



SHIRA EFRON, KAREN SCHWINDT, EMILY HASKEL

Chinese Investment in Israeli Technology and Infrastructure

Security Implications for Israel and the
United States



For more information on this publication, visit www.rand.org/t/RR3176

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-1-9774-0435-0

Published by the RAND Corporation, Santa Monica, Calif.

© Copyright 2020 RAND Corporation

RAND® is a registered trademark.

Cover design: Rick Penn-Kraus

Limited Print and Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of its research documents for commercial use. For information on reprint and linking permissions, please visit www.rand.org/pubs/permissions.

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Support RAND

Make a tax-deductible charitable contribution at
www.rand.org/giving/contribute

www.rand.org

Preface

Relations between China and Israel have expanded rapidly since the early 2000s in numerous areas, including diplomacy, trade, investment, construction, educational partnerships, scientific cooperation, and tourism. Israel seeks to expand its diplomatic, economic, and strategic ties with the world's fastest-growing major economy and diversify its export markets and investments away from the United States and Europe. China seeks Israel's advanced technology and values Israel's location as part of the Belt and Road Initiative. In recent years, Chinese investments in Israel have grown substantially. They include investments in high-tech companies that produce sensitive technologies, as well as the construction and operation of key infrastructure projects. Chinese investment in sensitive technologies and construction of major Israeli infrastructure present distinct concerns for Israel and the United States.

This report, born out of a broader internally funded RAND Corporation study on Israeli-Chinese ties, includes an examination of the extent and nature of Chinese investments into Israeli technology and infrastructure and a review of the security implications these pose for Israel and the United States. It is an exploratory effort, rather than a comprehensive research endeavor, relying on unclassified and publicly available materials as well as interviews with over a dozen Israeli and U.S. current and former government officials, subject-matter experts, and business executives. We found that the primary concern regarding investment relates to Chinese ownership of companies that might possess sensitive technology or data; concerns over construction are focused on the use of infrastructure projects to further Chinese foreign

policy goals. The operation of infrastructure projects affords China unique surveillance opportunities and possibly economic and political levers of influence.

The report concludes with a set of open-ended questions that merit further investigation to better understand the magnitude of risks associated with growing Chinese investment in the Israeli market. It should be of interest to policymakers, analysts, and academic researchers studying Israel, U.S.-Israel relations, and China and that country's international relations.

This research was sponsored by the Office of the Secretary of Defense and conducted within the Cyber and Intelligence Policy Center of the RAND National Defense Research Institute (NDRI), a federally funded research and development center (FFRDC) sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community.

For more information on Cyber and Intelligence Policy Center, see www.rand.org/nsrd/ndri/centers/intel or contact the director (contact information is provided on the webpage).

Contents

Preface iii

Figures and Tables..... vii

Summary..... ix

Acknowledgments xxvii

Abbreviations..... xxix

CHAPTER ONE

Introduction 1

Evolution of Israeli-Chinese Defense Ties 2

Data Collection and Methods..... 5

Organization of this Report 7

CHAPTER TWO

China’s Outbound Investment Strategy 9

Background: Evolution of China’s Policy on Outbound Foreign
Investment 9

Chinese Technology Goals..... 12

How Israel Fits with China’s Policy Goals 17

CHAPTER THREE

Foreign Investment and Regulatory Policies in Israel 21

Why Engagement with China Is Attractive to Israel 21

Israeli Regulation on Foreign Investment..... 23

CHAPTER FOUR

Chinese Technology Investment and Construction in Israel..... 35

Overview of Chinese Investment and Construction Activity.....35

Chinese Entities 39

Israeli Companies 55

Conclusion.....62

CHAPTER FIVE

Security Risks for Israel and the United States 63

Government or Military Connections of Chinese Companies Doing
Business in Israel 63

Cyber and Intelligence Threats Arising from Chinese Investments and
Construction Activities.....66

Incompatibility Between Israeli and Chinese Interests in the
Middle East 73

Impact on the Israel-U.S. Relationship.....75

Conclusion.....79

CHAPTER SIX

Concluding Thoughts and Research Gaps for Further Study 81

Follow-On Questions 84

APPENDIX

Chinese Investments in Israel 87

References 101

Figures and Tables

Figures

4.1.	Known Chinese Investment in Israel, 2007–2018.....	37
4.2.	Aerial Image of the Ashdod Port Area	46
4.3.	Map of the Red Line of the Tel Aviv Rail Built by China Railway Tunnel Group.....	55
5.1.	China’s Dual-Use Ports	76

Tables

4.1.	Overview of Chinese Companies That Have Invested or Built Infrastructure in Israel.....	40
4.2.	Overview of Israeli Technology Deals.....	56
4.3.	Overview of Israeli Venture Capital Deals.....	59
A.1.	Chinese Investments in Israel	88

Summary

Bilateral ties between Israel and China began in 1950, but the two countries recently substantially expanded their relationship. China is interested in Israeli advanced technology, wants to learn from Israel's success in innovation, and considers Israel an important player within the Middle East and a useful node in China's ambitious Belt and Road Initiative (BRI)—China's vision to connect Europe, Asia, and Africa via land and sea. Israel, for its part, seeks to diversify its relationships beyond its traditional partners, the United States and Europe, and wants to benefit from enhanced ties with the world's fastest-growing major economy. Since 2013, Chinese companies have increasingly become more involved in Israel by purchasing Israeli companies and successfully bidding on key infrastructure construction projects. Such activity has been significