sector investments in critical technologies and industries. If it embraces its role as the first mover, signaling its resolve to continue these policies and expand such programs internationally, the United States can reassure its partners that they too will have access to more alternative investments if they act to make their own economies safe.

The time has come for Israel to understand the permanence and extent of the U.S. shift, which is being accelerated by COVID-19. Indeed, like other key U.S. partners, Israel may find itself increasingly in the middle of growing, contentious geopolitical and economic tensions between the United States and China. Israel must act to protect its vibrant innovation-driven technology and avoid allowing China to drive a wedge between the United States and Israel. To be sure, with repeated U.S. urging, the Israeli cabinet passed a law to review foreign investment in Israel. It also already has legal standards for controlling dual-use exports. Whether this new law has been effectively translated into an operating regulatory regime is unknown, but it is already clear that it has exceptions, such as high-technology ventures. These efforts, in short, remain insufficient.

By taking decisive action to remove pernicious Chinese investment from its economy, Israel can cement its standing as one of the United States' most capable, dependable, and forward-leaning partner, and establish a model for international economic governance for other

democratic states to emulate. It is imperative, therefore, that Jerusalem and Washington act individually and together on two fronts: to bolster legal defenses against Chinese economic penetration and to create vetted market-driven alternatives to hazardous Chinese investment.

Neither the United States nor Israel have a well-developed plan on how Israel can reorient its economy or how it can build, nearly from scratch, a U.S.-type investment and export control regimes. This report is unique in that it engages in an extensive examination and comparison of approaches to inbound investment and outbound commerce review, both in the United States and Israel, offering insight as well from the European Union and Australia. It uses this analysis to make concrete institutional and legal recommendations for how Israel can strengthen its fractured investment review system and disparate export controls regime, neither of which is well-understood outside of Israel. This report also considers how the United States can assist Israel to strengthen its legal regime and make necessary but economically difficult changes, including through increased trade and investment as well as redoubling their bilateral security cooperation. If Washington and Jerusalem are able to protect their economies from China, the U.S.-Israel relationship can become the preeminent model when constructing a new democratic alliance for the 21st century.

Specifically, we recommend:

A. Israel adopt a thorough and coordinated whole-of government strategy for assessing and responding to the threat posed by China, elements of which include:

   i. Reviewing foreign misappropriation of Israeli technology;
   ii. Focusing counterintelligence resources on curbing Chinese infiltration of Israeli academia;
   iii. Systematizing protocol for screening inbound investment;
   iv. Strengthening Israeli unilateral export controls;
   v. Joining relevant multilateral export control agreements.

B. The United States assist and encourage Israel in protecting its economy from Chinese exploitation by:

   i. Tailoring relevant Israeli-US intelligence sharing to raise appropriate topics to the “Five Eyes” level;
   ii. Providing information on best practices and making available U.S. government experts to advise and consult with Israeli counterparts;
   iii. Acknowledging the benefits of and Israel’s need for foreign investment;
   iv. Expanding U.S. and international financing available for infrastructure projects in Israel;
   v. Enabling U.S. government investment in Israel’s technology sector;
   vi. Providing clear requirements for and assurance of granting Israel Strategic Trade Authorization;
   vii. Frontloading funds from the Memorandum of Understanding on U.S. defense to Israel.

C. The United States and Israel work together to create investment and export opportunities that are safe for democracy, establishing an economic coalition that other partners can join as well by:

i. Negotiating and signing a robust Bilateral Investment Treaty;
ii. Updating the current U.S.-Israeli Free Trade Agreement;
iii. Creating a Select Committee on Technology Control;
iv. Exploring a multinational Trusted Capital Program;
v. Investing in joint scientific training and research & development;
vi. Deepening strategic competition.

U.S. policies with respect to China are undergoing their largest change since Nixon went to Beijing. Grasping that shift in a full, clear-eyed manner and joining it is vital for Israeli security and prosperity, as well as the continued strength of the U.S.-Israel partnership.

II. Introduction

Since 2017, there has been substantial, bipartisan consensus in Washington on the urgent need to confront Chinese attempts to subvert the U.S.-led international order not just militarily but also economically. This has translated into U.S. efforts to curtail not only the import of Chinese products, but also Chinese investments and involvement with U.S. infrastructure and dual-use technologies.

According to a recently declassified *U.S. Strategic Framework for the Indo-Pacific*, "China seeks to dominate cutting-edge technologies, including artificial intelligence and bio-genetics, and harness them in the service of authoritarianism." The Framework calls for the United States to "prevent China's industrial policies and unfair trading practices from distorting global markets" and for U.S. allies to adopt a similar approach[8] in order to become "resistant to Chinese activities aimed at undermining their sovereignty, including through covert or coercive influence."[9] The United States continues to pressure European countries regarding 5G choices and Chinese investment in dual-use technologies; it is vital, however, that such pressure be accompanied by mutually beneficial cooperation. Unable to match China's economic output or deter security competition alone, Washington seeks to leverage its global partnerships. The U.S. approach to Israel is no different and just as urgent.

Beijing's economic engagement in Israel has skyrocketed since China and Israel formalized relations in 1992. By 2018, Israel's exports to China had grown by two orders of magnitude over 1992—from $38.7 million to $4.79 billion. That same year, Israel's imports from China ($10.47 billion) exceeded even those from the United States ($10.25 billion). In terms of trade balance, China was Israel's second most important economic partner in 2018 at $2.85 billion, only behind its much larger $6.53 billion trade with the United States.[10] China contributes an estimated ten to 20 percent of all foreign investment in Israel.[11] Much of that is in infrastructure and the technology sector.

This dramatic Israeli exposure to Chinese involvement in critical infrastructure, investment in Israeli companies researching or producing dual-use technology, and purchase of Israeli dual-use technologies is alarming for U.S. policymakers. The concern extends beyond any one Chinese project or investment, encompassing a comprehensive and systematic effort by China to insinuate itself into Israeli infrastructure and exploit its intellectual property, just as it has in the United States. In interviews, American officials have expressed frustration that their Israeli counterparts have not been forthcoming nor acknowledged there is a problem.[12] With the Israeli security establishment primarily focused on the country's numerous threats throughout the Middle East, the dangers that China poses have slipped below the radar until very recently.

It is impossible for the United States to completely decouple from China, but it is seeking to disconnect its supply chains in areas of vital interest, including but not limited to medical, security, microchip technology, 5G, and critical minerals. As the United States pursues this shift and encourages its allies to do the same, Israel could find itself outside of trusted U.S. military, financial, commercial, and technological networks, unless it acts decisively. Reciprocally, Israel represents "an innovation hub" of entrepreneurship and offers unparalleled partnership opportunities that would be an asset to the United States in the Great Power competition with China.

A systematic and concerted effort undertaken jointly by the United States and Israel to both protect their economies against Chinese penetration as well as create new mechanisms for safe and vetted bilateral investment and R&D could deepen this already strong partnership. This JINSA study identifies the facts, analyzes the issues in their complexity, and proposes a strategy for the United States and Israel to solve this set of China-caused issues, one that can also serve as a model for other U.S. allies.

III. China's Global Strategy

Under the leadership of Xi Jinping, China is contesting the liberal international order and U.S. global leadership through a geo-economic strategy that leverages civil-military fusion to exploit legal commercial activity for geopolitical aims.

A. Geo-economics

In 2017, China announced it was beginning a "new era" in which it would "take center stage in the world."[13] Part of this newly aggressive Chinese approach involves seeking an expanded role in the Pacific, by claiming a far-reaching and unsubstantiated sphere of interest, backed up by growing power projection capability designed to displace U.S. presence and influence in the region. According to the Department of Defense's annual *Military and Security Developments Involving the People's Republic of China 2020*, the People's Liberation Army of China Navy (PLAN) has an "increasingly modern and flexible force" that is also the world's largest at "approximately 350 ships and submarines, including more than 130 major surface combatants."[14] In comparison, the U.S. Navy currently has 293 ships. The DoD report also noted that "China has already achieved parity with—or even exceeded—the United States in several military modernization areas, including shipbuilding, land-based conventional ballistic and cruise, and integrated air defense."[15] This path to Chinese global power lies in harnessing China's quickly growing economy to provide the means to build a military that could compete with the United States.

But there is also, as Hal Brands and Jake Sullivan have written, a second path to global power for China. This path, political and economic in nature, involves building "a new Chinese-led security and economic order across the Eurasian landmass and Indian Ocean, while establishing Chinese centrality in global institutions."[16] China's strategy seeks wealth for domestic reasons, but it also pursues economic dominance as a route to geopolitical power and the degradation of U.S. influence. This approach rests on the fundamental understanding that the United States' strong economy undergirds its material military might but that its economic performance depends on the open, global commercial and financial markets it has helped create over the last seven decades. A less confrontational and potentially costly path to Chinese victory, thus, can be found in undermining this source of American power—not just its economy but the global order that supports it.

In this manner, geo-economics and geopolitics are unified in Chinese strategy, much more so than in Western concepts of strategy. Chinese officials take seriously the implications that military and economic strategies are in service of ultimately political overarching aims. Thus, beginning in the early 2000s, Beijing switched from restricting foreign investment to a new policy of "Going Out" to encourage Chinese investment in key economic sectors abroad. Outbound investment grew over 70 times larger in less than fifteen years, from $2.7 billion in 2002 to $196.2 billion in 2016.[17] In 2013, Beijing also adopted the Belt and Road Initiative (BRI) as part of its foreign policy posturing, one component of which included major investments in infrastructure across Asia, the Middle East, and Europe by state-owned enterprises.[18]

This geo-economic strategy proceeds in two phases. First, it combines economic and security priorities by securing valuable natural resources, developing superior technological capabilities, and establishing foreign markets for manufactured goods. In this way, China benefits materially from the open economic order that the United States built and shoulders the burden of maintaining. Second, China is able to exploit its penetration of the global economic order to weaken and subvert it by creating economic dependencies that allow it to influence other countries' political decision making, driving economic wedges between allies, and—perhaps most importantly—gaining access to intellectual property and other data that allow it to distort market outcomes and exploit the innovation-driven economies of its adversaries. The Chinese concept of civil-military fusion has proven critical to this second part of its geo-economic strategy.

B. Civil-Military Fusion

China has long sought access to Western military technology, usually through illegal and covert means to bolster its capabilities. More recently, however, it has come to see the legal and overt acquisition of civil technology as even more important to its global strategy. Through the concept of civil-military fusion, China seeks to use its own seemingly civilian and private entities to gain access to seemingly civilian technologies that it can exploit for military and geopolitical aims.

This approach is at least partially grounded in the understanding of how U.S. innovation has evolved since the Cold War. During the competition with the Soviet Union, the U.S. government funded R&D of technologies to drive military primacy, it was only later that these technologies—like the Global Positioning System or Internet—became commercially available and viable. Today, this logic has been flipped on its head. Cutting edge research and emerging technology—artificial intelligence, autonomy, quantum computing—originates in the private sector while the government rushes to catch up. China is aware of this dynamic, having closely studied the U.S. defense industry and the fall of the Soviet Union when building its civil-military fusion projects. According to Elsa Kania, "Assessing the Potential for Civil-Military Integration," a 1995 report from the former Office of Technology Assessment, "has had substantial readership in China, where it is cited to this day as an example of U.S. efforts to leverage commercial technologies to achieve the benefits of technology transfer for cost savings."[19]

The Chinese geo-economic strategy utilizes civil-military fusion to similarly capture the military and geopolitical benefits of commercial technology, except not just the technology developed by its own industries but also that of Western firms. Since 2017, the Central Commission for the Development of Military-Civil Fusion has guided these efforts with plans to develop and acquire dual-use and innovative technologies. For example, the Science and Technology Military-Civil Fusion Special Projects Plan in August 2017 focused on quantum technology, AI, and biology, with some comparing it to the U.S. Defense Advanced Research Projects Agency (DARPA).[20] Through its investments in companies developing cutting edge technology, through research and design partnerships with Western institutions, and by deploying Chinese nationals to work in Western companies, universities, and labs, China has worked to gain access legally to sensitive IP that it can appropriate and exploit.

China uses Western research to fuel economic development and increase its military capabilities relative to the United States. Its economic policy, Made in China 2025 (MIC 2025), often calls for civil-military integration, with the goal of transferring civilian technology innovated domestically or abroad to the People's Liberation Army.[21] China also uses the West's commercial technology against it, in a bid to undermine the competitiveness of economies built on private sector innovation. By using Western firms' intellectual property to bring to market similar products more quickly and cheaply than those firms are able to, China is able to grab their market share—without any of the sunk costs into research and design—in some cases driving Western companies out of business, depriving Western societies of jobs, and Western governments of revenue. In the case of critical technologies like telecommunications, the Chinese security apparatus is also able to introduce vulnerabilities that allow it to access others' data.

China's geo-economic strategy of civil-military fusion is a comprehensive, global, and systematic effort to exploit legally permissible commercial relationships—such as investment in or purchase of dual-use technology—to subvert the open, global economic order on which U.S. strength, and that of its allies and partners, depends. This threat applies as much to Israel as it does the United States or European nations. Perhaps even more so, because of the vitality and economic importance of Israel's technology sector.

IV. U.S. Exposure to China

The United States has sought to persuade China to act as a responsible member of the international community since the two formalized their relations in 1979. The optimistic belief that economic openness between the two countries would moderate the ruling Chinese Communist Party (CCP) has not come to fruition. Instead, the CCP remains committed to its communist ideology and undermining the U.S.-led international system. Previously, the CCP's aversion to the liberal order was obscured by a strategy in which China sought, according to Den Xiaoping to "hide its capabilities and bide its time." Starting with the 2008 financial crisis and accelerating with the rise of Xi Jinping, however, the CCP has shifted to a more visibly aggressive stance, seeking to promote "great changes unseen in a century."[22]

As a result, the United States faces numerous economic and national security threats from a rising China. China's rapid military procurement, particularly its shipbuilding and missile production, enables it to project greater power abroad. Similarly, its pattern of investments abroad, in infrastructure and critical technologies, is aimed at expanding its economic strength and influence. Between 2011-2018, China accounted for over 90 percent of the Department of Justice's counterintelligence cases benefiting a state and "more than two-thirds of the Department's theft of trade secrets cases have had a nexus to China."[23] Indeed, FBI Director Christopher Wray testified before the Senate Judiciary Committee in July 2019 that "there is no country that poses a more severe counterintelligence threat to this country right now than China." According to Wray, China is trying to "steal their way up the economic ladder at our expense," "a threat that's deep and diverse and wide and vexing…. It affects basically every industry in this country."[24] While America's exposure to China has been significant and global in scale, its recent realization of the dangers has fostered serious efforts to address many of the major issues that Israel also faces, namely predatory infrastructure investments, acquisition and funding of dual-use technologies, and IP theft.

A strong bipartisan consensus has emerged in Washington, perhaps belatedly, on the need to reexamine U.S. economic relations with China. This consensus has only been reinforced by the novel coronavirus pandemic, which has exposed both how critical supply chains, such as pharmaceuticals and personal protective equipment (PPE), are dependent on China as well as how Beijing has aggressively moved to exploit a global crisis to expand its power and influence. Now, U.S. officials have begun exercising more significant regulatory restrictions and reviews on Chinese investment.

Due, in part, to these efforts, Chinese-based direct investment into the United States has been steadily declining from its 2016 peak of $45 billion. It fell to $29 billion in 2017, $5.4 billion in 2018, and $5 billion in 2019.[25] As of May 2020, Chinese investment in the United States had significantly dropped to roughly $200 million, though due largely to the coronavirus pandemic and the lockdowns in both countries.[26] While not all Chinese investment is inherently harmful, the drop in investment coincides with tightened export controls. Tight enforcement of these regulations going forward simultaneously could allow for a rise in Chinese funding, particularly once economies rebound after the pandemic, while blocking malign investments that endanger national security.

Though vulnerabilities, loopholes, and inconsistencies certainly remain, the U.S. effort to defend itself against Chinese economic exploitation has proven robust, yielding increased scrutiny for malicious Chinese investments, significant reductions in Chinese investment into the United States, and stepped-up law enforcement action against Chinese agents.

A. Infrastructure Investment

Chinese investment in U.S. infrastructure and transportation has fallen nearly 100 percent since 2017, when Chinese investment in this sector peaked at $10.41 billion.[27] By 2019, there were no recorded major Chinese infrastructure or transportation investments. Like the drop in Chinese investment as a whole, this drop reflects the United States' increasingly robust regulatory power. The United States has a rigorous process for reviewing investments from foreign companies and individuals into American companies. The Committee on Foreign Investments in the United States (CFIUS) is the primary interagency body overseeing these investments. Responding to the growing threat from Chinese investment, Congress passed the Foreign Investment Risk Review Modernization Act (FIRRMA) in 2018 to expand CFIUS's power. FIRRMA added the ability to review real estate transactions close to U.S. military facilities, which will cut down on China's ability to spy on critical U.S. infrastructure by purchasing nearby property. CFIUS is among the world's most extensive foreign investment oversight systems, with both Congress and the executive branch proposing new regulations in recent years to tighten its regulatory control.

i. U.S. Homeports and China

Currently, none of the homeports for U.S. Navy ships, either in the continental United States or overseas, have a disclosed Chinese stake in their management or ownership (all homeports are at U.S. or allies' naval bases). However, China does operate certain port services and facilities at commercial ports near—but not immediately adjacent—to U.S. Navy homeports. State-run China Shipping Lines is an equity partner with a U.S. joint venture that runs shipping container services for part of the Port of Seattle,[28] which is roughly 20-, 30-, and 50-miles' sailing distance from U.S. Navy homeports in Bremerton, Everett, and Bangor, respectively (they are also separated from Port of Seattle by geographical features such as Kitsap Peninsula and Whidbey Island). Other homeports in the continental United States are either physically remote from commercial ports or any nearby commercial port is run by private U.S. companies or government.

B. Military Appropriation of Dual-Use Technology Purchases

As part of its efforts to improve civil-military fusion, China has been purchasing dual-use technologies abroad, like semiconductors, cybersecurity, AI, biotechnology, and quantum technology. In 2012, for example, the United Technologies Corporation and two subsidiaries admitted in federal court in Connecticut to selling software to China that helped it develop the Z-10, its first modern military attack helicopter. According to U.S. Attorney David Fein, the company "took what it described internally as a 'calculated risk,' because it wanted to become the exclusive supplier for a civil helicopter market in China with projected revenues of up to $2 billion."[29]

The U.S. export controls regime is designed to restrict Chinese companies' ability to acquire dual-use technologies by directly purchasing American products, but it still suffers from several limitations. Export controls are also often slow to recognize the technologies critical to security because they focus on "products rather than broad technologies," according to Defense Innovation Unit Experimental (DIUx).[30] Another challenge is that different U.S. agencies are responsible for determining technologies covered under export controls, primarily the State and Commerce departments, with the Department of Defense advising.

While existing U.S. policy does not eliminate the challenge, Washington has woken up to the need for improvements. Washington has put new regulations in place to enhance restrictions on technology sales, focusing on radar equipment, optical materials, and semiconductors. Former Deputy Assistant to the President Tim Morrison argued, "The Chinese have said to us, 'anything you give to us for a commercial purpose is going to be given to the military,' what point is there in maintaining a distinction in our export control regulations?"[31] This statement is both an acknowledgment that U.S. foreign investment oversight and export controls have not adequately blocked the extent of China's technological pursuits while also demonstrating U.S. resolve to adapt and tighten those controls. To that end, in April 2020, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) instituted two new export control rules that target China's civil-military fusion by expanding the definition of military end-use and cutting down on loopholes.

C. Acquiring Dual-Use Intellectual Property

Beyond purchasing existing dual-use systems, one of China's primary goals is to acquire innovative technologies, developed by others, that it can sell for commercial gain as well as use to its military advantage. The CCP has specifically focused on emerging technologies like semiconductors, robotics, AI, financial technologies, and augmented and virtual reality, that would put the United States and its partners at an economic disadvantage. To that end, Chinese investment has been interested in technology startups, particularly those in Silicon Valley.

Between 2006-2012, Chinese investment in the U.S. technology sector amounted to roughly $35 billion.[32] According to CB Insights, between 2012-2017, China-based firms and individuals have invested $19 billion into 641 different U.S. technology companies.[33] Investment in early technologies peaked in 2015 with Chinese investors funding 271 deals for a total of $11.5 billion or approximately 16 percent of that year's technology deals.[34] Chinese investment may account for roughly 10 percent of all U.S. venture investment per year.[35]

CFIUS enables the U.S. government to monitor foreign transactions but was not designed to stop the purchase of individual technology platforms. Initially, investments that did not result in a foreign actor having controlling interest did not fall under its jurisdiction. With the passage of FIRRMA in 2018, CFIUS now has much more expansive review jurisdiction over transactions that could facilitate the transfer of technologies but do not necessarily result in a foreign entity having control of a U.S.-based company. Still, it appears that Chinese attempts to acquire IP through investments, particularly in start-ups, has waned. In 2019, Chinese venture capital investment into the United States decreased from $4.7 billion to $2.6 billion because of "technology market turbulence," political trouble between the two countries, and U.S. regulations.[36]

D. Intellectual Property Theft

China attempts to steal intellectual property through a combination of illegal and legal means. The CCP has authorized cyber hacking and physical theft of American businesses and research institutions. Through these intrusions and espionage, the Chinese government has acquired important commercial information that gives Chinese companies an unfair advantage over foreign competitors. The CCP also positions Chinese academics at American research institutions and leverages its protectionist foreign investment policies to coerce American companies to direct IP theft.

Chinese telecommunications firm Huawei is near the top of companies that raise the most concerns among U.S. officials. The business appeared on a Pentagon list released in June 2020 as having ties to the Chinese military.[37] On January 16, 2019, a U.S. indictment alleged that the company stole trade secrets from T-Mobile, including the physical theft of a mechanical arm. Another indictment on January 24, 2019, detailed how Huawei illegally hid its transfer of goods to its businesses in Iran by using an unofficial subsidiary. Finally, a superseding indictment on February 11, 2020, added charges for conspiracy to steal IP, conspiracy to engage in wire fraud, and racketeering conspiracy.[38] The charges allege that Huawei and its Silicon Valley subsidiary Futurewei stole trade secrets necessary to make routers and then sold them in the United States. While CISCO is not named as the victim in the indictment, it claimed in a Texas lawsuit against Huawei and Futurewei that "slavish copying" allowed access to simpler code while "improper means" were employed to acquire better-protected code.[39] Nor are Huawei's copies of CISCO routers used only to steal market share. They are also built with backdoors and vulnerabilities to allow Chinese intelligence services to surveil the data they transmit. The latest indictment alleges that Huawei helped the Iranian regime install surveillance technologies that it used against anti-regime protestors in 2009. Huawei misrepresented its business dealings in Iran and North Korea to U.S. financial institutions and Congress.

i. IP Theft in Academia

China uses a combination of espionage and financial programs to induce the theft of research at academic institutions. Many Chinese students and researchers studying abroad are trained and directed to steal data and bring it, along with research expertise and techniques learned in the United States, back for Chinese commercial and military use. It is crucial to note that Beijing is particularly interested in attracting professionals who can limit U.S. efforts to decouple its critical supply chains from China.[40] Recruitment initiatives like the Thousand Talents Program seek to lure scientists to bring their knowledge to China, both to conduct their research in China but also to enable where local companies can steal proprietary information for their own commercial gain.[41]

In the assessment of FBI Director Christopher Wray, "this means American taxpayers are effectively footing the bill for China's own technological development. China then leverages its ill-gotten gains to undercut U.S. research institutions and companies, blunting our nation's advancement and costing American jobs."[42] One participant of the Thousand Talents Program, Hongjin Tan, a Chinese national who was a lawful American permanent resident, was convicted in a U.S. court of stealing more than $1 billion from an Oklahoma-based petroleum company. Another Thousand Talents Program recruit, Shan Shi, stole IP about syntactic foam—an important submarine technology.

Increasingly, U.S. law enforcement has focused on, and begun dismantling, Chinese IP theft in academia. In January 2020, the FBI indicted Charles Lieber, the chair of Harvard University's Chemistry and Chemical Biology Department, and two Chinese nationals in separate cases. According to court documents, Lieber became a "Strategic Scientist" at China's Wuhan University of Technology (WUT) in 2011 and a participant in China's Thousand Talents Program "in or about 2012 to 2017." This was done without Harvard's knowledge and in violation of federal grants that required him to disclose foreign ties.[43] Prosecutors also indicted Yanqing Ye, a Boston University robotics researcher, for concealing that she was a lieutenant in the Chinese army serving at the National University of Defense Technology (NUDT), a leading Chinese military academy, and lying about being a student on her J-1 visa. Ye's electronic devices revealed that "at the direction of one NUDT professor, who was a PLA Colonel, Ye had accessed U.S. military websites, researched U.S. military projects and compiled information for the PLA on two U.S. scientists with expertise in robotics and computer science."[44] The FBI's third indictment was against Zaosong Zheng, a cancer researcher at Beth Israel Deaconess Medical Center in Boston, who was arrested at Boston Logan International Airport with 21 vials of biological samples. Prosecutors allege that he was bringing them back to China.[45]

ii. Economic Exploitation of IP

Beijing has protectionist policies that force U.S. companies desiring to sell products in China into joint ventures with Chinese companies. These policies restrict foreign companies from specific commercial activity in China without having a Chinese partner. Beijing has also demanded that American companies transfer their technologies to gain the administrative licenses necessary to conduct commerce in China. The CCP implements many of these protectionist policies through informal means, but its complete control over the Chinese government and economy compels any company wishing to do business in China to abide by its rules.[46] While the Chinese government argues that foreign firms willingly enter these arrangements, these policies give an unfair advantage to Chinese companies by forcing their competitors to relinquish innovative technologies to gain access to China's large and growing market. Therefore, American companies face a disadvantage in China that does not exist for Chinese companies in the United States. Chinese theft is estimated to already cost the U.S. economy between $180 billion and $540 billion a year.[47]

Despite success in confronting other parts of China's geo-economic strategy, dealing with IP theft and transfer remains a challenge for the United States. In January 2020, the United States and China agreed to Phase One of a trade deal that included Beijing pledging to end its practice of forced technology transfer and to enact stronger IP rights protections.[48] The deal requires China to publish a plan on how it will put these measures into place, but it includes no specific monitoring or enforcement mechanisms. Determining Chinese compliance will prove difficult as will ascertaining whether an American company sells its technology or IP to Chinese companies willingly or under government duress. Meanwhile, the coronavirus has already put the viability of the agreement in doubt. Due to the pandemic, China is not on track to fulfill one of the agreement's core components, a pledge to purchase $200 billion in U.S. goods and services.[49]

V. China's Investment in Israel and Its Dangers

In the United States, Israel, and around the world, China's efforts to increase its global military and economic power through the acquisition of critical technologies and domination of vital industries occurs not just by theft, but also through open commerce. In particular, China exploits regular commercial activities such as: provision of critical civilian infrastructure services; investment in commercial dual-use technology, which, under U.S. law and policy as well as international law, is distinct from military technology; and joint R&D. Through these means, China gains access to critical infrastructure that allows it to control global commerce, advanced technology that it can adapt for military purposes, and intellectual property that it copies and reproduces at a significantly lower cost to reduce the economic competitiveness of the Western private sector. All of these activities, in turn, also aid and abet further Chinese commercial, political, and military espionage and theft.

Discussions of Chinese investment in Israel often refer to a handful of high-profile and particularly troubling cases—the Haifa port or Sorek desalination plant, for example. However, China's activity in Israel, and by extension Israel's vulnerability to Chinese exploitation, is far greater than these individual instances suggest.

Israel could become susceptible to Beijing's targeting of U.S. partners with a combination of lawfare, cyber operations, and coercive economic pressure. For example, a Chinese official recently tweeted a manipulated image of an Australian soldier holding a bloody knife against the throat of an Afghan child. The picture was falsified and posted seemingly to diminish Australia's global standing as the two countries' trade disputes grow and after Canberra called for an international inquiry into the coronavirus's origins.[50] Beijing's ability to translate these unconventional pressure tactics into political and strategic leverage grows alongside its trade relationships. The longer Chinese companies have ties to sensitive Israeli industries, the greater the leverage that China will be able to exert. Given that many nations and international bodies have preexisting animosity towards Israel that predisposes them to China's manipulative tactics, Jerusalem could be susceptible to this type of pressure campaign.

Realizing just how far-reaching Chinese efforts at economic penetration are, and the danger they pose to Israel and the U.S.-Israel partnership, is necessary to understand the alarm being sounded by U.S. policymakers, which extends beyond any one project and beyond the inadequacy of Israel's defenses and response to date, and instead, emphasizes the importance of a systematic and thorough response.

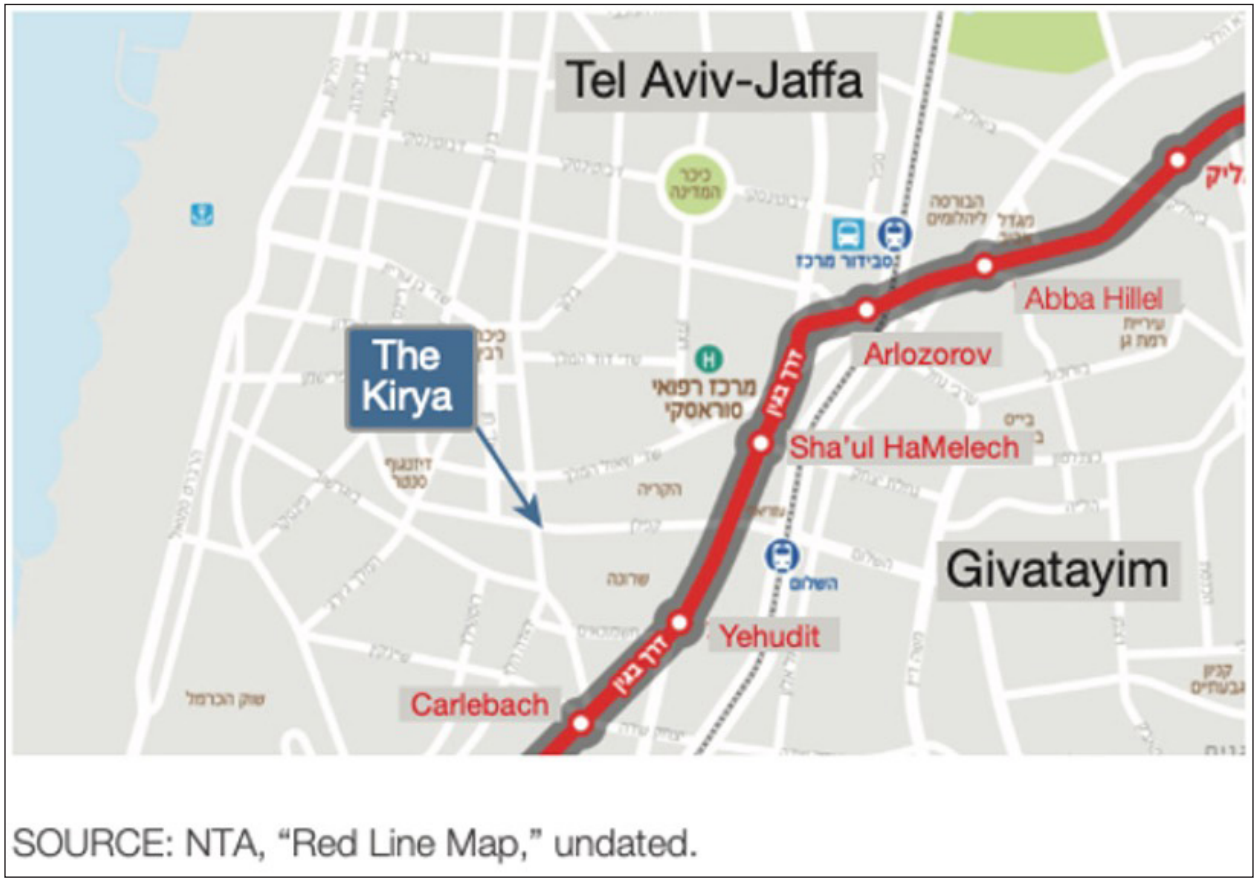
A. Infrastructure Investment

Chinese companies have become increasingly active in Israel's economy through construction projects. State-owned Chinese companies have been involved in major Israeli infrastructure projects totaling $4 billion, including the digging of the Carmel tunnels in Haifa, construction of a light rail in Tel Aviv, the expansion of the Ashdod port, and, most alarming for U.S. security, the extension of the Haifa port.[51] As is typical with Chinese foreign ventures, these companies have significant ties to the Chinese military[52] and are likely motivated as much by the state's strategic interests as economic concerns, although discerning which motivations are state-driven may be a difficult task. However, given the lack of randomness in Chinese investments

in Israeli infrastructure—all the projects are in strategic locations—Beijing's long record of espionage, and, most recently, the announcement that China and Iran may soon sign a 25-year trade and military partnership agreement, the potential for Chinese surveillance of key Israeli infrastructure is both real and concerning.

For instance, China Civil Engineering Construction Corporation (CCECC) has been linked to numerous infrastructure projects in Israel. It bored tunnels for Highway 23, also known as the Carmel Tunnels, in 2009[53] and for the Gilon tunnel on northern Israel's Acre–Carmiel line in 2014.[54] In June 2015, it won together with Danya Cebus a bid to build the Carlebach underground station of the Tel Aviv light rail, which connects the Red and Green Lines near HaKirya, the location of the Israel Defense Forces' (IDF) headquarters.[55] That same year, Israel's NTA Metropolitan Mass Transit System awarded CCECC a contract to build underground stations and tunnels for the eastern part of the Tel Aviv light rail.[56] Yet, CCECC's parent company is the China Railway Construction Corporation (CRCC), which the World Bank blacklisted for nine months in June 2019 "in connection with misconduct under the East-West Highway Corridor Improvement Project in Georgia."[57] CRCC also appears on a list of companies that have ties to the PLA that the Pentagon released in June 2020.[58]

Tel Aviv Light Rail Red Line



SOURCE: NTA, "Red Line Map," undated.

Shira Efron, Karen Schwindt, and Emily Haskel, *Chinese Investment in Israeli Technology and Infrastructure: Security Implications for Israel and the United States* (Santa Monica, CA: RAND Corporation, 2020), p. 55.

Similarly, state-owned China Railway Tunnel Group, the other Chinese enterprise contracted to build the Tel Aviv light rail, has a history of conducting business in Iran.[59] In fact, three months prior to being awarded the $800 million Tel Aviv project in May 2015, its parent company launched a $2 billion project to build a high-speed rail between Tehran and Isfahan.[60] Yehuda Bar-On, CEO of NTA, has said that Israeli security services are advising on the project but that they did not say working with the Chinese companies could pose a problem.[61] However, China could use this construction project to install persistent surveillance of HaKirya, one of Israel's most important military structures.

Yet another example of Chinese military-linked companies working in Israel is the China Harbour Engineering Company (CHEC), a subsidiary of the China Communications Constructions Company (CCCC), which is constructing an expansion of the Ashdod Port. But CCCC's past engagements include various Chinese military construction projects as well as, allegedly, China's island reclamation projects in the South China Sea.[62] CHEC has constructed projects for the PLA that are suspected of being intelligence collections sites, such as one in Argentina.[63]

U.S. outreach to Israel has thwarted some Chinese infrastructure projects. Under pressure from the White House last year, Israel awarded a tender to build the Sorek 2 desalination plant south of Tel Aviv to IDE Technologies—a local company—over Hutchison Water, which is part of the Hong Kong-based CK Hutchison Group. The announcement came less than two weeks after Secretary of State Pompeo visited Israel in part to discuss Chinese investments in the country.[64] Sorek 2's close proximity to the Palmachim air base and Sorek Nuclear Research Center could have led to Chinese intelligence-gathering on these sensitive facilities. When finished, Sorek 2 will be the largest plant of its type in the world. Yet, several major and particularly sensitive projects continue in Israel with Chinese involvement.

i. Haifa Port

In 2015, Israel's Transportation Ministry accepted a bid put forth by the Shanghai International Port Group (SIPG), a majority state-owned enterprise, to invest $2 billion to construct a new terminal at the Haifa port and operate that terminal for 25 years beginning in 2021.[65] Notably, the Transportation Ministry agreed to the arrangement without input from Israel's security cabinet or its National Security Council and to relatively little international fanfare.[66] Now, intelligence and political concerns over Chinese operation of port terminals in Israel are driving a wedge between U.S. and Israeli officials.

In particular, the future Haifa terminal presents an unacceptable security risk to U.S. interests as it is situated right next to Israel's main naval base. The U.S. Sixth Fleet frequently makes Haifa a port of call, a powerful symbol of American commitment to Israel's security and to the U.S.-Israel military relationship. These visits also demonstrate a U.S. presence in the Eastern Mediterranean, which is increasingly becoming a hotbed of security competition. However, future U.S. Navy visits could face limitations or end altogether because of the potential intelligence value that China could gain with SIPG operating a port terminal near where U.S. naval vessels would dock.

The location grants Chinese officials access to a variety of information, from that pertaining to industrial control systems to the level of activity at the Israeli naval base, which may include naval maneuvers by the United States and other Israeli allies. A U.S. Navy ship that visited

the Haifa port with SIPG operating a nearby terminal could expose its electronic warfare capabilities or radar systems. Chinese agents could hack the port infrastructure or visiting ships through numerous cyber or low-tech means, such as directly installing computer viruses with USBs or tools that can monitor network activity.

Similar concerns about the presence of a competitor's systems and personnel near sensitive U.S. military hardware have already led the United States to downgrade its security cooperation with treaty allies. In 2019, the Department of Defense removed Turkey from the F-35 Joint Strike Fighter program after Ankara procured the Russian S-400 air defense system. Israel, which has maintained its Qualitative Military Edge (QME) over regional adversaries with U.S. support and financing, should well understand this U.S. desire to protect its military technology amid renewed great power competition.

Ashdod Port

SOURCE: Google Maps and consultations with Israeli experts; see Efron et al., 2019.
NOTE: Locations are not exact.

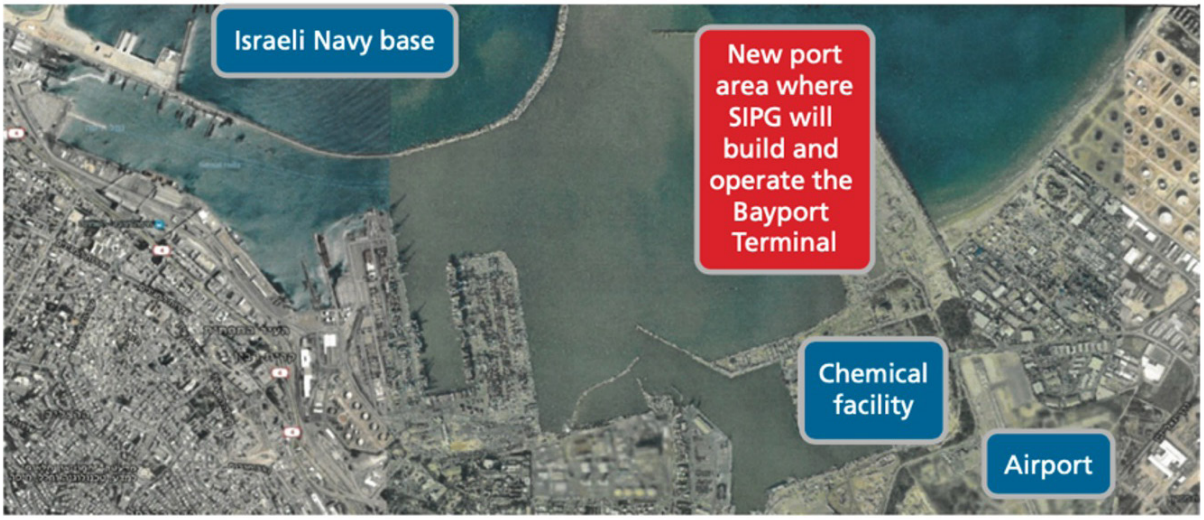
Shira Efron, Howard J. Shatz, Arthur Chan, Emily Haskel, Lyle J. Morris, and Andrew Scobell, *The Evolving Israel-China Relationship* (Santa Monica, CA: RAND Corporation, 2019), p. 110.

Indeed, in September 2018, Israeli Rear Admiral (Ret.) Shaul Horev argued that SIPG's operation of the Haifa terminal could threaten its relationship with the Sixth Fleet. Likewise, Admiral (Ret.) Gary Roughhead, former chief of U.S. Naval Operations, warned in December 2018 that the U.S. Navy could have to port elsewhere because "Chinese port operators will be able to monitor closely US ship movements, be aware of maintenance activity and could have access to equipment moving to and from repair sites and interact freely with our crews over protracted periods…. the information systems and new infrastructure integral to the ports and the likelihood of information and electronic surveillance systems jeopardize US information and cybersecurity."[67]

Soon afterwards, the White House began to apply pressure on Israeli Prime Minister Benjamin Netanyahu, with the State Department warning Israeli officials that intelligence sharing might suffer between the United States and Israel if the latter moved forward with the Haifa port arrangement.[68] During a March 2019 meeting with Netanyahu, the president reportedly echoed the same sentiment by indicating that U.S.-Israeli relations could weaken if Israel continued expanding its relations with China.[69]

After concern grew both about the security threats that SIPG could pose and the consequences of straining ties with the U.S. military, Netanyahu ordered a panel to consider establishing a structure for reviewing foreign investments.[70] Despite such pressures and regulatory reforms in Israel, China is expected to assume operation of the port in 2021. If this occurs, the United States will need to determine whether it will continue to dock its Sixth Fleet

Haifa Port



SOURCE: Google Maps and consultations with Israeli experts.
NOTE: Locations are not exact.

Shira Efron, Howard J. Shatz, Arthur Chan, Emily Haskel, Lyle J. Morris, and Andrew Scobell, *The Evolving Israel-China Relationship* (Santa Monica, CA: RAND Corporation, 2019), p. 108.

at Haifa.[71] A common defense from Israeli officials has been that "the new Chinese-operated terminal is about one kilometer away and not within line of sight of the existing terminal that traditionally docks U.S. warships."[72] However, when JINSA asked senior executive branch officials to address their concerns over the Haifa port plan, these officials stated that the U.S. administration has not seen the details of the port plans or how Israel will mitigate concerns about SIPG. Israel also refused a request to allow the U.S. Coast Guard to review the Haifa port, a disappointing decision that limits Israel's ability to ease U.S. concerns.[73]

These concerns, however, extend beyond the intelligence value that China could gain by operating a terminal at the Haifa port. U.S. officials also worry that Chinese operation of the port would give Beijing leverage if Israel tries to show independence on an issue of Chinese concern.[74] In such a case, China could penalize Israel with slowdowns or diversion of Chinese shipping elsewhere.

Finally, the deals involving Ashdod and Haifa are part of a larger pattern to increase China's global reach by operating key foreign ports. In addition to the potential espionage benefits, operating these ports will help Beijing advance its geo-economic strategy by connecting—and giving China control over commercial flows into and out of—economic markets around the world as part of China's Maritime Silk Road Initiative (MSRI) to link European and Asian shipping lanes.[75] Chinese attempts to build a near monopoly on commercial shipping ports is particularly pronounced and troubling in the Eastern Mediterranean, a region of growing economic importance due to offshore natural gas discoveries. These discoveries are, in turn, producing regional tensions between competing nations, like Greece and Turkey, which China could exploit to its economic and political advantage.

Overseas, the United States has less oversight over the construction and operation of the ports the U.S. Navy visits. For example, U.S. Navy homeports overseas in Spain and Bahrain are adjacent to commercial ports operated by companies from other countries (Turkey and Netherlands, respectively). China does have stakes in various overseas ports where U.S. Navy ships make routine port visits or otherwise dock temporarily in Europe (e.g., Naples, Piraeus, Marseille) and the Indo-Pacific (e.g., Singapore, Australia). Notably, unlike with the controversy arising from a Chinese company operating a new terminal at the Haifa Port, U.S. officials have not said U.S. Navy ships would stop visiting these ports because of their connections to China. Unlike when it visits Israel, the U.S. Navy can dock away from the commercial port areas where the risks of Chinese espionage are highest.[76] Vessels visiting Haifa would not be able to make similar precautions because of Chinese investment in Ashdod and, even more so, in Haifa because all vessels entering the port will have to pass the terminal that SIPG operates. U.S. Navy officials have been concerned that Israel's process for approving the Chinese contract did not adequately include national security officials, and the close proximity of the Chinese operated terminal to the military dock presents a particular risk for espionage.

B. Military Appropriation of Dual-Use Technology Purchases

Under the rubric of civil-military fusion, China has been directly purchasing dual-use technologies abroad, including from Israel. These technologies have a history of being adapted by China to advance its military capabilities.

PLA Navy submarines and frigates use German and French engines acquired through commercial means. MTU Friedrichshafen of Germany builds civilian marine diesel engines under license in China, but these have also reportedly been included in the PLA Navy Song-class attack submarines.[77] Engines from S.E.M.T. Pielstick, the French subsidiary of German supplier MAN Diesel & Turbo, reportedly power the PLA Navy's Jiangkai I and II frigates.[78]

Although Israel may feel confident that, even should its putatively civil technologies end up in Chinese military hardware, its own security will not be threatened, such certainty is misplaced. China might not just keep Israeli technology for itself but also share it with its partners, some of whom are Israeli adversaries.

In July 2020, *The New York Times* reported the existence of an 18-page draft military agreement between China and Iran that "would vastly expand Chinese presence in banking, telecommunications, ports, railways and dozens of other projects. In exchange, China would receive a regular and, according to an Iranian official and an oil trader, heavily discounted supply of Iranian oil over the next 25 years."[79] According to the *New York Times*, the agreement also suggests future joint military exercises, intelligence sharing, and R&D. The $400 billion agreement could lead China to divert dual-use technology it purchases or otherwise acquires to Iran, which could then use it against Israeli and U.S. interests in the Middle East. Iran is actively looking to improve its military capabilities, particularly drone and cruise and ballistic missiles, and could have a greater ability to do so as restrictions from the 2015 Iran nuclear agreement expire over the coming years.

Moreover, given increasing U.S. concerns about China's military build-up, continued Israeli sales of sensitive technology could strain U.S.-Israeli relations, as it has in the past. Indeed, Israel and China have a history of arms sales that the United States has previously intervened to stop. In each case, the disputes between U.S. and Israeli officials created serious tensions between the countries, though these were compartmentalized to the disagreement, allowing strong bilateral relations to continue and grow. In the 1990s and 2000s, American pressure forced Israel to cancel the installation of the PHALCON advanced airborne radar system for PLA surveillance planes. Israel tried to convince Congress to allow the PHALCON sale, but prominent members came out against it.[80]

In 2005, the Bush administration demanded that Israel Aerospace Industries (IAI) refuse to service or upgrade HARPY drones previously sold to China in 1994 for $55 million. The HARPY is a loitering drone designed to attack radar systems and has suppression of enemy air defense (SEAD) capabilities. Taiwan expressed concern to U.S. officials that the 100 drones Israel sold to China could be used in an invasion of the island.[81] In response, the United States temporarily suspended Israel from the F-35 Joint Strike Fighter program. Israel agreed to cancel the arms deal with China and let U.S. officials review future sales. The HARPY incident led to Israel's 2007 Export Control Law, which expanded the requirements for export licenses and restricted arms sales and export of dual-use technology. The dispute also led to the resignation of Israel's Defense Ministry director general Amos Yaron after six years in the position, reportedly under American pressure.[82] In December 2013, Meir Shalit, the head of Israel's defense export control agency, likewise resigned under American pressure after he approved the sale to France of Ricor cryogenic miniature coolers, which are utilized in electro-optical systems like infrared-guided missiles, without restricting their resale. The miniature coolers were then resold to China, and officials believe they ended up in Iran. Shalit flew to Washington to brief American officials and apologize, then resigned.[83]

Since those disagreements, Israel made commitments to the United States that, by all indications, it has kept. Israel put in place and executed policies ceasing all voluntary Israeli transfers of U.S. and Israeli military technologies to China. Now, Beijing is seeking similar military benefits from civil technologies. Israel will need to recognize the threat, both to itself and the United States, and take the same sort of concerted action on dual-use technologies that it took to stop military sales to China.

C. Acquiring Dual-Use Intellectual Property

Fundamentally, Chinese foreign direct investment (FDI) is illusionary. Chinese capital enters at the cost of creating Chinese competitors. Chinese companies do not have to invest nearly as much in R&D because they misappropriate technologies via investment or stealing and then the Chinese government subsidizes their growth in order to weaken, or even eliminate, Western competitors. While this strategy has been at work in the United States, United Kingdom, Canada, Japan, Europe, Australia, and Israel, most countries have struggled to craft policies with mechanisms to effectively block predatory investments.[84]

Israel's success as a "start-up nation" offers China a unique opportunity to improve its technological capability. The most important pathways for Chinese investment in dual-use technology have been mergers and acquisitions, joint ventures, and investments in mature companies, start-ups, and venture capital funds. According to data compiled by RAND, "between 2011 and 2018, Israel's technology sector received the most Chinese investment, both in terms of monetary value ($5.7 billion) and number of companies (54 of the 87 investments reviewed)."[85] Chinese investment provided $325 million in the first three quarters of 2018 to Israeli technology start-ups, a 37 percent increase from the previous year, while doubling in venture capital from $500 million in 2014 to $1 billion in 2016, according to RAND.[86]

Chinese investment in companies that manufacture and develop drones, satellites, semiconductors, artificial intelligence, and even aluminum and steel could lead to their sensitive capabilities winding up in the hands of the Chinese government and military. Investments from Alibaba into ThetaRay ($15 million) and Go Capital into Kaymera ($10 million) create the risk that China will acquire the dual-use cybersecurity technologies these companies produce. Particularly dangerous is Huawei's acquisition of Toga Networks, an IT and telecommunications company, for reportedly $150 million and HexaTier, a database security company, reportedly for $42 million. According to Reuters, "Huawei will use HexaTier to set up a research and development center in Israel for databases in the cloud."[87] China and Israel have also established the Sino-Israeli Robotics Institute (SIRI) in 2015 as "the centerpiece of a new $2 billion industrial park in Guangzhou that will be dedicated to bringing to life the robotics research done by Israeli and Chinese researchers," *The Times of Israel* reported, while Chinese investors, along with the city of Guangzhou, agreed to invest $20 million in the Israeli Robotics Association.[88] In light of these and similar investments, Israeli officials should continuously monitor the country's innovation base as the Chinese state seeks access to IP for commercial and military use.

On the other hand, Israeli research has generally downplayed the threat from Chinese investment in technology, instead focusing on the political divisions it causes with Washington as the primary problem to overcome. Zeev Holtzman, founder and chairman of IVC Research Center, claims that between 2016 and May 2020, total investments in Israel's high-tech sector were $33.15 billion, with $1.43 billion being from China (4 percent of total investments).

Meanwhile, total exits in the sector amounted to $73.67 billion, with $6.2 billion being Chinese acquisitions (eight percent of the total exit value). According to Holtzman, the total venture capital that Israeli high-tech firms raised in the same time period was $10.8 billion, with Chinese investments totaling less than $500 million (five percent of the total).[89] The largest transfer leaving Israel was Chinese acquisitions of Playtika, a gaming company for $4.4 billion. While investments in these companies may appear innocuous, gaming technologies, such as virtual reality, are becoming increasingly similar to military simulators.[90] Therefore, breakthroughs in the gaming sector, which would seem to have little impact on national security, could be the foundation for further innovations that have military use.

Indeed, there are multiple examples from the United States and Europe that demonstrate how Chinese acquisition of Western companies is used to increase Chinese military capabilities or assume control of critical supply chains. In 2008, Chinese railway Zhouzhou CRRC Times Electric purchased the UK-based Dynex Semiconductor, which is reportedly important to the electromagnetic catapults on the PLA Navy's new aircraft carrier.[91] According to a 2018 DIUx report, "the Chinese semiconductor industry now controls a significant percentage of the supply of older chips used in maintaining U.S. military aircraft and equipment designed 40 years ago and still in service." The report further warned that, "China has targeted several key technologies such as jet engine design which will reduce current U.S. military superiority and is actively working to acquire companies that will close this gap."[92]

D. Intellectual Property Theft

China seeks foreign IP through various approaches, including illegal means such as state-sponsored hacking, physical theft, and counterfeiting. But it also uses legal activities—foreign investments, coordinating with foreign companies on R&D, and embedding Chinese scholars and students at foreign universities—to enable its IP theft. China also coerces foreign companies to give up their IP in exchange for access to the large Chinese market. Whatever the means, the objective is the same: get the IP and exploit it for China's commercial and military benefit.

i. IP Theft in Academia

Israel enjoys a robust academic environment, particularly in science and technological fields, which faces similar risks as the United States. Israel and China established a scholarship for Chinese students to study in Israel in 2015. According to Emma Afterman, head of international policy for Israel's Council for Higher Education, there are currently 1,000 Chinese students on Israeli campuses every year, with most studying science, engineering, and technology. On the other hand, only a few hundred Israelis study in China every year.[93]

Israel currently has four academic intuitions in China, including Guangdong Technion Israel Institute of Technology in Shantou, which is the first Israeli university in China, and the XIN Center, a "joint center for innovative research and education to be funded by government and private enterprise" that "will seek to develop solutions for pressing problems in areas such as water, energy, the environment and medicine," as well as growth-sectors like nanotechnology.[94] While China has no academic institutions in Israel, it has Confucius Institutes at the Hebrew University of Jerusalem and Tel Aviv University campuses.[95] In February 2019, the Senate's Permanent Subcommittee on Investigations determined that the CCP controls

Confucius Institutes. The United States designated the institutes as a foreign mission of the CCP in August 2020, requiring them to notify the U.S. government about funding, personnel, and curriculum.[96]

ii. Economic Exploitation of IP

Once China possesses foreign IP, it deploys it, not just to develop new military capabilities but to wage economic warfare against free market democracies and the international economic order. By copying and marketing products designed by Western firms, China is able to undercut them, gain market share, and cause economic harm to the companies whose IP it has stolen.

Other examples of the economic harm done by Chinese access to IP remain plentiful. Hackers believed to be working in China sat inside the Canada-based telecommunication firm Nortel Networks' system for a decade, stealing the company's IP. While Nortel once "dominated the market for fiber-optic data transmission systems," according to one report, and "invented a touchscreen wireless device almost a decade before the iPhone and controlled thousands of fiber-optic and wireless patents," it was bankrupt by 2009.[97] McAfee's *Night Dragon* report in 2011 similarly warned that "global oil, energy, and petrochemical companies" faced advanced, persistent cyberattacks that were "targeting and harvesting sensitive competitive proprietary operations and project-financing information with regard to oil and gas field bids and operations."[98] In 2013, a report by cybersecurity firm Mandiant claimed that the PLA's Unit 61398 (known as Advanced Persistent Threat 1 or APT 1) stole hundreds of terabytes of data from at least 141 companies, with 115 based in the US and 3 in Israel.[99] Mandiant drew a reasonable assessment that China's theft benefited its domestic businesses.

But hacking and other covert practices are not the only way for China to gain access to IP that it can then use in its geo-economic strategy to bankrupt the West. Through its investment in Western companies and joint ventures and through the power of its domestic market of over one billion consumers, China is able to lure or pressure companies to share their IP with it.

By leveraging protectionist policies, Beijing can entice foreign companies and academic institutions to engage in joint ventures with Chinese companies. For example, the Computing Technology Industry Association claims U.S. information technology companies struggle to sell products in China because of, among other factors, "forced transfer of technology and IP to Chinese joint venture partners, [and] weak enforcement against widespread IP theft, discrimination against foreign IP under the guise of national security...."[100] China's approach to foreign aircraft manufacturers provides another example. China's three largest airlines—Air China, China Eastern, and China Southern—are all state-owned, providing Beijing "leverage to maintain a balance between purchases of foreign aircraft and to pressure them to form [joint ventures] with Chinese companies and localize production," according to a 2018 report by the Office of the US Trade Representative.[101]

China also forces foreign companies seeking to do business in China to expose their IP, allowing it to reverse engineer or outright copy technology. The 2017 Cybersecurity Law requires foreign companies with operations inside China to store their data on Chinese servers, making them susceptible to government inspection. Another exposure point to potential Chinese theft occurs when foreign companies provide technical data in their applications for Chinese patents. Israeli companies have increasingly patented their goods and services in

China since the 1990s. Meanwhile, there has not been a similar increase of Chinese patents in Israel. According to data compiled by RAND, Chinese nationals applied for twenty-one patents from 1994 to 2015, while Israelis filed 283 requests during this same period.[102] Israeli applications in China have steadily grown, but Chinese patent submissions in Israel peaked in 2011. This uneven relationship suggests that China sees Israel as a source for building IP and not as a market for their own IP.

China's use of legally permissible entry points into U.S., European, and Israeli economies has given it significant access to cutting-edge Western technologies and global infrastructure. The ramifications of this are reflected not just in rising Chinese military power but also in its comprehensive and systematic efforts to subvert the international economic order. Those most vulnerable to these Chinese efforts are countries that depend on innovation and technology for their economic growth, like Israel.

VI. Legal Protections Against Chinese Exploitation: Comparing U.S., Allied, and Israeli Approaches

The United States and some of its allies have taken critical steps in recent years to strengthen both their foreign investment review and export control architectures. Unfortunately, despite some positive progress in Israel, its legal frameworks in these areas remain ad hoc and ill-defined.

A. U.S. Legal Framework

As awareness has grown in the United States and among its allies of how the open global economic order they have built is being exploited and subverted by China, policymakers have sought both to bolster existing, and create new, legal frameworks and institutions and to create new ones to thwart Chinese ambitions. These attempts rest on two foundations: foreign investment review and export control. Put simply, the first monitors inbound capital, restricting Chinese investment in critical domestic infrastructure and companies; the second limits outbound purchases, prohibiting legal transfer to China of a range of dual-use and emerging commercial technologies with potential applications in the military and security realms.

These twin pillars are interrelated and mutually reinforcing. To be effective, both must be in place. For instance, if unable to purchase certain technology on the open market, China could simply invest in the companies that produce it, acquiring the core intellectual property in that manner. Conversely, if China is cut off from acquiring or investing in companies but can still legally acquire their products, it will still be able to access sensitive dual-use technology. Moreover, both approaches must draw on the same definition and list of proscribed technologies, infrastructure, and IP that is to be kept out of Chinese hands, lest any loopholes be exploited. Thus, the protection of open markets from Chinese subversion requires comprehensive, systematic, and regular legal standards, institutions, and practices.

i. Monitoring Inbound Activity: CFIUS and FIRRMA

The process for reviewing inbound foreign investment into the United States is thorough and robust. The primary interagency body responsible for this review is the Committee on Foreign Investments in the United States (CFIUS).[103] Chaired by the Secretary of the Treasury, the voting members of CFIUS include the secretaries of Defense, Homeland Security, State, and Energy; the Attorney General; the U.S. Trade Representative; and the head of the White House Office of Science and Technology.[104] Non-voting members are limited to the Director of National Intelligence and the Secretary of Labor.[105]

In 2018, amid increased concerns that Chinese investment in the U.S. technology sector was being used to either undercut American technological superiority or advance China's military capabilities, Congress passed the Foreign Investment Risk Review Modernization Act (FIRRMA). The legislation significantly expanded the scope of CFIUS review and reshaped the

framework of the entire regime for reviewing inbound foreign investment.[106] As a result of these changes, CFIUS reviewed the greatest number of transactions in 2019—231 joint voluntary notices (JVNs), up from 229 in 2018 and only 93 in 2010.[107] For further analysis of CFIUS' performance in 2019, see Section A.iii of the Appendix.

CFIUS's authority initially was restricted to performing national security reviews of specifically "covered transactions," which are defined statutorily as any proposed or pending merger, acquisition, or takeover involving a "foreign person" that may result in their gaining "control" over a U.S. business.[108] However, FIRRMA expanded CFIUS review to "non-covered transactions" such as: real estate close to a military site or government facility; non-controlling investments in certain high-risk sectors, or investments where a foreign government has significant interest, either directly or indirectly; or deals that appear to be attempting to dodge CFIUS review.[109]

Under the formal CFIUS/FIRRMA regime, the parties to a transaction may voluntarily file for CFIUS review, or CFIUS may compel review if it believes a proposed or pending transaction presents a possible national security risk. The Office of Investment Security Monitoring and Enforcement within the U.S. Treasury Department is responsible for identifying such transactions, including those transactions subject to mandatory review that have not been properly reported.[110] For those who opt not to file in advance of a given transaction, CFIUS maintains the authority to review the transaction post-hoc indefinitely. The formal review process can take anywhere from one to three months and involves extensive consideration of eighteen different factors. For more information on the procedural aspects of the formal review process, including the particular factors associated with review, see Section A.i of the Appendix.

Aside from these formal channels, an informal review mechanism has gained popularity within the CFIUS/FIRRMA regime. This third path allows for individual CFIUS members to conduct informal reviews of transactions without any set time limit, while allowing the firms and investors involved to maintain discretion and avoid the possible negative reaction that might accompany a formal CFIUS investigation.[111] The informality of the arrangement also enables CFIUS members to work with the interested parties to restructure the transaction to remove any possible security risks.

CFIUS may approve a transaction, impose conditions upon it, or refer the transaction to the President for review, who may then decide to block the transaction if the concerns raised by CFIUS are determined to be sufficiently substantial. Since the establishment of CFIUS, a total of six transactions have been blocked. Thus, the vast majority of transactions are either approved, subjected to mitigating conditions, or canceled following concerns related to CFIUS review. Additional details on the usage of the blocking power may be found in Section A.ii of the Appendix.

ii. Monitoring Outbound Activity: U.S. Export Controls

The United States protects military and sensitive commercial technologies from being acquired by malicious foreign actors through a robust unilateral regime of export controls as well as through subscribing to multiple multilateral regimes.

a. Unilateral Regime

Through the Export Controls Reform Act of 2018 (ECRA), the Arms Export Control Act, the International Emergency Economic Powers Act, and other statutory provisions, Congress has delegated to the executive branch the authority to conduct substantial oversight over exports. The Arms Export Control Act grants the president statutory authority to regulate the export of defense equipment and services. Meanwhile, the ECRA—and in particular, Part I of the ECRA, titled the "Export Controls Act of 2018" (ECA)—authorizes the president to impose controls on putatively commercial exports that might nevertheless have military applications, certain so-called "dual-use" technologies, such as nuclear energy-related items or the Global Positioning System (GPS).[112] More specifically, the ECA gives the Bureau of Industry and Security (BIS), a division of the Department of Commerce, the statutory authority to administer the export licensing and enforcement mechanisms related to critical technologies.

The ECA complements the CFIUS/FIRRMA regime by overseeing potentially harmful investments related to dual-use technologies. The fundamental mechanism at the disposal of BIS for engaging in export controls is the Export Administration Regulations (EAR).[113] Those items subject to the controls laid out in the EAR are assembled in a list known as the Commerce Control List (CCL), which is then divided into ten sensitive categories of exports.[114] An item's classification on the CCL corresponds with a specific set of licensing requirements, under the administration of the BIS, for exporting that particular item.

According to the EAR, dual-use items have "civil applications as well as terrorism and military or weapons of mass destruction (WMD)-related applications."[115] Many dual-use products will not require a license for exporting. However, if the item is either on the Commerce Control List (CCL) or related to "national security, foreign policy, short-supply, nuclear non-proliferation, missile technology, chemical and biological weapons, regional stability, crime control, or terrorist concerns," then the parties seeking to export the items must submit a comprehensive export license application to BIS for approval.[116] Further information on the Commerce Department's processes for defining and licensing dual-use items is provided in Section A.iv of the Appendix.

Interestingly, the EAR also contains a particular mechanism for addressing the transfer of technologies within U.S. borders that nonetheless reach foreign nationals. Referred to as "deemed exports," these products represent a legal fiction of sorts, as they require an export license be obtained from BIS before the controlled technology can be released to a foreign person within U.S. borders.[117] The destination country is regarded as the person's country or countries of nationality. Many of the licenses granted by BIS for "deemed exports" are for unpublished or not widely shared scientific research, often conducted at research and development institutions, universities, and bio-chemical firms and within the medical and computer sector.[118]

The EAR stipulates the timeline for approving dual-use licenses and the punishment for violations. The Department of Commerce has nine days to address a license application or issue, whether that involves referring the license to a different department, granting the license, denying it, or returning it to the applicant. If the license is referred elsewhere, the second agency has 30 days to resolve the issue. Those who violate the EAR's license regime with regards to dual-use technologies may face up to $1 million in fines or 20 years imprisonment.[119]

b. Multilateral Regime

In addition to unilateral control mechanisms established by Congress and implemented by the executive branch, the United States belongs to four multilateral export control regimes, each devoted to curbing the proliferation and potential usage of a particular type of good or weapon: the Wassenaar Arrangement (aimed at limiting conventional weapons and certain dual-used technologies and goods), the Nuclear Suppliers Group (aimed at containing the proliferation of nuclear weapons), the Australia Group (aimed at limiting development of chemical and biological weapons), and the Missile Technology Control Regime (aimed at limiting the proliferation of missiles and related missile technology). According to the Commerce Department, "[m]ost items on the CCL are controlled in accordance with the United States' commitments" to the multilateral export control regimes.[120] In order to receive Strategic Trade Authorization-1 (STA-1) status, which makes it easier for a country to import CCL-designated items from the United States, a nation must become a member of all four groups, though there are certain exceptions.[121] For more information detailing the specific items each regime controls, please see Section A.v of the Appendix.

B. Allies' Legal Frameworks

Despite the obvious threats posed by Chinese investments, convincing U.S. allies and partners to take the threat of Chinese economic penetration with equal seriousness has been a challenge for Washington. Yet, some U.S. allies have strong regimes in place for protecting their economies, like Germany, or have acted quickly to strengthen their protections, like Australia. Reviewing the successes and the pitfalls of the approaches taken by various other U.S. partners may help Israel construct a more effective and efficient process for protecting its economy, particularly given that foreign investment screening and dual-use export control continue to evolve and course correct to meet emerging threats.

i. European Union

In early 2017, France, Germany, and Italy expressed concern regarding the influx of foreign investments into strategic industries located in EU member states, particularly investments from China.[122] This concern was notable, given that the EU was the most popular destination globally for foreign direct investment (FDI) in 2017.[123] After considerable debate, on March 21, 2019, the European Parliament and the Council issued Regulation (EU) 2019/452 to address this apprehension and to establish a more precise and unified approach to screening foreign investments.[124] EU 2019/452 went into force on April 10, 2019, applying to transactions starting October 11, 2020 forward.

While its provisions do not create a harmonized framework of review across Europe, they do encourage information-sharing and cooperation between the member states when conducting independent reviews of foreign investment originating from outside the EU, which may be warranted on the grounds of "security or public order."[125] Under EU 2019/452, the "review" of a particular transaction can be initiated by the government of the member state hosting the transaction, the governments of other non-hosting member states, or the EU Commission.

Although the regulation establishes general guidance for screening mechanisms for foreign investments, it does not force EU countries to adopt such review processes, allowing them

to maintain their "necessary flexibility."[126] The regulation does require each member state to submit an annual report to the European Commission outlining the FDIs that took place in its territory and discussing how the FDI screening mechanisms were applied over the course of the year, but the EU's role is advisory, rather than mandatory. EU 2019/452 ultimately invites a patchwork of screening mechanisms across the European continent, which may lead to the creation of investment havens more receptive to dubious transactions.[127]

ii. Germany

Earlier this year, the German Parliament adopted legislation increasing the mechanisms available to the German government for reviewing non-European investments, in part as a response to COVID-19. Germany's screening regime is a product of the Foreign Trade and Payments Act, in conjunction with the Foreign Trade and Payments Ordinance.[128]

Under Germany's screening regime, the review process can take up to seven months and is overseen by the Federal Ministry of Economics (BMWi). Investment review by the BMWi is triggered when a non-German investor acquires a certain percentage of voting rights in a German company. Threshold percentages triggering review are lower for those companies that are in either the defense sector or one of several protected sectors, which include critical infrastructure, telecommunications, media, and some portions of healthcare.[129] Transactions subject to mandatory review are temporarily void until approved by the BMWi and are rendered legally void if BMWi decides to halt the transaction.[130]

If parties attempt to conclude a transaction without the required approval, they may be subject to a fine and imprisonment of up to five years, specifically if the foreign investor is granted the ability to exercise voting rights over the domestic company, if earnings are distributed to the foreign investor, or if the foreign investor is given access to sensitive information regarding national security.[131] Parties to a transaction in a non-protected sector may voluntarily file for BMWi approval. Approval is deemed to have been granted if BMWi does not conduct a comprehensive review of the transaction within two months of the voluntary filing.[132] For discussion of the BMWi's historical usage of its blocking power, see the Appendix.

iii. Australia

In Australia, the protocol for reviewing foreign investment is an amalgamation of stipulations put forth in the Foreign Acquisitions and Takeovers Act of 1975 (FATA) and Australia's Foreign Investment Policy.[133] Before conducting certain transactions, a foreign person or entity must apply to the Foreign Investment Review Board (FIRB) for approval.[134] After consulting with the FIRB, the Treasurer of Australia determines whether a foreign investment should proceed, based on whether the given transaction is seen as contrary to national interests. In making such a decision, the Treasurer also has the ability to consult with other governmental agencies and exchange confidential information related to the transaction.[135]

In determining whether an investment runs contrary to national interests, the Treasurer may consider the transaction's impact on national security, industry competition, the domestic economy, and Australia's laws and policies, as well as the type of investment that the transaction concerns.[136] The Treasurer may also consider the character of the investor himself.[137] According to FATA, the Treasurer has 30 days to consider an application with the

possibility of a 10 day extension, but per the latest amendments, the Treasurer is free to extend this period by an additional 90 days.[138] Under temporary coronavirus measures, the Treasurer has up to six months to consider a transaction, and all foreign investments, regardless of investment amount or industry, require review, though the zero-threshold trigger is expected to be lifted in January of 2021.[139]

In 2017, Australia established the Critical Infrastructure Centre within the Department of Home Affairs, which operates as a complement to FIRB.[140] It contains a comprehensive record of the critical infrastructure assets within the country, allowing the government to better manage possibly risky transactions across various sectors.[141] The Centre furnishes the Treasurer with information on transactions involving critical infrastructure assets.[142]

Recent reforms to the review process, proposed in July 2020, focus on national security, revisions to the pre-coronavirus thresholds, and stronger enforcement mechanisms. If approved, the criminal and financial penalties for violating the FATA are expected to increase significantly.

C. Israel's Laws and Institutions

Though Israel recently announced the creation of a formal committee to review inbound foreign investments, an informal review process has been steadily building over the last 50 years. However, the current protocol is not particularly robust and represents a cobbling together of various regulations, as opposed to the application of one cohesive framework akin to the ones described above.

i. Current Israeli Protocol for the Review of Inbound Foreign Transactions

a. Defense Industry

The defense industry is a critical sector of the Israeli economy with intimate ties to the national security establishment, and recent legislation monitoring the sector reflects that reality.[143] Israel's Knesset passed the Defense Corporations Law of 2006[144] to shield Israeli defense corporations from possible foreign acquisition or control, in order to mitigate the associated security risks.[145] Per the law, a committee comprised of the prime minister, minister of defense, and the minister of economy and industry have the authority to designate specific corporations as "defense corporations" based on the national security threats possibly posed by the corporations' business decisions, thus rendering them subject to increased oversight.[146] Defense corporations in turn face various restrictions related to their transfer, acquisition, and ownership.

b. Real Estate Industry

As evidenced by the FIRRMA reforms to CFIUS, real estate may present its own risks, based on its proximity to highly sensitive material associated with the national security apparatus. Thus, the Israeli Lands Law[147] of 1960 requires that the sale or transfer of land to a foreigner be approved by the chairman of the Israeli Lands Council, who must consult with the ministers of defense and of foreign affairs, and consider the effect of the sale or transfer on "the public

good and security."[148] The oversight also may be exercised if the land has not been purchased outright, but the foreign investor is leasing the property for longer than five years or has the option to do so.[149] Thus, any foreigner gaining substantial rights to Israeli land will be subject to oversight from several ministers.[150]

c. Telecommunications Industry

The telecommunications industry poses its own security threat because inbound foreign investment may translate into foreign actors and potentially foreign governments gaining access to sensitive information. Israel's regulation of the telecommunications industry over the last several decades represents an attempt to address that threat.[151]

The primary law involved is the Communications Law of 1982,[152] which requires any party engaging in "telecommunications activities" to have a telecommunications license.[153] The Law defines such activities as "the broadcasting, transfer or reception of signs, signals, writing, visual forms, sounds or information by means of wire, wireless, optical system or other electromagnetic systems," essentially meaning that the provision of any telecom services in Israel will demand a license.[154]

The licensing process itself is where the Israeli government may exercise more advanced oversight over foreign investment. When issuing telecom licenses, the minister of communications has the authority to demand certain conditions regarding the ownership structure of the telecom entity or, more precisely, the "holding, transferring or purchasing of Means of Control in a license applicant or in a Licensee" as well as conditions "concerning the appointment of officers" within the telecom entity.[155] These conditions can be updated as the minister sees fit.

d. International Trade

International trade is another arena where the Israeli government may exercise increased oversight over foreign investment. Both free trade agreements (FTAs) and bilateral investment treaties (BIT), negotiated by the Ministry of Economy and Ministry of Finance respectively, allow for the inclusion of specific provisions that offer increased protection of certain sectors, even if such provisions deviate from the standard FTA or BIT most favored nation and national treatment stipulations.[156] For instance, the Israel-Japan BIT includes specific carve-outs in Article 15[157] that allow for deviations from the Model BIT for the sake of national security interests.[158]

ii. Proposed Protocol for Israeli Review of Inbound Foreign Transactions

Last October, Israel's National Security Council announced the creation of a committee to oversee inbound foreign investment, in part due to considerable pressure from the United States to create an analog to CFIUS.[159] The purpose of the committee is to further incorporate national security concerns into the review process for foreign investments and to establish a more centralized and organized oversight apparatus. According to the October 2019 announcement, the committee "will assist regulators in factoring considerations of

national security into the approval process for foreign investments in the areas of finance, communications, infrastructures, transportation and energy."[160]

At this point, not a considerable amount is known about the new oversight body. Senior representatives from the Ministries of Finance and Defense, as well as from the National Security Council, are expected to fill its ranks, while observers from the Ministries of Foreign Affairs and Economy, as well as the National Economic Council, will be present.[161] At least initially, the review process is expected to be voluntary. The Security Cabinet is slated to meet twice a year to review the work of the committee.

Since the committee is yet to be operational, the particulars are not quite complete. According to the October announcement, the review process is supposed to be completed within 45 days. It is unclear whether the committee, seated within the National Security Council, will have the authority to nullify transactions, though at this point its role appears to be entirely advisory in nature.[162] It is also uncertain whether additional reporting, disclosure, or notification requirements will be added to the regime previously discussed.[163]

Whatever committee takes shape will represent a sharp balance between serious national security concerns and strong economic interests. Though Israel seems resistant to establishing formalized mechanisms of review for fear of chilling foreign investment, it is arguably an advantage for potential foreign clients to better understand the investment review regime under which they will operate. However, the "catch" of establishing formalized mechanisms is that the Israeli government effectively must commit itself to halting potentially critical inflows of capital, an act it has suggested it is not particularly keen on performing.

iii. Export Controls: Israeli Review of Outbound Foreign Transactions[164]

As it stands now, Israel has two tracks for regulating exports: one for commercial goods and technologies and another for military-related goods and technologies. Similar to the United States, the export control mechanisms described below also apply to "deemed" exports, which involve the transfer of controlled information and items to a foreign national within Israeli borders.

Israel has a set of export controls analogous to the U.S. EAR for overseeing the export of commercial goods, and parallel to the U.S. Department of Commerce, those regulations are administered by the Israeli Ministry of Economy and Industry. The regime has been criticized as insufficiently robust, and under recent pressure from the U.S. State Department, the Ministry of Economy and Industry released a draft enforcement procedure for public comment in May 2020.

Conversely, Israel's oversight mechanisms for the export of military and defense goods are quite serious and thorough. The Ministry of Defense administers the regime, which runs parallel to the International Traffic in Arms Regulations (ITAR), 22 U.S.C. 2778 *et seq.*, put in place by the United States. It is understood that, as unofficial policy, the Ministry of Defense often consults the U.S. State Department when reviewing applications for licenses relating to military or defense items.

The Defense Corporations Law of 2006 described above was followed by the Defense Export Control Law of 2007[165], which similarly granted oversight authority to exports of defense equipment and technology, the transfer of defense know-how, and the provision of defense services outside Israel. As a rule, the law requires that persons seeking to complete such transactions register themselves and the associated exports of goods or services with the Defense Export Control Agency (DECA), a division of the Israeli Ministry of Defense.[166] Following registration, interested parties must apply to DECA for certain marketing and export licenses. Only then is the transaction permitted to move forward. It is worth noting that DECA is granted wide discretion when it comes to licensing, meaning that transactions can be squashed for a host of different reasons.[167]

There are four lists of controlled items to which the ministries overseeing exports adhere: the Wassenaar Arrangement dual-use list; a compiled list of chemical, biological, and nuclear-related items; the Missile Technology Controls Regime list; and the Israeli rendition of the Wassenaar Arrangement's Munitions list.

Each year, the list of controlled items published by the Wassenaar Arrangement is adopted into law by the Israeli Knesset, with the exception of Category 5—Part 2, which covers items related to "Information Security."[168] If any item appears on this list and is either intended for defense or military purposes or has an end use for such (the end user is usually a strong indicator of the end use), the Ministry of Defense, not the Ministry of Economy and Industry, will regulate such items by overseeing the licensing processes. In addition, a list of chemical, biological, and nuclear-related items—representing an amalgamation of lists compiled by the Nuclear Suppliers Group, the Australia Group, and the Chemical Weapons Convention—remains part of the Israeli export control regime and under the auspices of the Ministry of Economy and Industry.

In addition to the lists described above, the Ministry of Defense operates under two additional lists from which it culls export controls. The first is a list assembled and published by the Missile Technology Controls Regime, while the second is the Combat Equipment List, which is heavily borrowed from the Wassenaar Arrangement's Munitions list, but includes some modifications that ultimately render it distinct.

VII. The Substitute Problem

Beyond the institutional and bureaucratic challenges of constructing the sort of legal protections against Chinese economic penetration discussed above, there are perhaps bigger political and economic obstacles to overcome.

China's geo-economic strategy has been successful because of both the extent of inter-connection between Chinese and Western economies and the latter's lack of available alternatives. As was made lethally clear by the lack of personal protective equipment at the beginning of the COVID-19 pandemic, Western nations depend on supply chains originating in China and finding other suppliers or building new production capabilities is difficult and time intensive. In short, China has made itself indispensable and irreplaceable.

The same, or perhaps even greater, challenges apply to the task of reducing Chinese investment in and provision of critical infrastructure and sensitive dual-use technology. Beijing has spread massive amounts of capital around the globe while strategically developing production and technological capabilities that are vital to the global economy. The prospect of unlinking from China is daunting because there are no clear alternatives. There is no readily available alternative source of foreign direct investment on the level provided by China nor of important technologies, like 5G telecommunications equipment.

To protect themselves from China's economic exploitation, then, countries like the United States and Israel will have to first solve this "substitute problem," which has two elements. First, if there are no substitutes, countries face the prospect of real economic harm by choosing to limit their economic exposure to China. They also will be concerned that they might be acting alone, while their neighbors seemingly continue to prosper from Chinese investment. Second, because of this logic, each country would prefer to wait until there are substitutes available, rather than work to create them.

Part of the solution will likely be U.S.-allied efforts to develop substitutes and alternative supply chains and investment flows. The United States and Israel may be able to pioneer that effort by capitalizing on their respective technology bases—a strategy that can serve as a model for other democratic nations.

A. The Chinese Prisoners' Dilemma

China's geo-economic strategy has purposefully pursued building linkages to Western economies in order to develop such dependencies. Effectively, Beijing has made Western nations its economic prisoners. But they are prisoners not just in the sense of being trapped in a perilous economic relationship with China. They are also prisoners in the sense of being subject to the same divisive logic captured by the mathematical game known as the "prisoner's dilemma."

This game theory exercise supposes two criminals are caught and interrogated by the police. Each is offered the chance to go free if they testify against their partner, but only if their partner does not also implicate them. Individually, the best possible outcome for each criminal is to turn against their partner. Yet, if both partners seek this outcome, and each testifies against the

other, both go to prison and, because the police now have evidence against them, they do so for a longer time than if they had both remained silent.

Western countries confronting Chinese economic penetration are in a similar position to these prisoners. They are concerned not only about their own relationship with China, but also eyeing how their neighbors and partners approach the same topic. While policymakers may fear the economic ramifications of cutting off Chinese investments without ready substitutes, they may also fear the possibility that other countries will choose not to take this difficult step and will flourish, at least in the short-term, as a result.

Like the prisoners, then, Western countries face a coordination and commitment problem. They would be better off if they knew that all of their counterparts would take action against China, but without that certainty, they may all decide to hedge their bets and not risk acting alone. The best way to mitigate these concerns would be the introduction of substitutes for Chinese investment. This would eliminate the economic risks of acting and shift the cost-benefit analysis toward excluding China.

B. The First Mover Problem

The creation of substitutes for Chinese capital and products is needed to help ease the prisoner's dilemma logic, but another obstacle stands in the way of this solution. Given China's size and willingness to spend profligately, no one country is fully able to step in and replace it fully. Nor does any country possess both the technological capabilities and production facilities to supplant Chinese supply chains. Dependence on China might be dangerous, but complete autarky is not a plausible replacement.

Only by working in concert can democratic countries with free markets develop sufficient substitutes to minimize the economic dislocation of unlinking from China. Taken together, the United States, European nations, Japan, South Korea, Taiwan, Australia, and Israel have the wealth needed to create new pools of capital that can replace Chinese investments and the R&D capabilities to innovate replacements for Chinese technologies. Meanwhile, emerging markets in democratic countries like India can replace China both as a producer of consumer goods and as a source of new consumers of Western products.

This creates a catch-22. Countries will be reticent to ditch Chinese capital and supply chains until substitutes are available, but there is little incentive to develop such substitutes, so long as they maintain their economic relationship with China. Breaking through these obstacles requires a first mover—a country to lead the way not only in cutting itself off from pernicious Chinese economic activity but also in developing alternatives. The key, however, is that the first mover must act not just in its own interests, but also in those of its partners, extending to them the early benefits of a non-Chinese economic strategy as proof of concept that decoupling is viable.

C. Leadership, Trust, and Cooperation: America's Legacy

Acting first, and alone, to build the confidence of its partners has been the global role of the United States since the end of World War II. It is a role that the American public and policymakers alike have greeted with increasing skepticism. Yet, it is a role that the United States must play again if it hopes to ward off China's drive for dominance.

Strong bipartisan agreement about the dangers of continued dependence on Beijing has motivated U.S. policymakers to begin taking the difficult steps of excluding China from the U.S. economy while warning allies and partners to do the same. Yet the economic and political challenges of such decoupling, especially for countries with much smaller economies, like Israel, are significant. They cannot be overcome solely by the prospect of intangible and far-off threats. If the United States hopes that other countries follow its path, it will need to pair strict warnings with assistance for surmounting these significant barriers.

To free its partners from the Chinese prisoner's dilemma, the United States will have to convince them that it is committed to its current path of decoupling. Other countries need to be confident that if they act, they will not be acting alone. Convincing them of this should not be difficult, considering the Chinese threat has been elevated to the highest priority by the latest *National Security Strategy*. It is also the increasing focus of U.S. national security institutions, both governmental and not; and the bipartisan consensus that has emerged on this issue. Yet what is obvious in Washington may not be as readily perceptible from a distance. The recent history of abrupt policy reversals between and within administrations might also give U.S. partners reasons to doubt the durability of the current strategy. Repeated and prominent public signaling and private reassurance will be needed to convince U.S. partners, like Israel, that the United States is going to stay its course against China and that they should follow suit.

Secondly, the United States must also demonstrate that not only is it possible to develop economic substitutes for China, but that it is willing to give its partners access to those substitutes. This is likely to impose the costs of being an early, and generous, mover on U.S. taxpayers. But without such inducement, U.S. partners are going to be unsure of their ability to find replacements for China on their own and therefore, will be reticent to expel China from their economies. Early attempts by the United States to provide alternative sources of investment and new partnerships to develop alternative technologies will serve as a down payment on the creation of a new secure and prosperous economic order with other democracies. Countries that are early members of this new coalition will have an outsize influence in shaping it and reaping greater economic and strategic benefits, while deepening their relations with the United States, as a result.

D. Substitutes Exist: Current U.S. Programs

Fortunately, substitutes for China already exist. Numerous existing, updated, or newly created U.S. agencies and programs seek to provide or facilitate transparent and responsible investment in strategically vital infrastructure projects or technological innovations. Many of these initiatives are focused on the U.S. domestic market, but others also involve, or even focus on, U.S. partners abroad. Promoting the existence of these substitutes, expanding them, and involving partners like Israel in them will be critical to solving the substitute problem.

i. U.S.-Israeli Free Trade Agreement

Despite emerging concerns, China has become Israel's second-largest trading partner after the United States.[169] However, the U.S.-Israeli Free Trade Agreement (FTA) has served to increase and facilitate trade between the two partners over nearly four decades. Entered into force in 1985, the U.S.-Israeli FTA was the United States' first FTA and has served for a strong vehicle of economic growth for both partners.[170] Since its inception, U.S. exports to Israel have

increased by over 400 percent. Meanwhile, the United States remains Israel's largest trading partner, receiving roughly a quarter of Israeli exports. And as of 2019, Israel was the United States' 23rd largest goods trading partner and the 24th largest goods exports market for the United States.[171]

The age of the U.S.-Israeli FTA is both a blessing and a curse. As a result of being the United States' oldest FTA, the text itself is in need of significant updating. At the last meeting of the U.S.-Israel Joint Committee in 2016, the primary body responsible for overseeing the FTA, one issue that was presented related to reforming the manner in which certain standards and customs behave as impediments to trade. In 2017, the United States and Israel reached an agreement on new procedures to allow for exporters to receive approval when seeking duty-free status under the FTA.[172] Still, there remain various opportunities within the U.S.-Israeli FTA for possible improving trade relations between the United States and Israel.

ii. Trusted Capital Marketplace Initiative

The Pentagon's "Trusted Capital" Program, launched late in 2019, is representative of the need to balance national security concerns with innovation.[173] The program matches American innovators and small businesses in the defense sector with investors that pose a reduced security risk. Such investors are likely to not have any affiliation with countries of "special concern," such as China, Russia, or Iran.[174] The program envisions itself as a resource for smaller businesses that might otherwise be tempted to turn to less trustworthy funding in order to advance their technological innovations.[175]

iii. Strategic Trade Authorization Status

Strategic Trade Authorization Status, a mechanism for encouraging more trustworthy transactions, is actually a license *exception* to the EAR.[176] It authorizes the license-less export, reexport, and transfer of certain items that are unlikely to be used for the purposes the licenses are meant to prevent.[177] STA status does not apply to transactions that do not require a license or are otherwise prohibited by the EAR.

The STA system has two tiers: the first tier of countries (STA-1) consists of destinations to which the license-free export, reexport, and transfer of products and technologies controlled for a host of reasons is permitted; the second tier of countries (STA-2) features destinations to which the license-free export, reexport, and transfer of products and technologies only applies when such items are controlled for national security purposes.[178] In order to receive such status, a country must accede to all four multilateral export control regimes listed below, though certain exceptions have been made, as in the case of India.

iv. Export-Import Bank of the United States

The Export-Import Bank of the United States (EXIM) is an independent executive agency that serves as the official provider of export credit when private lenders are unable or unwilling to provide financing to U.S. exporters.[179] EXIM's recent reauthorization, signed in December 2019, directed the agency to create a new program, titled "Program on China and Transformational Exports," to ensure that American exporters can continue to compete with Chinese exporters on a global scale.[180] Indeed, China's aggressive usage of export credit

has dwarfed its competitors, including the United States, as President Xi attempts to expand trade and investment opportunities as part of the larger Belt and Road Initiative.[181] As noted by President and Chairman of EXIM Kimberly Reed in a recent hearing before Congress, "From 2015 to 2019, China's official medium- and long-term export credit activity alone was at least equal to 90 percent of that provided by all G7 countries combined."[182]

The explicit aims of the program are "to directly neutralize export subsidies for competing goods and services financed by official export credit, tied aid, or blended financing provided by China or by other covered countries" and "to advance the comparative leadership of the United States with respect to China, or support United States innovation, employment, and technological standards, through direct exports." In order to carry out these initiatives, the program calls for 20 percent of the agency's financing, or the equivalent of $27 billion, to be directed towards the new program, which according to Reed seeks "to support the extension of loans, guarantees, and insurance that are fully competitive with the rates, terms, and other conditions established by the People's Republic of China." According to Reed, the program is directed towards ten specific industries: (1) artificial intelligence; (2) biotechnology; (3) biomedical sciences; (4) wireless communications equipment (including 5G); (5) quantum computing; (6) renewable energy, energy efficiency, and energy storage; (7) semiconductor and semiconductor-machinery manufacturing; (8) emerging financial technologies; (9) water treatment and sanitation; and (10) high-performance computing.[183]

In FY 2019, prior to the authorization of the China initiative, EXIM authorized a total of nearly $8.2 billion to support just over $9 billion in U.S. exports.[184] These values were incurred despite the fact that the Board of Directors lacked quorum until May of 2019 and therefore, could not approve board-level transactions above $10 million.[185] In 2019, 27.5 percent of the total dollar value of EXIM's authorizations were directed towards small businesses, which comprised nearly 90 percent of the total number of transactions.[186]

v. U.S. International Development Finance Corporation

The U.S. International Development Finance Corporation (DFC) is a more financially stable analog to China's Belt and Road Initiative that offers an economic method to challenging China's growing strategic footprint globally. The DFC was established in 2018 under the Better Utilization of Investments Leading to Development (BUILD) Act as a combined successor to the Overseas Private Investment Corporation and USAID's Development Credit Authority. The DFC is America's development bank that utilizes partnerships with the private sector to invest in a variety of different industries, including energy, healthcare, critical infrastructure, and technology. DFC prioritizes investments in low-income and lower middle-income economies, directing financing towards small businesses in an effort to encourage entrepreneurship. The DFC's products include debt financing (up to $1 billion in loans and guaranties for terms of up to 25 years), equity financing (up to $1 billion per project), political risk insurance (up to $1 billion in coverage), and technical development.[187]

The DFC also provides a possible mechanism for stopping countries from adopting technology produced by China, and more specifically, by the Chinese telecommunications company Huawei. Unlike Beijing, Washington cannot order companies to invest in certain projects or direct banks to disperse loans to specific investors.[188] However, the DFC can offer a more transparent, financially sound, private sector, and environmentally friendly alternative to the often opaque, state-directed, and financially unsustainable approach forwarded by

the Chinese government.[189] The European Energy Security and Diversification Act of 2019 lifted restrictions under the BUILD act, authorizing the DFC to "provide support for projects in countries with upper-middle-income economies or high-income economies" so that it can "preempt or counter efforts by a strategic competitor of the United States to secure significant political or economic leverage or acquire national security-sensitive technologies or infrastructure in a country that is an ally or partner of the United States."[190] Having begun operations in January 2020, the DFC committed $200 million towards 10 different projects across Africa, Asia, and Latin America within its first three months.

In September 2020, the DFC approved a $1.5 billion political risk insurance deal associated with a natural gas deal in Mozambique's Rovuma Basin, a decision at least partly driven by a desire to prevent the transaction from falling into China's hands.[191] In the second quarter of 2020, the DFC approved $3.6 billion in new investments, including $62 million in political risk insurance to support the growth of Energy Resources of Ukraine Trading, which currently handles 10 percent of Ukraine's annual gas demand domestically; a $250 million tier-2 capital loan to the Africa Finance Corporation (AFC) to facilitate greater lending at lower rates; a $250 million tier-2 capital loan to Banco Davivienda in Colombia to support the dispersal of home loans to low-income borrowers; and a $150 million loan to BAC San Jose in Costa Rica in order to enable the bank to better aid underserved borrowers.[192]

Currently, DFC has been authorized under Executive Order 13992 to provide loans under the Defense Production Act to projects related to addressing the national response and recovery to COVID-19. This push has stemmed from a desire to increase the strength of the American industrial base and improve U.S. manufacturing capabilities, so as to prevent American reliance on a potential foe, like China, from forming during a national crisis.[193]

In October 2020, the United States announced the creation of the Abraham Fund, a program where the DFC, the United Arab Emirates, and Israel will promote $3 billion in private-sector and development projects. The initiative builds off the Abraham Accords, where the United Arab Emirates and Bahrain each agreed to normalize relations with Israel. Funding opportunities like this have the dual benefit of fostering diplomatic and economic growth between America's regional partners as well as edging out competing Chinese investment in critical sectors like infrastructure and energy security.[194]

vi. Blue Dot Network

As one of several focused projects under the DFC umbrella, Blue Dot Network (BDN) is a global infrastructure initiative undertaken by the United States, Japan, and Australia in November 2019 that aims to certify "quality infrastructure" projects that satisfy a host of metrics related to transparency, environmental consciousness, and developmental impact.[195] Envisioned as a more competitive, higher quality source of funding than that put forth by Beijing, the BDN is nonetheless more constrained by political and economic factors than its state-funded Chinese analog, the BRI, which has a less transparent, less sustainable, and less financially conservative approach to investment.[196]

The objective of BDN is to harness the investment appetite of U.S. pension funds and insurance companies and direct it towards not only addressing the global demand for infrastructure but also countering Chinese geopolitical influence in developing economies.[197]

With the rigorous certification standards put in place by BDN, it's possible—though quite ambitious—that infrastructure may become a full-fledged asset class, though much will depend on convincing private investors that such investments are worth the risk.[198]

vii. Defense Advanced Research Projects Agency (DARPA)

The Defense Advanced Research Projects Agency was created to encourage the advancement of science and technology and safeguard America's qualitative edge in the defense sector.[199] Established in 1958, DARPA is within the Department of Defense and is responsible for "research and development (R&D) that is intended to achieve transformative change rather than incremental advances"—for instance, through "notable commercial products and technologies such as the internet, global positioning system (GPS), automated voice recognition, and personal electronics."[200] DARPA does not directly conduct R&D but contracts with R&D firms, such as universities and private industries, offering an alternative method of financing for companies that might otherwise rely on other foreign investors or governments, like China, to expand their R&D efforts.

In 2018, the Pentagon announced that it planned to spend $2 billion over the next five years for DARPA to examine how artificial intelligence could be added to weaponry.[201] In 2019, DARPA's R&D was performed 65.5 percent ($2.3 billion) by industry; 17.4 percent ($615.6 million) by universities and colleges; 9.5 percent ($334.6 million) by intramural R&D performers, such as federal laboratories; 3.4 percent ($121.8 million) by other nonprofits, 3.3 percent ($115.2 million) by Federally Funded Research and Development Centers (FFRDC); and 1 percent ($34.7 million) by foreign entities.[202]

viii. Combating Terrorism Technical Support Office (CTTSO)

While DARPA examines long-term projects with end products five or more years down the road, the Combating Terrorism Technical Support Office (CTTSO) focuses on prototypes that can be used on the field in as few as two years. Like DARPA, CTTSO helps to meet DOD's need for cutting edge technology within the defense sector and offers an alternative source of funding for such efforts in order to prevent companies from turning to less savory investors.[203] In 2018, Adam Tarsi, a DoD official in CTTSO, spoke at the Combating Terrorism Technology Startup Conference at Tel Aviv University, where he announced U.S. funding for the winning ($100,000) and runner up ($10,000) firms. According to Tarsi, CTTSO has worked with Israel for years and the country is one of America's "chief partners" along with the United Kingdom, Canada, Australia, and Singapore.[204] Asked about Israel's Mossad investing in start-ups that could build innovations faster than American government or private sector counterparts, Tarsi said he was "not concerned at all" because "we are all rowing in the same direction. If there is an innovation that can benefit us, it will be shared with us."[205]

ix. Department of Defense Supply Chain Security Initiatives

Provisions within the National Defense Authorization Act (NDAA) of 2019 encourage safer investment practices on the part of companies by restricting the usage of telecommunications equipment or services produced by certain Chinese companies. In particular, Section 889(a)(1) of the NDAA of 2019 stated that the federal government may not:

(A) procure or obtain or extend or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system; or

(B) enter into a contract (or extend or renew a contract) with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.[206]

The act defined "covered telecommunications equipment" as being produced by Huawei, ZTE, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, any of their subsidiaries, "telecommunications or video surveillance services provided by such entities or using such equipment," or other firms that senior administration officials identify. This extended an interim rule that required the federal government and contractors to reconfigure supply chains to exclude certain Chinese companies like Huawei and ZTE. Contractors must annually submit to the government whether their supply chains include covered equipment or services.

In August 2020, data analytics firm Govini issued a report arguing that DoD's IT supply chains have dozens of Chinese companies in them, although it did not specify which companies are still part of DoDs supply chain.[207] According to Govini, China-based companies have the greatest share of the supplier base in "Telecommunications Equipment (20 percent) and Specialty Chemicals (17 percent), and have over 10 percent of the supplier base in nine other critical industries and in the Semiconductors industry, the number of China-based companies has grown 364 percent between 2010 and 2019, to 65 companies, increasing China's share to 13 percent from seven percent; the share of U.S. companies (144 in 2019) dropped to 28 percent from 56 percent due to a surge of other foreign suppliers."[208] Section 889 uses broad language that "could imply the government would be prohibited from doing business with a government contractor that has an internet service provider (ISP) that uses Huawei/ZTE equipment in providing internet service. An even more extreme example has been raised for contractors that use security cameras (even if only used in non-U.S. locations) that contain Huawei/ZTE components."[209]

x. America Labor, Economic competitiveness, Alliances, Democracy and Security (America LEADS) Act

Introduced in September 2020, the America Labor, Economic competitiveness, Alliances, Democracy, and Security (America LEADS) Act is a $350 billion plan to counter China that includes investing in U.S. industrial capacity. The legislation emphasizes the importance of U.S. science and technology providing $300 billion to R&D in these fields over four years and roughly $16 billion in the U.S. semiconductor industry.[210] With a core tenet of the plan being a desire to "support American alliances and partners," Israel is a natural fit for joint R&D efforts.[211] Additional funding, sponsorship, and project guidance for joint efforts between American and Israeli researchers and institutions would foster technological and scientific growth that would benefit the U.S. commercial and military innovation base, but also that of its most important partner in the Middle East, which faces similar threats from loss of intellectual property to China. Both countries should also examine their visa systems, academic requirements, and

job market priorities to allow more Chinese researchers who are already in the country to stay instead of returning to China.

xi. U.S.-Israel Joint Economic Development Group (JEDG)

Since 1985, the U.S.-Israel Joint Economic Development Group (JEDG) has met annually to discuss both countries' economies and reforms that Israel could take. At that time, Israel's economy faced high inflation, government budget deficits, and slow growth. JEDG helped reinvigorate the Israeli economy, fostering the "start-up nation" technological boom that Israel experienced in the 1990s and continues today.

The U.S. Treasury Department, U.S. State Department, and the Israeli Ministry of Finance have used JEDG to negotiate a memorandum of understanding that extends the 2003 U.S. pledge to provide $9 billion in loan guarantees to Israel.[212] When the more than 80 officials from both governments met in October 2019, U.S. Treasury Under Secretary for International Affairs Brent McIntosh praised the importance of JEDG "to expand cooperation and help accelerate growth in both our economies." Likewise, Director General of the Israeli Finance Ministry Shai Babad observed that "cooperation on the government level enables private sector firms to operate jointly through the establishment of R&D centers by U.S. multinationals and allows Israeli companies to expand to U.S. markets."[213] The Treasury Department's statement on the meeting says that the two sides discussed "risk management for foreign investments," among other issues, but Eran Nitzan, Israel's economic attaché in Washington, declined to comment if that meant Chinese investment.[214] The threats that Chinese investment poses to Israeli and U.S. national security should be a priority for future JEDG meetings. American officials should use the forum as an opportunity to develop a shared understanding of the problem Beijing poses and facilitate high-level talks on steps Jerusalem could take to alleviate U.S. national security concerns about Chinese investment in Israel.

VIII. Recommendations

China's comprehensive and systematic effort to penetrate, exploit, and subvert the open international economic order must be met by an equally determined and thorough response by democratic nations. The United States has begun disconnecting not only from Chinese controlled networks but also networks the Chinese are connected to. It is asking its allies, particularly Israel, to do the same. To date, Israeli efforts have not evinced an appreciation of the extent of the Chinese threat or of the seriousness of the U.S. request. Washington, on the other hand, has tended to fixate on individual Chinese projects without providing Israel enough guidance on how to enact the far-reaching legal and institutional reforms it is asking for. The United States also has failed to show both sufficient recognition of the challenge of finding substitutes for dangerous Chinese investments and a willingness to help its partner overcome that obstacle.

To protect themselves and each other from Chinese predations, the United States and Israel both need to make concrete efforts to address this challenge together. But perhaps most importantly of all, they also must take action together to build a new economic coalition that replaces the dependencies that China uses to weaken the international order. By taking the threat seriously, reforming its investment review and export control regimes, and harnessing its innovative private sector to the challenge of replacing China, Israel can secure its prosperity, draw even closer to the United States, and establish itself as a founding member of a new 21st century strategic alliance. In return, the United States needs to make clear to Israel that the United States will provide it with technical and economic assistance in making these difficult changes and reward it with an enhanced strategic partnership.

A. Recommendations for Israel

Israel has made progress in strengthening its protections against economic exploitation, especially with regard to foreign investment review. Yet, even these updated protections are likely insufficient against the Chinese threat. A more coordinated, comprehensive, and systematized legal regime is needed in Israel to identify sensitive infrastructure and technology, review inbound foreign investments, and control outbound exports. Such an approach will require a whole-of-government strategy that spans a variety of sectors. Each recommendation is discussed in further detail below.

i. Conduct Intelligence Review of Chinese activities in Israel

Israel should conduct an intelligence review of all Chinese activity and security risks, making economic penetration, investment in critical infrastructure, IP theft, and misappropriation of dual-use technology the center-piece of that review. Israel's military, intelligence, and financial agencies should conduct and issue unclassified and classified assessments of Chinese misappropriation of Israeli IP and technology. To better inform these reports, Israel should request intelligence sharing from and coordinate with relevant U.S. intelligence agencies. For example, the U.S. Defense Innovation Unit Experimental (DIUx) and Office of the U.S. Trade Representative have produced extensive investigations into Chinese policies and practices that harm U.S. companies and threaten national security.[215] The findings of these studies have provided the evidence of Chinese economic predation that helped shape the current U.S. focus on this threat.

Similarly, the Israeli government should publish as much information as possible in unclassified reports and limit delaying declassification. The Israel Defense Forces also have a uniquely high-level of public trust within Israel, allowing it to provide a security-focused and non-political explanation of the risks Beijing and Chinese investment poses. Likewise, tracking and revealing malicious actors and their methods, as Mandiant did with Unit 61398, improves public awareness and best practices.[216] Some information will understandably need to remain classified. Israeli agencies should distribute these classified findings to as many agencies and political leaders as Israeli law allows. Ministers and members of the Knesset overseeing relevant agencies should have regular briefings that include classified material.

ii. Focus Counterintelligence Resources on Infiltration of Israeli Academia

In addition to reviewing possible foreign misappropriation of Israeli technology, Israel should employ counterintelligence operations to examine possible foreign infiltration of Israeli academia. Academia provides a rich environment for the theft of incredibly valuable intellectual property, and Israel's academic climate is no exception. Every year, roughly 1,000 Chinese students, mostly in the STEM disciplines, opt to study in Israel. More rigorous evaluations should be conducted of the backgrounds and academic activities of such students while on Israeli campuses. Screening should evaluate incoming students for ties to the Chinese Communist Party; People's Liberation Army; and officials, organizations, or research institutions connected to the Chinese state and security agencies. Yet, it is impractical for any screening process to prevent academic infiltration entirely, so Israeli officials should educate Israeli academia about the warning signs for espionage and how to report concerns.

iii. Systematize Protocol for Screening Inbound Investment

Although Israel has made progress toward creating a CFIUS-like mechanism for reviewing foreign investments, the current framework remains patchy and ad hoc. In order to confront comprehensive and systematic Chinese economic penetration, Israel must create a regular and stringent process for screening investments coming into the country from abroad.

That being said, not all regimes are created equal. The foreign investment review system put into place by the EU, for example, falls woefully short of representing anything close to an actual mechanism of review. Israel would be wise to reject the informal, overly flexible approach taken by the EU. Conversely, Germany and Australia offer alternative methodologies that vary in their comprehensiveness and scope and may provide insight into possible ways Israel could structure its own regime.

Australia has been a trailblazer in terms of actively reforming its review processes to meet the ever-evolving threats posed by foreign investments (Section C.ii of the Appendix details various provisions of Australia's recent *Foreign Investment Reform Bill 2020* that crystallize these reforms). Yet, while Australia is a global leader in the review of foreign investments, the gold standard for both robustness and efficacy remains unequivocally CFIUS. Thus, this report details specific lessons learned and best practices gleaned from the U.S. model that Israel should adopt to adequately protect itself and to potentially emerge as a leader within this growing realm of national security.

a. Centralize the Review Process

Any proposal for reviewing foreign investments should shield against breakdowns in communication and encourage interactions between the branches of government possibly implicated by a given transaction. For instance, when the Transportation Ministry accepted the bid of Shanghai Port Group—a major Chinese investor—to invest in Haifa Port in 2015, it became a point of controversy as later details revealed that Israel's security forces had not been consulted prior to the bid being accepted. Thus, any foreign investment oversight mechanism must require heightened communication between the ministries most intimately associated with national security affairs.

b. Investment Review Should Not Be Exclusively Voluntary

An oversight regime that has a voluntary component should not be *exclusively* voluntary; otherwise, the oversight is left to the mercy of those conducting the transactions and anticipates a great deal of good faith that may not always be present. As discussed above, the CFIUS/FIRRMA regime allows not only for parties to a proposed transaction to voluntarily submit a proposed transaction for CFIUS review but also for CFIUS itself to initiate review if it believes a proposed transaction may pose a security risk. This hybrid model would strike the right balance of allowing for robust review without chilling foreign investment, which has been a chief concern of those within both the upper echelons of the Israeli government and the Israeli business community.

c. Include Mandatory Review in Certain Instances

The degree to which Israel makes review of transactions mandatory likely will be a source of debate. As discussed above, Israel similarly could establish particular parameters that necessitate review. Possible objective factors to consider applying as a review "trigger" might include: the percentage stake being acquired by the foreign investor, the industry in which the transaction is occurring, the investor's country of origin, and the role of the foreign government, if at all, in the transaction.

d. Allow Post-Hoc Review of Investments

If the committee intends to have a voluntary component prominent in its review mechanism, one way to incentivize parties to seek review prior to conducting a transaction is to grant the committee the authority to conduct post-hoc reviews of foreign investments. The indefinite threat of potential review in the future likely would compel investors to seek approval before concluding the transaction in order to avoid the possible pitfalls of concluding a transaction, only to have the committee nullify it in the future. Granting the committee the power to conduct post-hoc review will allow the voluntary component to be far more effective at actually capturing transactions of interest, sparing the committee the additional effort of having to "catch" every transaction in need of review.

e. Create Financial Intelligence Capability

In order to locate non-notified transactions—transactions that were not voluntarily reported by the parties—and non-declared transactions—transactions that required reporting but went unreported—CFIUS has an Office of Investment Security Monitoring & Enforcement whose sole

it is to monitor, oversee, and enforce the United States' foreign investment screening regime. For a mixed system of voluntary and mandatory reporting to be effective, there must be a financial intelligence arm to investigate potential transactions to ensure they comply with the committee's regulatory scheme.

f. Include the High-Tech Sector

Notably absent from this list of sectors is the technology sector, which has been a magnet for foreign—particularly, Chinese—investment. Between 2011 and 2018, Chinese direct investment into Israeli tech totaled $5.7bn, according to RAND, with investment into the tech sector dwarfing Chinese investment into any other Israeli sector. Israeli venture capital firms also serve as a draw for Chinese investment and pose an additional risk, since many of their portfolios tend to be technology or biotechnology heavy.[217] Thus, the committee mandate should undoubtedly include the technology sector if it is to effectively target one of the most popular—and riskiest—sectors for Chinese investment.

g. Review Both Controlling and Noncontrolling Investments.

While noncontrolling investments inherently pose a reduced risk from a national security standpoint, some should still be subjected to governmental scrutiny. It would be beneficial for the Israeli committee to apply similar scrutiny to noncontrolling investments, given the risks are not merely operational-based but also access-based in terms of the material that investors may be granted exposure to.

h. Subject Transactions Involving Foreign Governments to Heightened Scrutiny

Regardless of the thresholds that the Committee may or may not establish, all transactions involving a foreign government investor should be subjected to review. In instances like China, where the distinction between public and private entities has effectively collapsed, it may mean that the vast majority of transactions are subjected to review by the committee. Defining what constitutes a "foreign government investor" will be a matter of discussion for those forming the committee, as many foreign governments may passively hold foreign funds without engaging directly with the funds themselves.

i. Create a Lengthier Timeframe for Review

The Israeli committee should not feel tethered to establishing short timeframes of review that would thereby limit its ability to conduct exceptionally thorough reviews. One flaw of EU 2019/452—and of the previous Australian regime—is that the review windows hover (or formerly hovered) around 30 to 45 days, which given the breadth of transactions, is far too limited. While investors should be able to reasonably anticipate when their review will be completed, giving only one month to review often complex transactions is insufficient, as shown by both the Australian model and the CFIUS/FIRRMA regime.

iv. Strengthen Israeli Unilateral Export Controls

Compared to its foreign investment review process, Israel's export controls on dual-use technology are much stronger. Still, it also requires updating to meet the critical task of

continually assessing and responding to the risks posed by new and emerging dual-use technologies.

a. More Nuanced and Modernized Definitions

Generally speaking, the Israeli export control regime is young and, at times, lacks the nuance needed to carry out effective oversight that is robust, yet not suffocatingly restrictive to industry. Such inefficiency is evidenced by the following example: the Ministry of Defense is tasked with controlling any unmanned aerial vehicle (UAV), even the ones sold as children's toys.[218] This practice is a "vestige" of a time when UAVs were strictly military in nature, but the definition of what constitutes a UAV has not been modified to reflect such advancements.[219] Therefore, an effective export control regime may require the creation of an advisory committee to review and assess the lists currently being employed by Israel's various ministries to ensure that they are not simultaneously "overcontrolling" and "undercontrolling" exports based on imprecise definitions.

b. Incorporate More Risk-Based Assessments

The Israeli government also tends to blindly adopt control lists assembled by the multilateral regimes without giving much consideration to how those lists might interact with Israeli imports, often using such lists as a substitute for risk-based assessments that may be more effective at targeting potentially harmful exports.[220] For instance, placing increased controls on exports to certain countries, such as China, might be a smarter exercise than treating exports to all countries as equally risky. Indeed, a drone exported to China may very well be used to violate certain privacy rights, whereas a drone exported to Canada may not. The Israeli export control regime would likely benefit from establishing a "country of special interest" category, analogous to the one created under CFIUS/FIRRMA, in order to assess the possibility of increased risk resulting from the geographical destination of a given export.

v. Join Relevant Multilateral Export Control Agreements

Israel is not a member of any of the four multilateral export control regimes discussed above, and ideally, the United States should continue to encourage Israel to join—in the very least—the Wassenaar Arrangement, the Australia Group, and the Missile Technology Control Regime. In the case that Israel refuses to do so (a likely outcome given its past behavior), the U.S. government has several possible options at its disposal.

First and foremost, despite rejecting membership, Israel does track a great deal of its unilateral export control regime to the lists of controlled items assembled by the four regimes. With regards to the Wassenaar Arrangement in particular, Israel is not a member, but it does enjoy close collaboration with the regime, recently hosting a delegation from the Wassenaar Arrangement in November of 2019 where an in-depth exchange of information and best practices took place.[221] In terms of biological and nuclear weapons, though Israel is not a member of the Australia Group or the Nuclear Suppliers Group, it has established certain export controls for dual-use biotechnologies, as well as nuclear technologies and equipment, as evidenced by the *Import and Export Order (Control of Chemical, Biological, and Nuclear Exports), 5764-2004*.[222] Lastly, Israel is not a member of the Missile Technology Control Regime, but has pledged to abide by the regime and does use the regime's lists to heavily guide and inform its own.

The neighborhood in which Israel operates makes discretion with regards to its military programs absolutely essential, and such need for discretion explains much of Israel's decision to refrain from joining any of the multilateral export control regimes. Therefore, the United States should continue to encourage this cooperation. In addition, Israel should formally communicate to U.S. officials what it finds important in the agreements and reasons it has not yet joined them. Joining the multilateral export control agreements is the best long-term solution, but reaching this outcome will require significant dialogue and time.

In exchange for Israel continuing its informal commitments to the various regimes, the United States could consider offering one year of STA-1 status, subject to formal review each year based on Israel's performance. The United States could also use those systematic reviews to engage in substantive dialogue with the Israeli government and communicate more concretely and precisely which items it believes should be subject to more aggressive oversight.

B. Recommendations for the United States

While Israel has much work to do to strengthen and institutionalize protections against Chinese economic penetration, the United States should be willing to do more to provide its partner with guidance, expertise, and incentives to make these difficult changes. Perhaps even more importantly, the United States must signal to Israel that the benefits of excluding dangerous Chinese economic activity will be strategic as well as financial. Taking steps now to strengthen the U.S.-Israeli security relationship, while remaining frank about the obstacles that failure to address Chinese economic penetration would create for continued cooperation, can help reassure and encourage Israeli leaders.

i. Upgrade Israeli-U.S. Intelligence Sharing

The United States and Israel already share a great deal of intelligence, but there are roadblocks to improving the relationship. The "Five Eyes" agreement between the United States, the United Kingdom, Canada, Australia, and New Zealand enables these countries to fully cooperate on signals intelligence and otherwise closely guarded intelligence matters. There are diplomatic obstacles to Israel joining this group, just as there are for U.S. allies like Germany, South Korea, and Japan. However, as a previous JINSA report recommended, there is nothing stopping the U.S. president from releasing pertinent American intelligence to Israel that it also shares with "Five Eyes" nations.[223] Exchanging this information would help bridge the knowledge gap between Washington and Jerusalem about the national security risks that China poses. A greater understanding of the U.S. threat perception will better inform the Israeli decision-making process and potentially sidestep public disputes such as those that have occurred since Israel awarded a Chinese company a tender to operate a terminal at the Haifa Port. Improved intelligence sharing can also help Israeli investment oversight and export regulations stay up to date with the innovative dual-use technologies that China pursues.

ii. Provide Information on Best Practices

The most beneficial assistance that the United States can provide is to offer information on best practices when it comes to screening foreign investments. The screening process for outbound and inbound investments in the United States is one of the most rigorous in the world. Even if the Israeli government does not opt to adopt such stringent mechanisms, there is undoubtedly

much to be gleaned from the United States' experience with investment oversight. Many recommendations discussed above are drawn from both the shortcomings and successes of the CFIUS/FIRRMA regime.

iii. Acknowledge the Economic Benefit of Foreign Investment

An important element to consider when encouraging the Israeli government to adopt more stringent oversight mechanisms is to recognize the strength of the economic considerations that are being balanced against any oversight regime. There's a strong argument to be made that a regime as robust as the CFIUS/FIRRMA is a luxury of the United States' $19 trillion-dollar economy, where the rejection of an even remotely risky investments does not hamper economic growth in any meaningful way. This scenario may not be true in Israel, where the business community has been particularly wary of the Israeli government's appetite for oversight, and likewise, the government has been cautious about any regime that might result in the significant chilling of valuable foreign investments. Therefore, any discussions regarding Israel's adoption of an oversight regime must maintain intellectual honesty by giving credence to the differences in the size of the Israeli and U.S. economy—and how reliance on foreign investment may be determined by such a factor.

iv. Expand U.S. and International Financing for Projects in Israel

The U.S. International Development Finance Corporation (DFC) is a new institution that could counter China's Belt and Road Initiative (BRI) by providing alternative funding with better transparency. Given Beijing's head start on BRI spending and ability to control how Chinese companies invest abroad, the DFC requires a large increase in the amount of funds it can invest abroad. Congress should also appropriate projects specifically for sectors susceptible to harmful Chinese investment, such as dual-use technology. Washington should also encourage its other partners, especially Japan, Taiwan, India, and the European Union, to invest in Israel, potentially pursuing a common fund for developed democracies from which to invest in emerging technologies vital to preserving the competitiveness, and security, of open political and economy systems.

v. Enable U.S. Government Investment in Israeli Technology Sector

Appropriations for joint programs between American and Israeli R&D could increase both countries' technological development and center innovative thinking around a shared understanding of existing and future problems. Agencies like the Combating Terrorism Technical Support Office (CTTSO) should continue successful investments in Israeli technology, and Congress should appropriate funds for other national security agencies to make similar investments that would benefit concerns beyond counterterrorism. Approximately 97 percent of DoD's Research, Development, Test, and Evaluation (RDT&E) funding is appropriated through Title IV (Research, Development, Test, and Evaluation), which includes appropriations for the Army, Navy, Air Force, Space Force, a Defense-wide account, and the Director of Operational Test and Evaluation. The Defense-wide account includes appropriations for the Office of the Secretary of Defense, Defense Advanced Research Projects Agency (DARPA), Missile Defense Agency (MDA), and fifteen other DoD organizations.[224] Congress should authorize and appropriate specific funds for the U.S. national security community to invest in Israeli companies that would help achieve these agencies' missions.

Likewise, Congress could require the executive branch to construct new systems of cooperation between American and Israeli research and design efforts in the defense sector. Section 1299M of the FY 2021 National Defense Authorization Act authorizes the Secretary of Defense to establish a United States-Israel Operations-Technology Working Group for researching, developing, and fielding technologies and capabilities that could benefit both countries. The administration should quickly establish this working group so that it can begin building both countries' defense innovation bases.[225]

vi. Open Trusted Capital Program to Allied and Partner Countries

The Pentagon should explore opening its Trusted Capital Program to allied and partner countries. Designating foreign capital markets, finance entities, and companies that the Pentagon determines are free from influence of actors like China, Russia, and Iran could expedite business with American defense contractors and the U.S. government. These "whitelisted" entities would benefit from access to U.S. capital and encourage their competition to follow suit.

vii. Provide Clear Requirements for and Assurance of Granting Strategic Trade Authorization

Given Israel's valid concerns over joining the various multilateral export control regimes, it may be difficult to hinge Strategic Trade Authorization (STA) status on Israel's membership in all four regimes, as is the traditional requirement for such status. However, the United States may be able to grant an exemption to Israel, bestowing STA status in exchange for Israel agreeing to establish (1) a foreign inbound investment oversight committee that is more than advisory in nature and (2) an advisory committee to routinely review Israel's export control lists.

Exemptions within the realm of STA statuses are not unheard of. India was granted STA-1 status, despite its unwillingness to join the Nuclear Suppliers Group, and it's worth recalling that Israel largely adheres to most of the multilateral export regimes unofficially. The United States could hinge such exemptions on this continued commitment to these regimes, as well as on Israel's continued information sharing with certain regimes, such as the Wassenaar Arrangement.

viii. Frontload Memorandum of Understanding Funds

In 2016, the United States agreed to provide $33 billion in foreign military financing (FMF) and an additional $5 million in missile defense to Israel over a ten-year period. This memorandum of understanding (MOU) is the centerpiece of America's commitment to ensuring Israel's qualitative military edge (QME), which ensures Israel's ability to defend itself by itself against any of its neighbors. Currently, Israel receives funding in even yearly increments. However, frontloading, or providing more of the MOU's total $38 billion earlier in the ten-year cycle, would allow Israel to purchase much-needed American-made weaponry without raising the cost to the U.S. taxpayer.[226] Ensuring Israel has advanced capabilities earlier will help counter China's proliferation of weaponry and dual-use technology to adversaries like Iran.

C. Recommendations for Both Partners

Even as Israel is taking steps to strengthen its economic defenses—and the United States to assist it—more will be required. One of the larger risks associated with greater scrutiny of Chinese economic activity is the possibility of economic losses resulting from the exclusion, and possible chilling, of Chinese investment. The United States enjoys the luxury of the world's largest economy and, as a result, the ability to better hedge against any economic risks. Meanwhile, Israel's economy is a fraction of the size, making it much riskier for Israel to embrace a stringent CFIUS-like regime and comprehensive dual-use export controls. Thus, protecting against Chinese economic predation will not work without a strategy to develop the economic and technological capabilities to supplant China.

Solving the substitute problem is not just a challenge for the United States and Israel, but for all democratic countries that Washington hopes to persuade to join its cause. But the United States and Israel are uniquely capable of laying the foundations for a new economic order and strategic alliance of democracies, one that will serve as a model and inducement for other countries to join. Some of the most important steps that can be taken against China should, therefore, be taken together by Washington and Israel with the goal of building a durable, democratic economic coalition.

i. Negotiate and Sign a Robust Bilateral Investment Treaty

While Israel already enjoys favorable treatment within the trade realm as a result of the liberalizing mechanisms of the U.S.-Israeli FTA, it does not share a bilateral investment treaty with the United States that might otherwise promote foreign investment between the two nations. Doing so would establish increased levels of certainty during a period where heightened regulations on foreign investments into Israel might have a chilling effect.[227] The 2017 Israel-Japan bilateral investment treaty (BIT) provides a model for what an agreement with a particular schedule of exceptions might look like.[228]

This could be accomplished through a standalone agreement or as part of an updated U.S.-Israeli FTA (see below).

ii. Update the Current U.S.-Israeli Free Trade Agreement

The United States and Israel should modernize their FTA to account for the loss of possible foreign investments they might suffer by making their oversight regimes more robust. An updated FTA would have the dual benefit of reducing Israeli apprehensions about trade reforms while also strengthening the U.S.-Israel bilateral relationship. An improved FTA that addresses areas of concern, like dual-use technology and AI, alongside stricter Israeli economic oversight in these same areas would address the substitute problem by excluding malign Chinese investment and incentivizing U.S.-Israeli economic development.

The United States-Mexico-Canada-Agreement (USMCA), the revised version of which was concluded in 2019, is one of the more recent FTAs to be entered into by the United States and may offer a roadmap for enhancing the level of cooperation afforded by the U.S.-Israeli FTA.[229] Possible chapters from the USMCA that may be borrowed and incorporated into the U.S.-Israeli FTA are discussed in further detail below.

a. Digital Trade Chapter

The USCMA is unique in that it is the first FTA concluded by the United States to include digital economy provisions, including ones that explicitly protect emerging technologies, thus cultivating an environment more hospitable to lucrative innovation.[230]

Chapter 19 of the USCMA[231] outlines provisions that ban customs duties on digital products and prohibit countries from demanding the disclosure not only of source code but of "algorithms expressed in that source code."[232] Required disclosure is permitted only in instances where it is necessitated by a regulatory body or judicial authority for a "specific investigation, inspection, examination enforcement action or proceeding."[233] Furthermore, and perhaps most importantly, Chapter 19 also prohibits data localization, meaning countries are barred from requiring foreign companies to construct or lease separate data infrastructures within the domestic country (often an expensive venture).[234] Data localization is frequently cited as one of the greatest barriers to facilitating global services through its protectionism-based measures.

b. Intellectual Property Chapter

Chapter 20 of the USMCA represents an attempt by the United States and its fellow trade partners to increase intellectual property protections to a degree that reflects modern technological advancement. While intellectual property laws may superficially appear to stifle exchange, they substantively work to incentivize innovation and exchange between trade partners, as millions of jobs are dependent upon protecting the integrity of patents, copyrights, and trademarks.[235] Protecting IP rights benefits both users and producers.

Among the IP provisions in the USMCA are the removal of certain administrative barriers, thus allowing for easier trademark protection; enhanced protections for non-traditional trademarks, such as geographical indicators; and criminal procedures and penalties for IP theft.[236] Regardless of what form IP protections might take within the U.S.-Israeli FTA, codifying them in a meaningful manner that reflects the current technological climate would be unequivocally beneficial for both parties.

c. Increase Protections for Small and Medium-Sized Enterprises

Given Israel is often regarded as the "start-up nation," granting increased market access to smaller economic actors offers an undeniable advantage to Israeli small and medium-sized enterprises (SMEs) hoping to compete in the U.S. market. Below are several USMCA chapters that offer benefits to smaller enterprises, concretizing some possible initiatives that both partners might consider incorporating into the FTA. Including provisions of this nature in an updated U.S.-Israeli FTA would signal a heightened interest in promoting economic development in each respective member state through supporting the development of non-traditional actors that nonetheless play a valuable role in their respective economies.

1) Rules of Origin Chapter

The USMCA is novel in that it raises the *de minimis* requirements previously observed in NAFTA. Chapter 4 of the USMCA reduces overall costs to SMEs of conducting cross-border transactions by increasing the size of transaction at which customs and duties are triggered,

meaning compliance costs for smaller exporters are significantly decreased.[237] The United States might consider raising the current *de minimis* requirement for Israel, which currently stands at $500 USD.

2) Cross-Border Trade in Services Chapter

There are several ways to promote enhanced cross-border trade in services between the United States and Israel. The reasoning behind doing so is simple—for advanced economies, the portion of trade that consists of services has increased dramatically, and thus, the regulation of trade in services is an area ripe for economic impact.[238]

One option would be to adopt a chapter similar to that presented in the USMCA. Chapter 15 of the USMCA increases market access for smaller exporters by permitting SMEs to conduct business across borders without opening an office within the foreign state. The chapter also includes a provision that compels each party "to support the development of SME trade in services and SME-enabling business models, such as direct selling services, including through measures that facilitate SME access to resources or protect individuals from fraudulent practices."[239]

Another option would be to assume a strictly multilateral approach. A separate Trade in Services Agreement (TISA), consisting of 23 parties, including the EU, the United States, and Israel, was proposed in 2013, but saw little to no movement during the Trump Administration.[240] If seeking an alternative to the bilateral avenue of the U.S.-Israeli FTA, the Biden Administration might consider reinitiating negotiations with the parties previously involved as a means of not only expanding the benefits of such an arrangement across multiple actors but also of promoting a more multilateral international agenda on the whole.[241]

Finally, the third approach would involve combining both mechanisms. A TISA, such as the one described above, could be concluded and then complemented by including an additional chapter in the U.S.-Israeli FTA that assigns special, specific rules to the U.S.-Israeli relationship.[242] The details of this *lex specialis* would be a task for the United States Trade Representative.

3) Small and Medium-Sized Enterprises Chapter

Chapter 25 of the USMCA represents a concerted effort to encourage the proliferation and growth of SMEs across member states, as the USCMA is the first FTA to include a chapter that focuses exclusively on smaller exporters.[243] Chapter 25 establishes mechanisms for assisting SMEs in cross-border transactions and for encouraging further trade and investment opportunities for SMEs. More concretely, Chapter 25 creates a permanent committee to oversee SME affairs and establishes a platform for increased exchange between private SMEs.[244] Given the increased risk the lockdowns from coronavirus pose to small businesses, the implementation of such mechanisms likely would be highly welcome.

d. Taxation of Foreign Investment

Another possible approach would be to include a chapter within the U.S.-Israeli FTA that offers tax incentives for U.S. private equity investment into the Israeli technology sector.[245] Doing so would be a boon for a Biden Administration eager to steer U.S. capital away from Chinese markets, thus offering a positive enforcement mechanism for both parties.[246]

iii.Create U.S.-Israel Joint Economic Working Group Select Committee on Technology Control

In order to improve both Israel's export controls and those of the United States, Israel and the United States should develop a committee devoted to the sharing of technological developments as they relate to each country's respective export control regime. This committee could be analogous to the United States-Israel Operations-Technology Working Group, except instead of focusing on improving defense technologies shared by the two countries, it would focus more generally on technological developments and reflecting such developments within the two countries' export control regimes. Unlike the United States-Israel Operations-Technology Working Group, which would remain under the auspices of the U.S. Department of Defense, this committee would be formed in conjunction with the U.S. Department of Commerce, which specifically monitors U.S. exports and the ever-evolving definition of what constitutes "dual-use" technology. Thus, this committee would help to fine-tune each country's approach to dual-use technology and export controls through comprehensive and regular information sharing.

Furthermore, to facilitate a shared understanding of both countries' threat perceptions and alleviate any apprehension Jerusalem has about joining multilateral export regimes, the American and Israeli military and intelligence establishments should issue official annual reports made available to each other that represent their separate assessment of concerns, obstacles, limitations, and possible paths to joining the export regimes. The committee should regularly meet to discuss both gaps in these assessments and ways to improve existing export controls and to craft steps Israel could take to satisfy any remaining U.S. concerns, including ways to monitor Chinese capital within the technology sector.

iv. Explore a Multinational Trusted Capital Program

Instead of accepting foreign firms into its Trusted Capital Program (TCP), the Pentagon could also pursue a similar multinational program connected to or distinct from its domestic initiative. Such a system of "whitelisted" multinational capital would create a competing defense innovation block that could rival China's expensive BRI. Individual countries could establish their own TCP that would have rules and requirements specific to that country and then coordinate among the various TCPs to facilitate capital flows. Encouraging TCPs in foreign countries would help protect their start-ups from predatory investments. Another option would be for the United States to facilitate the creation of a singular multinational TCP that met the Pentagon's requirements and would cover all countries involved.

v. Invest in Joint Scientific Training and Research & Development

In response to Chinese efforts to lure scientists from abroad, America and Israel should adopt policies that seek not only to maintain talent and intellectual property within their countries but also to prevent them from flowing to China.[247] American and Israeli research institutions have the ability to attract some of the world's most talented researchers without the U.S. government paying the salary of every professional on their campuses.

In Foreign Policy, research analyst Ryan Fedasiuk recommended that the U.S. government "the best way to improve America's resilience to Chinese talent plans is to create more

opportunities for experts who might otherwise be attracted to them" by increasing "federal funding for science and technology, sponsoring and streamlining visas for foreign scientists, and expanding—not canceling—the STEM Optional Training Program for recent PhD graduates."[248] Increased funding and opportunities for long-term research in the United States could attract Israeli and American scientists who would otherwise join China's Thousand Talents Program.

vi. Deepen Strategic Cooperation

China and Iran's potential $400 billion military and economic agreement underscores the growing threats that Israel faces. Both Beijing and Tehran are attempting to establish spheres of influence and deny their adversaries the ability to operate in those spaces. China is doing so in the Western Pacific with its island building projects and naval buildup, and Iran is building a land bridge across Syria and Lebanon. Building on the already close U.S.-Israeli security relationship will be important to addressing these joint threats. It will also be instrumental in convincing Israel that any economic sacrifices it makes at Washington's behest will be backed up with political and strategic commitments to Israel's security. Signing a mutual defense pact and pursuing joint R&D on emerging defense technologies will help cement this partnership.

Iran is attempting to proliferate rockets and advanced precision-guided munitions throughout the Middle East, including directly to Israel's north in Syria and Lebanon. As JINSA has previously recommended in two reports and a draft treaty, a mutual defense pact between the United States and Israel would "add an extra layer of deterrence to Israel's strategic position, and to America's position in the Middle East, and ultimately last line of defense."[249] Such a narrow treaty "would cover only a defined set of exceptional circumstances that would place either country in extreme peril."[250] A narrow defense treaty between the United States and Israel could lend the deterrence both countries need to counter China's growing support for Iranian aggression.

Meanwhile, close R&D partnerships on technologies like hypersonic cruise missiles and glide vehicles could help the United States and Israel quickly strike from far distances to defeat the access denial strategies being pursued by China and Iran.[251] For this same reason, Washington and Jerusalem should explore unmanned air (UAV), undersea (UUV) ground (UGV), and surface (USV) vehicles that can provide both intelligence, surveillance, and reconnaissance (ISR) capabilities in addition to offensive firepower. With these technologies extending the range of American and Israeli operations, China or Iran's capability to deny physical access to territory would pose less of a challenge.

Appendix: Foreign Investment Review Regimes

A. United States

i. CFIUS: The Formal Review Process

Formal review may be voluntary or mandatory. In the case of voluntary review, the parties to the transaction submit a short-form declaration, resulting in a lighter 30-day review period and the potential to be granted a "safe harbor" letter, which shields the transaction from later CFIUS review, except in certain circumstances.[252] Conversely, under the current FIRRMA regime, notice of the transaction is mandatory (1) for any foreign investment into a U.S. company that produces, designs, tests, manufactures, fabricates, or develops one of 27 "critical technologies," as defined by the North American Industry Classification, or (2) if a foreign government is acquiring a "substantial interest" in certain types of U.S. businesses.[253] "Substantial interest" is defined as a foreign government holding an interest of 49 percent or more—directly or indirectly—in the foreign entity seeking to acquire a U.S. company in a critical sector and a 25 percent or more interest—directly or indirectly—between the foreign entity and the U.S. company.[254]

However, the Treasury Department proposed a new regulation in May 2020 mandating notice if items produced by the U.S. business privy to the transaction normally would require regulatory authorization under the U.S. export control regime.[255] The foreign investors subject to this oversight mechanism are those who hold a 25 percent voting interest or more (direct or indirect) in the foreign buyer seeking to complete the transaction. The second modification proposed by the new regulation more precisely defines what constitutes "substantial interest" by fine-tuning the requirements triggering mandatory review.[256] Namely, in order for review to be mandatory, the "substantial interest" must be in the "general partner, managing member, or equivalent" who "primarily directs, controls, or coordinates" the activities of a given entity.[257]

The four export licensing regimes for controlled items (and thus, the reference point for mandatory CFIUS review) include a license from the State Department under the International Traffic in Arms Regulation (ITAR), a license from the Department of Commerce under the Export Administration Regulations, an authorization from the Department of Energy, and a license from the Nuclear Regulatory Commission.[258]

Under the new rules, certain licensing exceptions will prevail, including license exceptions for widely available technology (License Exception for Technology and Software Unrestricted), for certain encryption items (License Exception for Encryption Commodities, Software, and Technology), and for certain trade partners that have received Strategic Trade Authorization status (STA).[259]

The formal review process may span from one to three months. Following the receipt of a declaration with basic information, CFIUS has 45 days to conduct a risk assessment. If a risk with the transaction is identified and not resolved, CFIUS has 45 days to conduct a national security review.[260] This is a far more extensive process, which involves the consideration of 18

different specific factors, 12 factors[261] previously established by the Foreign Investment and National Security Act (FINSA) in 2007 and six additional ones added by FIRRMA in 2018.[262]

During the national security review, the Director of National Intelligence is also required to conduct a review of the transaction within 30 days, a process which may demand consultation with the Director of the Office of Foreign Assets Control and the Director of the Financial Crimes Enforcement Network.[263] Depending on what industry the investment is set to include, an agency is chosen to spearhead the national security review, at which point the parties may opt to withdraw and resubmit the notification of their transaction.[264] If during this process, it is discovered that the transaction harms U.S. national security, that the foreign person party to the transaction is controlled by a foreign government, or that the transaction would result in critical infrastructure being controlled by a foreign person, the transaction is subjected to a third period of review, known as a national security investigation.[265]

The national security investigation is permitted to take up to 60 days. During this time frame, the parties are given another chance to address any outstanding issues while CFIUS retains the authority to impose mitigating conditions on the transaction.[266] The "investigation" period may include the negotiation of a mitigation agreement, the establishment of short-term protections, or the creation of a system for tracking the commitments of the parties. The parties to the transaction may also get the chance to resubmit their notice.[267]

In certain instances, following the three stages, CFIUS may still be dissatisfied with the level of risk associated with the transaction and refer it to the U.S. president, who has 15 days to block the transaction. After referral, some parties choose to withdraw the transaction in order to avoid presidential scrutiny.[268]

ii. CFIUS: Usage of the Blocking Power

While the president maintains the authority to block a transaction, the review rarely reaches that stage, given the popularity of mitigation agreements and the propensity of parties to withdraw the transaction following feedback from CFIUS. Since the establishment of CFIUS, U.S. presidents have blocked six transactions, half of which were by President Trump.

In September 2017, the United States stopped Canyon Bridge Capital Partners, a Chinese investment firm, from acquiring Lattice Semiconductor Corp. in Portland, Oregon for $1.3 billion. The usage of the blocking power occurred after Reuters reported in November 2016 that Canyon Bridge was partially funded by the Chinese government and had indirect ties to China's space program. According to the U.S. Treasury Department, concerns were raised over the sharing of intellectual property, the relationship between the Chinese government and Canyon Bridge, and the possible threat posed to the integrity of U.S. semiconductor supply chains.

In 2018, Singapore-based firm Broadcom was prohibited from acquiring semiconductor chip manufacturer Qualcomm for $117 billion. Despite the company being based in Singapore, concerns were raised that the transaction might impact the United States' competitive edge against China in the technological space, particularly because of Broadcom's cost-cutting behaviors.

Most recently, an executive directive forced Beijing Shing Information Technology Co., Ltd., a Chinese firm, to sell off its ownership in Delaware-based StayNTouch, Inc, declaring that the 2018 acquisition of the U.S. hotel property management software presented a national security risk. The order did not provide details on the evidence buttressing the order; however, the order is likely representative of growing concerns over Chinese access to the personal data of millions of Americans.

iii. CFIUS: 2019 Performance Report

According to CFIUS's annual report released this past summer, CFIUS had 325 actions in 2019—more than in any other year.[269] It reviewed 231 joint voluntary notices (JVNs) and 94 declarations. Given that certain FIRRMA provisions expanding CFIUS's jurisdiction were not implemented until January 2020, the number of reviews conducted by CFIUS should only increase under the widened mandate.[270]

Of the 231 JVNs, 113 were elevated for further investigation following the initial review period. Thirty-three JVNs were assigned mitigation measures, and 28 were cleared following entrance into mitigation agreements. Thirty of the JVNs were withdrawn, and half were refiled in 2020. Of the 94 declarations, only 35 received approval, while 32 were notified that a full review could not be completed, and the remaining 26 (one was withdrawn) were told to file full JVNs.

Under FIRRMA, the initial review period was extended from 30 days to 45 days, which in turn made CFIUS more efficient, as 45 days proved to be more ample time for making a final determination and "sparing" the transaction from facing a second round of review. In 2019, more than half of the 231 JVNs were cleared after the initial stage of review, while in 2018 under one-third were cleared.[271]

It also seems that attempts by Congress and the president to mitigate Chinese investment have had an impact. The number of JVNs filed by Chinese investors fell from 60 in 2017 to just 25 in 2019, with three declarations. Despite these numbers, questions remain as to whether investors are simply opting not to engage in voluntary review out of fear of heightened scrutiny, or whether the investment environment has been made sufficiently hostile as to "crowd out" Chinese buyers.[272]

iv. Export Controls: Administrative Mechanisms for Defining Dual-Use Technologies

It is important to note that the process of identifying dual-use technologies is an ongoing endeavor, given their rapidly changing nature. Thus, Section 1758 of the ECA grants BIS the ability to lead an interagency effort to identify the "emerging" or "foundational" technologies "essential to national security" that must be subjected to export controls and added to the Export Administration Regulations (EAR) controls. Once such technologies are identified, BIS publishes a Final Rule labeling them.[273] More importantly, once such technologies are categorized as "emerging," their designation then makes them "critical" under the CFIUS/FIRRMA regime, thereby granting CFIUS the jurisdiction to review foreign investments in U.S. businesses handling these products.[274]

For example, in April 2020, BIS issued two final rules and proposed another specifically targeting the popular phenomenon of "Military-Civil Fusion" (MCF) in China, where the distinction between the civil economy and the defense sector is routinely blurred.[275] The two rules issued in April went into effect on June 29, 2020, the same day comments were due for the third rule. These rules came in direct response to the 2019 National Defense and Authorization Act (NDAA), which ordered the Department of Commerce to generate new guidelines for restricting emerging technologies.[276]

The first final rule amends Rule 744 of the EAR in order to expand the scope of what is categorized as "military end use" and thus, subjected to licensing requirements. Under the latest restrictions, companies will be denied an export license if they possess knowledge that the product they are exporting, reexporting, or transferring will land in the hands of "military end users" or ultimately be applied for "military end use."[277] The second final rule eliminates an exemption that allowed some countries to export certain dual-use products on the CCL to 23 countries in Country Group D:1 (those countries traditionally subjected to increased restrictions due to national security concerns) without a license as long as the products were intended for "civil end-users for civil end-uses."[278] Finally, the proposed rule would remove an exemption that permits the reexport of certain CCL products to the same previous 23 countries, as long as the country of origin belonged to the Wassenaar Arrangement.[279]

v. Export Controls: Multilateral Export Control Regimes

The United States belongs to four multilateral export control regimes: the Wassenaar Arrangement, the Nuclear Suppliers Group, the Australia Group, and the Missile Technology Control Regime.

The Wassenaar Arrangement is a voluntary export control regime established in 1996 that includes 42 nations, all of whom have agreed to control the export and retransfer of a particular set of munitions and dual-use goods and technologies.[280] It is not intended to target any one state or region, but instead "to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations."

The Wassenaar Arrangement subjects dual-use goods and technologies to export controls if they are "key elements directly related to the indigenous development, production, use or enhancement of advanced conventional military capabilities whose proliferation would significantly undermine the objectives of the Wassenaar Arrangement." The group balances this estimation against how available a particular item is outside participating states, how effectively its exportation can be controlled, how well it can be specified, and whether it is "controlled by another regime," which may complicate the group's ability to control the item.[281]

The Nuclear Suppliers Group is an informal export control regime focused strictly on curbing the proliferation of nuclear weapons.[282] Its membership consists of 48 nuclear exporters that have agreed to coordinate the transfer of nuclear and nuclear-related material to non-nuclear states for strictly civilian purposes.

The Australia Group is a voluntary, informal export control regime established in 1985.[283] The group, consisting of 42 members, is devoted to curbing the proliferation of biological weapons. It has a set of export guidelines and shares six common control lists, which contain a variety

of items, from dual-use chemical manufacturing and biological equipment to materials for manufacturing chemical weapons to biological agents.

The Missile Technology Control Regime is also a voluntary, informal export control regime established in 1987 whose purpose is to curb the proliferation of missiles capable of delivering nuclear weapons and other weapons of mass destruction.[284]

B. Germany

i. Interaction between German Regime and EU 2019/452

EU 2019/452 encourages EU member states to institute mechanisms that permit halting a transaction if it is "*likely* to affect" security or public order—a transaction no longer needs to definitively to do so. Germany's Foreign Trade and Payments Act and accompanying Foreign Trade and Payments Ordinance reflects that tightened restriction.[285] Similarly, under EU 2019/452, the German Federal Ministry of Economics (BMWi) now has the authority to impose restrictions on transactions that might affect other EU member states or EU projects, not just Germany.[286] Article 4 of EU 2019/452 also instructs EU member states like Germany to consider more carefully how the transactions might affect "critical infrastructure,"[287] "critical technologies and dual use items,"[288] "supply of critical inputs,"[289] "access to sensitive information,"[290] and the "freedom and pluralism of the media."[291] Germany has applied this guidance by creating enforcement mechanisms based on particular industries.

As reflected in a recent amendment to the Act, which went into effect October 2020, the latest EU regulation permits the BMWi to consider additional factors related to the foreign investor, including whether the investor is directly or indirectly controlled by a foreign government, whether the investor has engaged in actions within Germany or another EU state that threatened the public order or security of that state, or whether there is a substantial risk that the investor violated Section 123(1) of the German Act against Restraints on Competition, which prohibits terrorism financing, money laundering, bribes, and other illicit financial schemes.[292]

The recent amendment also invites a lower standard for triggering scrutiny of a given transaction, from posing a "sufficiently grave threat" to simply "expected impairment" of the nation's public order and security.[293] Furthermore, transactions within critical infrastructure and critical industries are considered void unless they receive BMWi approval, a move that inevitably means more transactions will be subject to government review.[294]

ii. BMWi: Usage of the Blocking Power

In its 15 years of existence, the BMWi was only once authorized by the German government to formally block a transaction, though it came close to being granted such authorization several times. In 2016, the BMWi reviewed the potential acquisition of the German semiconductor Aixtron by Chinese company Fujian.[295] The BMWi initially cleared the deal, but eventually withdrew the clearance after receiving information from CFIUS, which eventually blocked the deal itself. As a result of the CFIUS block, the deal was abandoned, rendering the BMWi's blocking powers unnecessary.

The BMWi has also engaged in informalized mechanisms for blocking transactions when it does not have the proper jurisdiction over the transaction. In 2018, when the State Grid Corporation of China attempted to acquire a 20 percent stake in 50Hertz Transmission GmbH, a company responsible for operating one of Germany's four transmission grids, the BMWi convinced a Belgian transmission grid operator to purchase the stake instead and then resell it to a German state-owned bank.[296] A government request was cited as the reason for the elaborate purchasing scheme.

The only formal authorization to use its blocking power occurred in 2018 against a transaction involving Yantai Tahai Group, which provides various services within China's civil nuclear energy market.[297] Yantai attempted to acquire Leifeld, a German manufacturer of machine tools. BMWi conducted a month-long investigation, after which it determined the transaction posed potential risks to German national security interests, prompting the government to authorize a block of the transaction.[298] Upon hearing of the future block, Yantai abandoned the transaction.

C. Australia

i. FIRB: Usage of the Blocking Power

Between July 1, 2016 and June 30, 2017, the Australian Treasurer rejected three transactions, two of which were associated with the long-term lease of the New South Wales electricity network Ausgrid.[299] More specifically, in 2016, the Treasurer blocked the sale of Ausgrid to two investors from China and Hong Kong.[300] The investment, valued at $10 billion AUD, would have granted the foreign investors a 50.4 percent stake in Australia's largest energy grid.[301] According to Treasurer Scott Morrison, a "genuine national security issue" presented itself that justified blocking the transaction.[302]

Between July 1, 2017 and June 30, 2018, two proposed transactions were rejected—one involving residential real estate, the other concerning the purchase of agricultural land,[303] while the following fiscal year, only one transaction was rejected.[304] In November of 2018, then-Treasurer Josh Frydenberg blocked Hong Kong-based CK Infrastructure Group's bid of $13 billion AUD to buy Australian company APA Group and its associated energy network.[305] Though the FIRB could not arrive at a unanimous decision, it was concerned that such a transaction would grant a foreign company control over a majority of Australia's pipelines.

In April of 2020, the Foreign Investment Review Board (FIRB) blocked two proposed investments by Chinese investors into Australian mining companies on the basis of the investments being deemed contrary to Australia's "national interest."[306] The first proposed transaction, announced in August 2019, involved a $20 million AUD investment by Chinese state-owned steel producer Baogang Group Investment Pty Ltd. The second proposed transaction concerned a $14.1 million AUD investment by Chinese lithium chemical producer Yibin Tianyi Lithium Industry ("Yibin Tianyi") into Australian company AVZ Minerals. Though the transaction was technically withdrawn as opposed to outright rejected, Yibin Tianyi had received notice from the FIRB that its bid for an 11.8 percent ran "contrary to national interest" and subsequently withdrew its application.[307]

ii. FIRB: Proposed July 2020 Reforms

The *Foreign Investment Reform Bill 2020: National Security Reviews and Last Resort Power* was proposed in July of this year and would result in sweeping reforms to the review of foreign investments in Australia.[308]

a. Increased National Security Focus

Some of the more prominent proposals to modifying FIRB in 2021 include allowing the Treasurer to place conditions on a transaction or block it entirely, regardless of the investment value; mandating notification of a transaction if it takes place in a sensitive national security sector; mandating notification if a foreign person begins engaging in national security business; allowing traditionally non-reviewed transactions to be "called in" by the Treasurer on national security grounds; granting investors the ability to alert FIRB voluntarily in order to receive possible protection from a call-in or an exemption certificate; and allowing the Treasurer to block a previously approved investment on national security grounds.[309]

b. Revised Thresholds

The amendments proposed by the Foreign Investment Reform Bill include a narrowing of the definition of "foreign government investor" by excluding entities with over 40 percent government ownership in total, as long as each government is in possession of less than a 20 percent stake and no operational decisions are subject to governmental control.[310] While seemingly reasonable, this accommodation may not have been the best policy, given the manner in which foreign governments can still exert unspoken influence over business decisions, even if nominally, such input appears to be absent.

If funds do have a foreign government investor at 20 percent or higher, they are still able to apply for an exemption certificate. A large driver of these particular reforms is allowing for managed funds to invest in Australia without facing the categorization—and regulation—of being a foreign government investor.[311]

c. Stronger Enforcement Mechanisms

Under the proposed reforms, the criminal and financial penalties for violating the Foreign Acquisitions and Takeovers Act of 1975 (FATA) increase significantly. For example, under the current regime, the penalty for a company failing to gain approval from the FIRB is $277, 500 AUD, an amount that was seen as an insufficient deterrent for bad behavior.[312] Under the proposed reforms, the same breach would garner a fine of $11,100,000 AUD or 75 percent of the investment value, capped at $555,000,000, whichever of the two values was greater. In certain situations, imprisonment terms have been raised from a mere three years to a decade, while financial penalties have risen by a factor of 10 for particular violations.[313]

Endnotes

1. "Asymmetric Competition: A Strategy for China and Technology," China Strategy Group, Fall 2020, p.3, https://beta.documentcloud.org/documents/20463382-final-memo-china-strategy-group-axios-1.
2. Kirsty Needham, "Australia demands apology from China after fake image posted on social media," Reuters, November 29, 2020, https://www.reuters.com/article/us-australia-china/australia-demands-apology-from-china-after-fake-image-posted-on-social-media-idUSKBN28A07Y.
3. The President of the United States, *National Security Strategy of the United States of America*, The White House, December 2017 https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.
4. U.S. National Security Council, *U.S. Strategic Framework for the Indo-Pacific*, The White House, February 2018, https://www.whitehouse.gov/wp-content/uploads/2021/01/IPS-Final-Declass.pdf.
5. Farnaz Fassihi and Steven Lee Myers, "Defying U.S., China and Iran Near Trade and Military Partnership," *The New York Times*, July 11, 2020, https://www.nytimes.com/2020/07/11/world/asia/china-iran-trade-military-deal.html.
6. Bob Davis and Lingling Wei, "Biden Plans to Build a Grand Alliance to Counter China. It Won't Be Easy." *The Wall Street Journal*, January 6, 2020, https://www.wsj.com/articles/biden-trump-xi-china-economic-trade-strategy-policy-11609945027?st=eqqsqv5bccevhj2&reflink=desktopwebshare_permalink.
7. Arie Egozi, "US To Israel: No More Chinese Deals; Pompeo's Flying Visit," *Breaking Defense*, May 13, 2020, https://breakingdefense.com/2020/05/us-to-israel-no-more-chinese-deals-pompeos-flying-visit/
8. Ibid. p. 6.
9. Ibid. p. 3.
10. "Israel Exports, Imports and Trade Balance By Country 2018," World Integrated Trade Solution, World Bank, https://wits.worldbank.org/CountryProfile/en/Country/ISR/Year/LTST/TradeFlow/EXPIMP/Partner/by-country.
11. Hagai Shagrir, *Israel-China Relations: Innovative Comprehensive Partnership, Israel-China Relations: Opportunities and Challenges*, Institute for National security Studies, Memorandum No. 194, August 2019, p. 20.
12. JINSA Interviews with American Officials on Background.
13. Hannah Gardner, "Xi Jinping: Time for 'new era' China to 'take center stage in the world'," *USA Today*, October 18, 2017, https://www.usatoday.com/story/news/world/2017/10/18/xi-jinping-time-new-era-china-take-center-stage-world/774958001/.
14. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2020*, September 2020, p. 44.
15. Ibid. p. 38.
16. Hal Brands and Jake Sullivan, "China Has Two Paths to Global Domination," *Foreign Policy*, May 22, 2020, https://foreignpolicy.com/2020/05/22/china-superpower-two-paths-global-domination-cold-war/.
17. Bijun Wang and Kailin Gao, "Outward Direct Investment: Restricted, Relaxed and Regulated Stages of Development," in Ross Garnaut, Ligang Song, and Cai Fang, eds., China's 40 Years of Reform and Development: 1978–2018 (Canberra: ANU Press, 2018), pp. 619–636.
18. Shira Efron, Karen Schwindt, and Emily Haskel, *Chinese Investment in Israeli Technology and Infrastructure: Security Implications for Israel and the United States* (Santa Monica, CA: RAND Corporation, 2020), p. 1.
19. Elsa B. Kania, "In Military-Civil Fusion, China is Learning Lessons from the United States and Starting to Innovate," *Strategy Bridge*, August 27, 2019, https://thestrategybridge.org/the-bridge/2019/8/27/in-military-civil-fusion-china-is-learning-lessons-from-the-united-states-and-starting-to-innovate.
20. Ibid.
21. Anthea Roberts, Henrique Choer Moraes, Victor Ferguson, "Geoeconomics: the Chinese Strategy of Technological Advancement and Cybersecurity," *Lawfare*, December 3, 2018, https://www.lawfareblog.com/geoeconomics-chinese-strategy-technological-advancement-and-cybersecurity.
22. Rush Doshi, "Beijing Believes Trump Is Accelerating American Decline," *Foreign Policy*, October 12, 2020, foreignpolicy.com/2020/10/12/china-trump-accelerating-american-decline/.
23. John C. Demers, "China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses," Statement to the Committee on the Judiciary, U.S. Senate, December 12, 2018, https://www.justice.gov/sites/default/files/testimonies/witnesses/attachments/2018/12/18/12-05-2018_john_c._demers_testimony_re_china_non-traditional_espionage_against_the_united_states_the_threat_and_potential_policy_responses.pdf.
24. Steven T. Dennis, "FBI Chief Says China Is Trying to 'Steal Their Way' to Economic Dominance," *Time*, July 24, 2019, https://time.com/5633390/fbi-christopher-wray-china-counterintelligence/.
25. Thilo Hanemann, Daniel H. Rosen, Cassie Gao, and Adam Lysenko, *Two-Way Street—US-China Investment Trends—2020 Update*, Rhodium Group, May 11, 2020, p. 18.

26. Ibid., p. 23.
27. Ibid., p. 20.
28. Kristen Millares Young, "China Shipping Lines to expand at port," *Seattle PI*, April 21, 2008, https://www.seattlepi.com/business/article/China-Shipping-Lines-to-expand-at-port-1271001.php.
29. Mark Hosenball and Andrea Shalal-Esa, "United Technologies sent military copter tech to China," Reuters, June 28, 2012, https://www.reuters.com/article/us-usa-china-helicopters/united-technologies-sent-military-copter-tech-to-china-idUSBRE85R1AG20120628.
30. 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, January 2018, p. 24.
31. Karen Freifeld and Alexandra Alper, "Exclusive: U.S. officials agree on new ways to control high tech exports to China—sources," Reuters, April 1, 2020, https://www.reuters.com/article/us-usa-china-technology-exclusive/exclusive-u-s-officials-agree-on-new-ways-to-control-high-tech-exports-to-china-sources-idUSKBN21K007.
32. 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, January 2018, p. 4.
33. "From China with Love: AI, Robotics, AR/VR Are Hot Areas for Chinese Investment In US," CB Insights, August 1, 2017" www.cbinsights.com/research/chinese-investment-us-tech-expert-research/.
34. 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, January 2018, p. 5.
35. Paul Mozur and Jane Perlez, "China Tech Investment Flying Under the Radar, Pentagon Warns," *The New York Times*, April 7, 2017, https://www.nytimes.com/2017/04/07/business/china-defense-start-ups-pentagon-technology.html.
36. Thilo Hanemann, Daniel H. Rosen, Cassie Gao, and Adam Lysenko, *Two-Way Street—US-China Investment Trends—2020 Update*, Rhodium Group, May 11, 2020.
37. Demetri Sevastopulo and Katrina Manson, "Pentagon lists 20 companies aiding Chinese military," *Financial Times*, June 24, 2020, https://www.ft.com/content/cd44c4ae-adda-4c5b-aa0e-853505c25d31.
38. Charlotte Butash, "What's in the New Huawei Indictment?" *Lawfare*, February 25, 2020, https://www.lawfareblog.com/whats-new-huawei-indictment.
39. Ethan Baron, "Chinese company Huawei's Silicon Valley outpost allegedly stole trade secrets from Cisco," *Mercury News*, February 13, 2020, https://www.mercurynews.com/2020/02/13/chinese-company-huaweis-silicon-valley-outpost-allegedly-stole-trade-secrets-from-cisco/.
40. Ryan Fedasiuk and Jacob Feldgoise, "The Youth Thousand Talents Plan and China's Military," Center for Security and Emerging Technology, August 2020, https://cset.georgetown.edu/wp-content/uploads/CSET-Youth-Thousand-Talents-Plan-and-Chinas-Military.pdf.
41. White House Office of Trade and Manufacturing Policy, *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World*, White House, June 2018.
42. Christopher Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States," Federal Bureau of Investigation, July 7, 2020, https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states.
43. Department of Justice Office of Public Affairs, "Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases," Press Release, Department of Justice Office of Public Affairs, January 28, 2020, https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related.
44. Department of Justice Office of Public Affairs, "Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases," Press Release, January 28, 2020, https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related.
45. Department of Justice Office of Public Affairs, "Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases," Press Release, January 28, 2020, https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related.
46. Office of the United States Trade Representative, *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade act of 1974*, Executive Office of the President, March 22, 2018, p. 177.
47. The Commission on the Theft of American Intellectual Property, *Update to the IP Commission Report: The Theft of American Intellectual Property*, The National Bureau of Asian Research, February 2017, p. 2.
48. Economic and Trade Agreement Between the Government of the United States of American and the Government of the People's Republic of China, January 15, 2020.

49. David Lawder and Andrea Shalal, “Exclusive: U.S.-China trade deal review postponed as China ramps up farm, energy purchases,” Reuters, August 14, 2020, https://www.reuters.com/article/us-usa-trade-china-meeting-exclusive/exclusive-us-china-trade-deal-review-planned-for-saturday-postponed-sources-idUSKCN25A29Q.
50. Kirsty Needham, “Australia demands apology from China after fake image posted on social media,” Reuters, November 29, 2020, https://www.reuters.com/article/us-australia-china/australia-demands-apology-from-china-after-fake-image-posted-on-social-media-idUSKBN28A07Y.
51. Efron, Schwindt, and Haskel, p. 38.
52. Ibid., p. 40-45
53. Doron Ella, “Regulation of Foreign Investments and Acquisitions: China as a Case Study,” *Israel-China Relations: Opportunities and Challenges*, Institute for National Security Studies, Memorandum No. 194 August 2019, p. 70
54. Jeremaya Goldberg, “Tunnels completed on new Israeli line,” *International Railway Journal*, April 24, 2014, https://www.railjournal.com/regions/middle-east/tunnels-completed-on-new-israeli-line/
55. Eytan Halon, “Chinese infrastructure giants set sights on increased Israel activity,” *The Jerusalem Post*, December 9, 2018, https://www.jpost.com/opinion/how-israel-and-china-are-increasing-their-cooperation-on-the-railways-573678.
56. “Red Line Light Rail in Tel Aviv,” *Tunnelbuilder*, August 8, 2016, https://tunnelbuilder.com/News/Red-Line-Light-Rail-in-Tel-Aviv.aspx.
57. World Bank, “World Bank Group Debars China Railway Construction Corporation Ltd. and two subsidiaries,” Press Release, World Bank, June 5, 2019, https://www.worldbank.org/en/news/press-release/2019/06/05/world-bank-group-debars-china-railway-construction-corporation-ltd-and-two-subsidiaries.
58. Demetri Sevastopulo and Katrina Manson, “Pentagon lists 20 companies aiding Chinese military,” *Financial Times*, June 24, 2020, https://www.ft.com/content/cd44c4ae-adda-4c5b-aa0e-853505c25d31.
59. Efron, Schwindt, and Haskel, p. 45.
60. “Chinese Company Connects Tel Aviv Rail, Tehran,” *Times of Israel*, July 6, 2015, https://www.timesofisrael.com/chinese-company-connects-tel-aviv-rail-tehran/
61. Efron, Schwindt, and Haskel, p. 54.
62. Ibid., p. 44.
63. Ibid., p. 46.
64. Agence France Press and Times of Israel, “Amid US pressure, Israel taps local firm over China for $1.5b desalination plant, *The Times of Israel*, May 26, 2020, https://www.timesofisrael.com/amid-us-pressure-israel-taps-local-firm-over-chinese-bid-for-desalination-plant/.
65. William A. Galston, “What’s Beijing Doing in Haifa?” *The Wall Street Journal*, May 28, 2019, https://www.wsj.com/articles/whats-beijing-doing-in-haifa-11559085122.
66. Michael Wilner, “U.S. Navy may stop docking in Haifa after Chinese take over port,” *The Jerusalem Post*, December 15, 2018, https://www.jpost.com/israel-news/us-navy-may-stop-docking-in-haifa-after-chinese-take-over-port-574414.
67. Michael Wilner, “U.S. Navy may stop docking in Haifa after Chinese take over port,” *The Jerusalem Post*, December 15, 2018, https://www.jpost.com/israel-news/us-navy-may-stop-docking-in-haifa-after-chinese-take-over-port-574414.
68. Times of Israel Staff, “Pompeo warns US could curb security ties with Israel over China relations,” *The Times of Israel*, March 21, 2019, https://www.timesofisrael.com/pompeo-warns-us-could-curb-security-ties-with-israel-over-china-relations/.
69. Barak Ravid, “Trump told Netanyahu that Israel's China ties could harm security cooperation,” *Axios*, April 14, 2019, https://www.axios.com/trump-netanyahu-israel-china-security-cooperation-243ea932-765b-490f-9002-9744192b8905.html.
70. Mehul Srivastava and Katrina Manson, “US pressure over China prompts Israeli review of $1.5bn tender,” *Financial Times*, May 13, 2020, https://www.ft.com/content/f2988ffe-103d-4ac7-9a63-76be270e49ba
71. Jonah Jeremy Bob, “China wins on Haifa port, but fights with US for the future—analysis,” *The Jerusalem Post*, December 12, 2019, https://www.jpost.com/israel-news/china-wins-on-haifa-port-but-fights-with-us-for-the-future-analysis-610510.
72. Geoffrey F. Gresh, “To Rule Eurasia’s Waves: The New Great Power Competition at Sea,” (New Haven, CT: Yale University Press, 2020), p. 72.
73. JINSA Interviews with American Officials on Background.
74. JINSA Interviews with American Officials on Background.
75. The two major enterprises executing these ventures are China Merchants Port Holdings and COSCO Shipping, who acquired a majority stake in the Greek company Piraeus Port Authority and has pledged to invest $660 million into the port. Beijing regards Piraeus as one of its flagship BRI achievements, and Piraeus has become the second-largest port in the Mediterranean after Valencia. See: David Glass, “Greece aims to build on Chinese cooperation in Piraeus port,” Seatrade Maritime News, June 9, 2020, https://www.seatrade-maritime.

com/ports-logistics/greece-aims-build-chinese-cooperation-piraeus-port; Eleanor Albert, "China's Global Port Play," *The Diplomat*, May 11, 2019, https://thediplomat.com/2019/05/chinas-global-port-play/.

76. For example, the Piraeus investment is concerning for many of the same reasons previously discussed about Chinese investment into infrastructure, but U.S. naval vessels typically uses anchorages one nautical mile on the island of Psyttaleia or two and a half nautical miles southeast at Falirou Bay, decreasing the likelihood of espionage.
77. Mark Hosenball and Andrea Shalal-Esa, "United Technologies sent military copter tech to China," Reuters, June 28, 2012, https://www.reuters.com/article/us-usa-china-helicopters/united-technologies-sent-military-copter-tech-to-china-idUSBRE85R1AG20120628.
78. Meera Selva, "Heating up the arms race," *Handelsblatt Today*, May 8 2016, https://www.handelsblatt.com/today/from-our-magazine-heating-up-the-arms-race/23539836.html?ticket=ST-226976-l0qfHMbx7KIH0h60mAjY-ap1; "Chinese Military's Secret to Success: European Engineering," *Voice of America*, December 13, 2013, https://www.voanews.com/east-asia/chinese-militarys-secret-success-european-engineering.
79. Farnaz Fassihi and Steven Lee Myers, "Defying U.S., China and Iran Near Trade and Military Partnership," *The New York Times*, July 11, 2020, https://www.nytimes.com/2020/07/11/world/asia/china-iran-trade-military-deal.html.
80. David Rogers, "Israel Avoids Wrath of Congress By Pulling Phalcon Sale to China," *The Wall Street Journal*, July 13, 2000, https://www.wsj.com/articles/SB963446235663694414.
81. Scott Wilson, "Israel Set to End China Arms Deal Under U.S. Pressure," *The Washington Post*, June 27, 2005, https://www.washingtonpost.com/archive/politics/2005/06/27/israel-set-to-end-china-arms-deal-under-us-pressure/72734d39-e37c-4ae7-a61f-2cca56516a1e/.
82. "Defense Ministry D-G Amos Yaron Announces Resignation," *Haaretz*, August 29, 2005, https://www.haaretz.com/1.4937702.
83. Ora Coren, "Washington Obstructing Israeli High-tech Exports to China," *Haaretz*, January 21, 2014, https://www.haaretz.com/israel-news/business/.premium-u-s-barring-israeli-tech-export-to-china-1.5313832.
84. Liz Alderman, "Wary of China, Europe and Others Push Back on Foreign Takeovers," *The New York Times*, March 15, 2018, https://www.nytimes.com/2018/03/15/business/china-europe-canada-australia-deals.html.
85. Efron, Schwindt, and Haskel, p. xv.
86. Ibid., p. ix.
87. Tova Cohen and Catherine Cadell, "Huawei in Talks to Buy Israeli Cyber Company HexaTier: Sources," Reuters, December 20, 2016, https://www.reuters.com/article/us-huawei-tech-hexatier-m-a/huawei-in-talks-to-buy-israeli-cyber-company-hexatier-sources-idUSKBN1491O6.
88. David Shamah, "Israel gets $20m to create robot workers for China," *The Times of Israel*, December 21, 2015, https://www.timesofisrael.com/israel-gets-20m-to-create-robot-workers-for-china/.
89. ויס-הרא"ב-לארשי רוטקסו ייהה—קט-מנמואה סנעצכ התקע?" ומצלוה באז," Data and Insights, May 2020
90. Ed Felton and Terah Lyons, "The Administration's Report on the Future of Artificial Intelligence," White House Blog , October 12, 2016, https://www.whitehouse.gov/blog/2016/10/12/administrations-report-future-artificial-intelligence.
91. Mark Hookham and Richard Kerbaj, "Has China used British technology to build a railgun?" *The Times*, March 4, 2018, https://www.thetimes.co.uk/article/has-china-used-british-technology-to-build-a-railgun-n7blzkmdg.
92. 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, January 2018, p. 15.
93. Ivan Levingston, "U.S. Scrutiny of Israel's China Ties Expands to Universities," *Bloomberg*, May 18, 2020, https://www.bloomberg.com/news/articles/2020-05-19/u-s-scrutiny-of-israel-s-china-ties-expands-to-universities.
94. "Guangdong Technion Israel Institute of Technology in Shanto," *The Jerusalem Post*, October 22, 2018, https://www.jpost.com/special-content/technions-campus-in-china-569944; Tova Cohen, "Tel Aviv, Tsinghua Universities Set Up $300 Mln Research Center," Reuters, May 19, 2014, https://finance.yahoo.com/news/tel-aviv-tsinghua-universities-set-300-mln-research-140720930—sector.html.
95. Confucius Institute Headquarters, "About Confucius Institute/Classrooms," http://english.hanban.org/node_10971.htm.
96. Patricia Zengerle, "Senate Panel Wants Chinese-Funded Institutes to Change or Leave U.S.," Reuters, February 27, 2019, https://www.reuters.com/article/us-china-education-usa/senate-panel-wants-chinese-funded-institutes-to-change-or-leave-us-idUSKCN1QG33G; Deb Riechmann, "Trump administration: Confucius Institute is arm of Beijing," *The Washington Post*, August 13, 2020, https://www.washingtonpost.com/world/national-security/trump-administration-confucius-institute-is-arm-of-beijing/2020/08/13/37418da0-dd8a-11ea-b4f1-25b762cdbbf4_story.html.
97. Natalie Obiko Pearson, "Did a Chinese hack kill Canada's greatest tech company?" *BNN Bloomberg*, July 1, 2020, https://www.bnnbloomberg.ca/did-a-chinese-hack-kill-canada-s-greatest-tech-company-1.1459269.

98. McAfee Foundstone Professional Services and McAfee Labs, *Global Energy Cyberattacks: "Night Dragon*," McAfee, February 10, 2011, p. 3.
99. *APT1: Exposing One of China's Cyber Espionage Units*, Mandiant, 2013, pp. 3, 22.
100. Office of the United States Trade Representative, *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade act of 1974*, Executive Office of the President, March 22, 2018, p. 7.
101. Ibid., p. 33.
102. Shira Efron, Howard J. Shatz, Arthur Chan, Emily Haskel, Lyle J. Morris, and Andrew Scobell, *The Evolving Israel-China Relationship* (Santa Monica, CA: RAND Corporation, 2019), p. 68.
103. Robert D. Williams, "CFIUS Reform and U.S. Government Concerns over Chinese Investment: A Primer," *Lawfare Blog*, November 13, 2017, https://www.lawfareblog.com/cfius-reform-and-us-government-concerns-over-chinese-investment-primer.
104. Ibid.
105. Ibid.
106. Ibid.
107. Committee on Foreign Investment in the United States, Annual Report to Congress: CY 2019, https://home.treasury.gov/system/files/206/CFIUS-Public-Annual-Report-CY-2019.pdf. *See also* Kirkland & Ellis, CFIUS Releases its 2019 Annual Report—Key Points for Dealmakers, August 12, 2020, https://www.kirkland.com/-/media/publications/alert/2020/08/cfius-releases-its-2019-annual-report--key-points.pdf.
108. Williams, "CFIUS Reform and U.S. Government Concerns over Chinese Investment: A Primer."
109. "Non-controlling investments" are defined as under 10 percent of voting shares in publicly traded companies or under 10 percent of total assets of non-publicly traded U.S. firm. CFIUS's jurisdiction to review transactions involving a noncontrolling investment depends upon whether the foreign investor subsequently gains access to "material nonpublic technical information" belonging to the business; if the investor gains either membership to the company's board or observer rights; or if the investor plays a substantive role in decisions related to critical technology. This modification was enacted as an investor with a noncontrolling interest might still "affect certain decisions made by, or obtain certain information from, a U.S. business with respect to the use, development, acquisition, or release of critical technology." James K. Jackson, "The Committee of Foreign Investment in the United States," Congressional Research Service, February 14, 2020, p. 11, 16-17.
110. U.S. Department of the Treasury, CFIUS Monitoring and Enforcement, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-monitoring-and-enforcement.
111. Jackson, p. 15.
112. Ian F. Ferguson and Paul K. Kerr, *The U.S. Export Control System and the Export Control Reform Initiative*, Congressional Research Service, January 28, 2020, p. 1.
113. 15 C.F.R. § 730 *et seq*. Ibid, p. 3.
114. The Export Control Classification Number (ECCN) is an identifying number that details into which category and sub-category a particular item falls. The categories within the CCL include the following: Nuclear & Miscellaneous; Materials, Chemicals, Microorganisms, and Toxins; Materials Processing; Electronics; Computers; Telecommunications; Information Security; Sensors and Lasers; Navigation and Avionics; Marine; and Aerospace and Propulsion. These categories are then further divided into five sub-categories: Systems, Equipment, and Components; Test, Inspection, and Production Equipment; Material; Software; and Technology.
115. 15 C.F.R. § 730.3. Ferguson et al., p. 3.
116. An overview of the application process can be found on the Bureau of Industry and Security website, under the page titled, "Guidelines for Preparing Export License." U.S. Department of Commerce, Bureau of Industry and Security, "Guidelines for Preparing Export License," https://www.bis.doc.gov/index.php/all-articles/16-policy-guidance/product-guidance/267-guidelines-for-preparing-export-license.
117. 15 C.F.R. § 734.13(b). U.S. Department of Commerce, Bureau of Industry and Security, Deemed Exports, https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports.
118. Ibid.
119. Ibid., p. 4.
120. Ferguson and Kerr, p. 8. The influence of the multilateral export regimes cuts both ways in terms of tightening or relaxing restrictions. For instance, in 2010, an amendment to the EAR removed CCL controls on items whose encryption use was "ancillary" to the item's function.
121. For instance, India was granted STA-1 status by the Trump Administration in 2018, despite not acceding the Nuclear Suppliers Group.
122. Joshua Kirschenbaum, Etienne Soula, and Meaghan Clohessy, *EU Foreign Investment Screening - At Last, A Start*, Alliance for Securing Democracy (September 24, 2019), https://securingdemocracy.gmfus.org/eu-foreign-investment-screening-at-last-a-start/.
123. Ibid.
124. Ibid; Regulation (EU) 219/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, March 21, 2019 O.J. (L 791) 1-14.

125. Kirschenbaum et al., *EU Foreign Investment Screening - At Last, A Start*; Regulation (EU) 2019/452 Article 1(1).
126. Regulation (EU) 2019/452 Article 1(1).
127. Some EU states, such as Germany and France, have quite robust screening regimes, while some states, such as Sweden, have no regime in place whatsoever as of June 2020.
128. Debevois and Plimpton, *Foreign Direct Investment Rules in Selected European Countries—An Overview*, Debevoise in Depth, p. 5, June 16, 2020 https://www.debevoise.com/insights/publications/2020/05/foreign-direct-investment-rules-in-selected.
129. Ibid, p. 5-6. If a non-German investor acquires greater than 10 percent of the voting rights or assets of a German company that is in either the defense sector or a non-defense, protected sector, that investor is obligated to file with the BMWi. For non-protected sectors, the threshold stake is increased to 25 percent if the investment poses a possible threat to the public order or security of Germany.
130. Ibid, p. 9.
131. Ibid, p. 10.
132. Ibid, p. 8.
133. John Tivey and Barnaby Matthews, "Foreign direct investment reviews 2019: Australia," White & Case, December 27, 2019 https://www.whitecase.com/publications/insight/foreign-direct-investment-reviews-2019-australia#:~:text=The percent20decision percent20to percent20approve percent20or,contrary percent20to percent20the percent20national percent20interest.
134. Hogan Lovells, *Foreign Investment in Australia: What you need to know—COVID-19 Edition*, September 17, 2020, p. 5, https://www.lexology.com/library/detail.aspx?g=24c4d41d-ac6f-4057-9397-9990f4f20d59&filterId=19e323c7-b692-49dd-a120-a899289d494d
135. Ibid.
136. Ibid, p. 27.
137. Ibid.
138. Bird & Bird LLP, "Changes to Foreign Investment—Protecting Australia's National Security," July 2, 2020 https://www.lexology.com/library/detail.aspx?g=7a32ebe8-0f73-48cf-8f8f-4818fc368831.
139. Reuters Staff, "Australia to review all foreign investments during coronavirus," March 29, 2020 https://www.reuters.com/article/us-health-coronavirus-australia/australia-to-review-all-foreign-investments-during-coronavirus-idUSKBN21G0XL.
140. *Foreign Investment in Australia: What you need to know—COVID-19 Edition*, p. 29.
141. Ibid.
142. Ibid.
143. Daniel Rosenblatt, Foreign Oversight Investment in Israel: An Israeli "CFIUS" (Part 2 of 3), Lexology, April 4, 2020 https://www.lexology.com/library/detail.aspx?g=e1e25c77-2026-496a-b65a-8084c77e76f3.
144. חוק מיזוג מיינוחטיב מיסרטניא לע הנגה) מיינוחטיב מידיגאתה חוק), תשס"ו-2006.
145. Rosenblatt, Foreign Oversight Investment in Israel: An Israeli "CFIUS" (Part 2 of 3).
146. Ibid.
147. חוק יעקרקמ לארשי, תש"ך-1960.
148. Rosenblatt, Foreign Oversight Investment in Israel: An Israeli "CFIUS" (Part 2 of 3).
149. Ibid.
150. Ibid.
151. Ibid.
152. חוק תרושקתה קזב(מירודישו קזב), תשמ"ב-1982.
153. Rosenblatt, "Foreign Oversight Investment in Israel: An Israeli 'CFIUS' (Part 2 of 3)."
154. חוק תרושקתה.
155. חוק תרושקתה. See also Rosenblatt, Foreign Oversight Investment in Israel: An Israeli "CFIUS" (Part 2 of 3).
156. Rosenblatt, Foreign Oversight Investment in Israel: An Israeli "CFIUS" (Part 2 of 3).
157. Government of Japan and the Government of Israel, Agreement between Japan and the State of Israel for the Liberalization, Promotion and Protection of Investment, February 1, 2017, https://jusmundi.com/en/document/pdf/Treaty/IIA-3721/en/en-israel-japan-bit-2017-israel-japan-bit-2017-wednesday-1st-february-2017.
158. Rosenblatt, Foreign Oversight Investment in Israel: An Israeli "CFIUS" (Part 2 of 3).
159. The 34th Government of Israel, Security Cabinet Statement, October 30, 2019 https://www.gov.il/en/departments/news/spoke_national_security301019.
160. Ibid.
161. Daniel Rosenblatt, "Foreign Oversight Investment in Israel: An Israeli 'CFIUS' (Part 3 of 3)," Lexology, April 6, 2020 https://www.lexology.com/library/detail.aspx?g=e527b865-3f3c-454d-8cbb-c312a5691926.
162. Simon Weintraub, Daniel Green, and Micki Shapira, "Establishment of Advisory Committee on Foreign Investment," Lexology, November 3, 2019 https://www.lexology.com/library/detail.aspx?g=d5affe08-87aa-4358-8ef6-2c54ae54f660.
163. Rosenblatt, "Foreign Oversight Investment in Israel: An Israeli 'CFIUS' (Part 3 of 3)."

164. Unless noted, the information in this section "Export Controls: Israeli Review of Outbound Foreign Transactions" was obtained in an interview on September 17, 2020, with Daniel Rosenblatt of Herzog Fox & Neeman.
165. חוקיפה קוח לע אוצי ביטחנוי, תשסז"ז-2007.
166. Rosenblatt, "Foreign Oversight Investment in Israel: An Israeli 'CFIUS' (Part 2 of 3)."
167. Ibid.
168. Wassenaar Arrangement Secretariat, Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Public Documents, Vol. II, December 2019 https://www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-PUB-002-Public-Docs-Vol-II-2019-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-19.pdf.
169. Douglas J. Feith, "The Chinese Challenge to the U.S.-Israeli Relationship," Wall Street Journal (May 15, 2020) https://www.wsj.com/articles/the-chinese-challenge-to-the-u-s-israel-relationship-11589576485.
170. Office of the United States Trade Representative, Israel https://ustr.gov/countries-regions/europe-middle-east/middle-eastnorth-africa/israel.
171. Ibid.
172. Office of the United States Trade Representative, Israel Free Trade Agreement, https://ustr.gov/trade-agreements/free-trade-agreements/israel-fta.
173. Jack Penders and Maiya Clark, *How Pentagon's "Trusted Capital" Program Can Secure Financing for Defense Industrial Base*, The Heritage Foundation, November 27, 2019.
174. Ibid.
175. Ibid.
176. Federal Register, Export Control Reform Initiative: Strategic Trade Authorization License Exception,
177. Ibid.
178. Ibid.
179. Export-Import Bank of the United States, *2019 Annual Report: Keeping America Strong*, February 29, 2020, p. 2.
180. Ibid, p. 6.
181. Ibid, p. 5.
182. American Business Television, "Addresses COVID-19 Response and New 'Program on China Transformational Exports' to Keep America Strong," https://americanbusinesstv.com/abtv-business-news/economy/small-business/addresses-covid-19-response-and-new-program-on-china-and-transformational-exports-to-keep-america-strong/.
183. Export-Import Bank of the United States, *2019 Annual Report: Keeping America Strong*, p. 6.
184. Ibid.
185. Ibid.
186. Ibid.
187. Pillsbury Law, "Understanding the New $60 Billion U.S. International Development Finance Corporation," August 17, 2020 https://www.pillsburylaw.com/en/news-and-insights/dfc-development-finance-corporation.html.
188. Lisa Viscidi and Sarah Phillips, "Countering China through Infrastructure Investments," Global Americans, March 31, 2020 https://theglobalamericans.org/2020/03/countering-china-through-infrastructure-investments/.
189. Ibid.
190. Prioritization of Efforts and Assistance for Energy Infrastructure Projects in Europe and Eurasia, 22 U.S. Code § 9563.
191. Adva Saldinger, "US DFC board approves deal so 'it doesn't fall into Chinese hands,'" Devex, September 11, 2020 https://www.devex.com/news/us-dfc-board-approves-deal-so-it-doesn-t-fall-into-chinese-hands-98068.
192. U.S. International Development Finance Corporation, "DFC Approves $3.6 Billion of New Investments in Global Development in Larges Quarter Ever," Press Release, September 9, 2020 https://www.dfc.gov/media/press-releases/dfc-approves-36-billion-new-investments-global-development-largest-quarter.
193. Adva Saldinger, "Trump authorizes US DFC to invest in domestic COVID-19 response," Devex, May 15, 2020 https://www.devex.com/news/trump-authorizes-us-dfc-to-invest-in-domestic-covid-19-response-97246.
194. U.S. Embassy in Israel, "US, Israel, UAE announce establishment of Abraham Fund following Accords commitment," Press Release, October 20, 2020, https://il.usembassy.gov/us-israel-uae-announce-establishment-of-abraham-fund-following-accords-commitment/.
195. Matthew Goldman, Daniel Runde, and Jonathan Hillman, "Connecting the Blue Dots," Center for Strategic and International Studies, February 26, 2020 https://www.csis.org/analysis/connecting-blue-dots.
196. Ibid.
197. Matthew Goodman, "Blue Dot Network: The Belt and Road Alternative," The Diplomat, April 7, 2020 https://thediplomat.com/2020/04/blue-dot-network-the-belt-and-road-alternative/.
198. Goodman et al., "Connecting the Blue Dots."
199. Zachary Keck, "Is China Getting Ready to Create its Very Own DARPA?", National Interest, July 29, 2017 https://nationalinterest.org/blog/the-buzz/china-getting-ready-create-its-very-own-darpa-21715.
200. Marcy E. Gallo, *Defense Advanced Research Projects Agency: Overview and Issues for Congress*, Congressional Research Service, March 17, 2020, p. 1-2.

201. Zachary Freyer-Biggs, "The Pentagon plans to spend $2 billion to put more artificial intelligence into its weaponry," *The Verge*, September 8, 2018, https://www.theverge.com/2018/9/8/17833160/pentagon-darpa-artificial-intelligence-ai-investment.
202. Marcy E. Gallo, *Defense Advanced Research Projects Agency: Overview and Issues for Congress*, Congressional Research Service, March 17, 2020, p. 9-10.
203. Combatting Terrorism Technical Support Office, *2018 Review Book*, https://cttso.gov/Documents/ReviewBooks/2018ReviewBook_web.pdf.
204. Yonah Jeremy Bob, "U.S. defense official works with Israel on cutting edge anti-terror tech," *The Jerusalem Post*, July 6, 2018, https://www.jpost.com/israel-news/us-defense-official-works-with-israel-on-cutting-edge-anti-terror-tech-561797.
205. Ibid.
206. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Sec. 889. Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment.
207. Jackson Barnett, "DOD's IT supply chain has dozens of suppliers from China, report finds," FedScoop, August 14, 2020, https://www.fedscoop.com/dod-it-supply-chain-chinese-ownership/.
208. Govini, *The Challenge of Reshoring the Defense Department Supply Chain*, August 2020.
209. National Defense Industrial Association, "Section 889," https://www.ndia.org/policy/section-889.
210. Catie Edmonson, "Senate Democrats Present $350 Billion Strategy to Counter China," *The New York Times*, September 17, 2020, https://www.nytimes.com/2020/09/17/us/politics/democrats-china-strategy.html.
211. Sherod Brown Senate Office, "Senate Democrats Unveil the America Leads Act to Make Comprehensive Investments in America Workers, Competitiveness, Alliances, and Diplomacy to Confront the Rise of China," Press Release, September 17, 2020, https://www.brown.senate.gov/newsroom/press/release/democrats-america-leads-act-investments-american-workers-competitiveness-china.
212. Stuart Wiener, "US extends loan guarantees to Israel for four more years, *The Times of Israel*, October 12, 2012, https://www.timesofisrael.com/us-extends-loan-guarantees-to-israel-for-another-four-years/
213. U.S. Department of the Treasury, "Joint Statement on the U.S.—Israel Joint Economic Development Group," Press Release, October 24, 2019, https://home.treasury.gov/news/press-releases/sm802.
214. Omri Nahmias, "US-Israeli officials discuss AI collaboration, solving space mysteries," *The Jerusalem Post*, October 27, 2019, https://www.jpost.com/american-politics/us-israeli-officials-discuss-ai-collaboration-solving-space-mysteries-605892.
215. 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, January 2018; Office of the United States Trade Representative, *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade act of 1974*, Executive Office of the President, March 22, 2018
216. *APT1: Exposing One of China's Cyber Espionage Units*, Mandiant, 2013
217. Efron, Schwindt, and Haskel, p. xv.
218. Rosenblatt Interview, September 17, 2020.
219. Ibid.
220. Ibid.
221. Israel Ministry of Foreign Affairs, "Israeli Statement at the conclusion of the Wassenaar Arrangement Outreach Delegation Visit," Press Release, November 20, 2019, https://mfa.gov.il/MFA/PressRoom/2019/Pages/Israeli-statement-at-the-conclusion-of-the-Wassenaar-Arrangement-Outreach-Delegation-visit-20-November-2019.aspx.
222. אוציהו אוביה וצ(חוקיפ לע אוציי מוחתב אוציי ימיכה, יגולויבה יניערגהו(, תשסד"-2004
223. JINSA Gemunder Center U.S.-Israel Security Policy Project, *Atlas Supported: Strengthening U.S.-Israel Strategic Cooperation* (May 2018).
224. *Defense Primer: RDT&E*, Congressional Research Service, April 29, 2020
225. National Defense Authorization Act for Fiscal Year 2021, S. 4049, 116th Congress, 2020.
226. JINSA Gemunder Center U.S.-Israel Security Policy Project, *Arming Israel to Defeat Iranian Aggression: Frontloading Weapons Delivery* (November 2019).
227. Correspondence with Daniel Rosenblatt, Herzog Law, Tel Aviv, Israel. January 18, 2020.
228. Daniel Rosenblatt, Foreign Oversight Investment in Israel: An Israeli "CFIUS" (Part 2 of 3), Lexology, April 4, 2020 https://www.lexology.com/library/detail.aspx?g=e1e25c77-2026-496a-b65a-8084c77e76f3. See also Agreement between the State of Israel and Japan for the Liberalization, Promotion, and Protection of Investment, the Government of Israel and the Government of Japan, February 1, 2017.
229. Conversation with Timothy Brightbill, Wiley Rein LLP, January 12, 2020. *See* Office of the United States Trade Representative, United States-Mexico-Canada Agreement, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement.
230. Blog Post by Guest Blogger for Net Politics, "The Coming North American Digital Trade Zone," Council on Foreign Relations, https://www.cfr.org/blog/coming-north-american-digital-trade-zone.

231. United States-Mexico-Canada Agreement, Chapter 19 (entered into force July 1, 2020), https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf.
232. "The Coming North American Digital Trade Zone," Council on Foreign Relations.
233. Ibid.
234. Ibid.
235. Global Innovation Policy Center, USMCA Can Revamp IP for a New Generation, https://www.theglobalipcenter.com/usmca-can-revamp-ip-for-a-new-generation/.
236. Ibid.
237. United States-Mexico-Canada Agreement, Chapter 4 (entered into force July 1, 2020) https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/04 percent20Rules percent20of percent20Origin.pdfOffice of the United States Trade Representative, UNITED STATES–MEXICO–CANADA TRADE FACT SHEET Modernizing NAFTA into a 21st Century Trade Agreement https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/fact-sheets/modernizing.
238. Conversation with Timothy Brightbill, Wiley Rein LLP, January 12, 2020.
239. United States-Mexico-Canada Agreement, Chapter 15 (entered into force July 1, 2020) https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/15-Cross-Border-Trade-in-Services.pdf.
240. Correspondence with Daniel Rosenblatt, Herzog Law, Tel Aviv, Israel. January 18, 2020. *See* Rachel F. Fefer, *U.S. Trade in Services: Trends and Policy Issues*, Congressional Research Service, January 22, 2020, p. 22.
241. Correspondence with Daniel Rosenblatt, Herzog Law, Tel Aviv, Israel. January 18, 2020.
242. Ibid.
243. United States-Mexico-Canada Agreement, Chapter 25 (entered into force July 1, 2020) https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/25_Small_and_Medium-Sized_Enterprises.pdf; Bridgehouse Law, How Small to Medium-Sized Enterprises Will Benefit from the USMCA (July 7, 2020), https://bridgehouse.law/sme-benefits-from-usmca.
244. Bnamericas, "Much of the USMCA's success could hinge on new SME chapter," July 1, 2020, https://www.bnamericas.com/en/news/much-of-usmcas-success-could-hinge-on-new-sme-chapter
245. Correspondence with Daniel Rosenblatt, Herzog Law, Tel Aviv, Israel. January 18, 2020.
246. Ibid.
247. Ryan Fedasiuk and Jacob Feldgoise, "The Youth Thousand Talents Plan and China's Military," Center for Security and Emerging Technology, August 2020, https://cset.georgetown.edu/wp-content/uploads/CSET-Youth-Thousand-Talents-Plan-and-Chinas-Military.pdf.
248. Ibid.
249. JINSA Gemunder Center US-Israel Policy Project, *For a Narrow U.S.-Israel Defense Pact: Paper and Draft Treaty* (July 2019); JINSA Gemunder Center U.S.-Israel Policy Project, *A Narrow U.S.-Israel Defense Pact: Addressing Criticism* (November 2019)
250. JINSA Gemunder Center US-Israel Policy Project, *For a Narrow U.S.-Israel Defense Pact: Paper and Draft Treaty* (July 2019)
251. JINSA Gemunder Center U.S.-Israel Security Policy Project, *Atlas Supported: Strengthening U.S.-Israel Strategic Cooperation* (May 2018), p. 36
252. Jackson, p. 23.
253. Ibid.
254. Ibid, p. 20.
255. John P. Barker et al., "CFIUS Proposes Rule to Align Certain Mandatory Filing Requirements With Export Control Regulations," Arnold & Porter, May 22, 2020, https://www.arnoldporter.com/en/perspectives/publications/2020/05/cfius-rule-to-align-mandatory-filing-requirements.
256. Ibid.
257. Christine Daya, Nicholas Klein, and Thomas deButts, "CFIUS proposes export control-based reforms to its mandatory filing program," DLA Piper, May 22, 2020, https://www.dlapiper.com/en/us/insights/publications/2020/05/cfius-proposes-export-control-based-reforms-to-its-mandatory-filing-program/.
258. Ibid.
259. Ibid.
260. Ibid.
261. The factors for consideration prior to FIRRMA included the following: domestic production of national defense requirements; whether the transaction impacts the capability and capacity of such production; whether the transaction might cede control of a domestic industry to a foreign entity, thereby impacting U.S.' ability to meet its national security requirements; whether transaction might affect the sale of military goods to a state that engages in terrorism or the proliferation of nuclear, biological, or chemical weapons; whether the transaction might impact U.S. leadership in the technology space, thus undermining U.S. national security interests; whether the transaction might impact critical infrastructure, thus posing a national security risk; whether the transaction might impact critical technologies in the United States; whether the transaction involves a foreign

government-controlled entity (rather than a private interest); if a foreign government, whether that government adheres to nonproliferation regimes, engages in counterterrorism efforts, or creates openings for the transfer of technology with possible military applications; what the long-term energy needs, as well as critical material needs, are of the United States; and any other additional factors the committee or the President believes to be relevant. Jackson, p. 29.

262. The additional factors added under FIRRMA include the following: whether the transaction involves a party from a country of "special concern;" whether parties involved have history of complying with U.S. law; whether the transaction will hinder U.S. capability to meet its material national security needs; whether the transaction has a likelihood of exposing the data of U.S. citizens to either foreign governments or person who may use such information to undermine U.S. national security interests; whether a transaction is likely to cause or worsen American cybersecurity weaknesses. Ibid, p. 30.
263. Ibid at 12-14.
264. Ibid.
265. Ibid.
266. Ibid.
267. Ibid.
268. Ibid.
269. Committee on Foreign Investment in the United States, Annual Report to Congress: CY 2019, https://home.treasury.gov/system/files/206/CFIUS-Public-Annual-Report-CY-2019.pdf.
270. Kirkland & Ellis, CFIUS Releases its 2019 Annual Report—Key Points for Dealmakers, August 12, 2020, https://www.kirkland.com/-/media/publications/alert/2020/08/cfius-releases-its-2019-annual-report--key-points.pdf.
271. Ibid.
272. Ibid.
273. Akin Gump, *The Export Control Reform Act and Possible New Controls on Emerging and Foundation Technologies*, September 12, 2018 https://www.akingump.com/en/news-insights/the-export-control-reform-act-of-2018-and-possible-new-controls.html. BIS issued its first Final Rule defining "emerging technologies" in June of 2020, limiting the exporting of specific precursor chemicals, COVID-19, and single-use cultivation chambers with rigid walls.
274. Ibid.
275. William Alan Reinsch and Jack Caporal, *Unpacking Expanding Export Controls and Military-Civil Fusion*, Center for Strategic and International Studies, May 14, 2020 https://www.csis.org/analysis/unpacking-expanding-export-controls-and-military-civil-fusion.
276. Ibid.
277. Ibid.
278. Ibid.
279. Ibid.
280. Ferguson and Kerr, p. 8.
281. The Wassenaar Arrangement, *What is the Wassenaar Arrangement?*, https://www.wassenaar.org/the-wassenaar-arrangement/.
282. Ferguson and Kerr, p. 8.
283. Arms Control Association, *The Australia Group at a Glance*, January 2018 https://www.armscontrol.org/factsheets/australiagroup.
284. Debevois and Plimpton, *Foreign Direct Investment Rules in Selected European Countries—An Overview*, p. 10.
285. Ibid.
286. Ibid.
287. Regulation (EU) 2019/452 Article 4(1)(a).
288. Regulation (EU) 2019/452 Article 4(1)(b).
289. Regulation (EU) 2019/452 Article 4(1)(c).
290. Regulation (EU) 2019/452 Article 4(1)(d).
291. Regulation (EU) 2019/452 Article 4(1)(e).
292. Debevois and Plimpton, *Foreign Direct Investment Rules in Selected European Countries—An Overview*, p. 10.
293. Dr. Thilo Steit & Dr. Ludger Giesberts, "Germany's New Foreign Direct Investments (FDI) Act took effect on 11 October 2020," Lexology (Oct. 19, 2020).
294. Ibid.
295. David Garrod, Sebastian Casselbrant-Multala, and Lennart Garritsen, *Foreign Investment: An overview of EU and national case law*, Concurrences, p. 4, January 10, 2020 https://www.akingump.com/a/web/113312/aokJC/e-competitions-special-issue-foreign-investment-4835-7933-3554.pdf.
296. Ibid.
297. Ibid.
298. Ibid.

299. Foreign Investment Review Board, Annual Report 2016-2017, May 8, 2018, p. 22 https://firb.gov.au/sites/firb.gov.au/files/2018/05/FIRB-16-17-Annual-Report.pdf
300. BBC News, "Australia blocks Ausgrid energy grid sale to Chinese companies," August 19, 2016 https://www.bbc.com/news/business-37129047.
301. Reuters Staff, "Australia says block on energy grid China sale based on new information," August 15, 2016 https://www.reuters.com/article/us-australia-privatisation-ausgrid/australia-says-block-on-energy-grid-china-sale-based-on-new-information-idUSKCN10Q299.
302. Ibid.
303. Foreign Investment Review Board, Annual Report 2017-2018, February 15, 2019, p. 24 https://firb.gov.au/sites/firb.gov.au/files/2019/02/FIRB-2017-18-Annual-Report-final.pdf
304. Foreign Investment Review Board, Annual Report 2018-2019, May 4, 2020, https://firb.gov.au/sites/firb.gov.au/files/2020-05/FIRB-AR-2018-19.pdf 19
305. Andrew Corkhill, "Treasurer uses FIRB powers to reject CKI's $13 billion bid for APA Group on 'national interest' grounds," Lexology, November 22, 2018 https://www.lexology.com/library/detail.aspx?g=44c3f322-9677-47c1-91d9-50e0f0e14167
306. Kirsty Needham and Scott Murdoch, "Australia shakes up foreign investment laws for national security, Reuters, June 4, 2020 https://www.reuters.com/article/us-australia-investment/australia-shakes-up-foreign-investment-laws-for-national-security-idUSKBN23C01J.
307. John Tivey, Nirangjan Nagarajah, Stephen Carlton, and Joshua Butler, "Australian foreign investment approval measures in response to COVID-19 and other recent Australian foreign investment approval developments," White & Case: Publications, May 21, 2020 https://www.whitecase.com/publications/alert/australian-foreign-investment-approval-measures-response-covid-19-and-other
308. Bogle et al., *Foreign Investment in Australia: What you need to know—COVID-19 Edition*, p. 31.
309. Ibid.
310. Ibid, p. 32.
311. Ibid.
312. Duncan Bedford, Emma Murray, Meg Morgan, and Andrew Bukowski, "FIRB Reforms Article Series—Part 6: Penalties and Enforcement," McCullough Robertson: News & Insights, August 27, 2020 https://www.mccullough.com.au/2020/08/27/firb-reforms-article-series-part-6-penalties-and-enforcement/
313. Ibid.

JINSA

The Jewish Institute for
National Security of America

1101 14th Street, NW | Suite 1030 | Washington, DC 20005 | www.jinsa.org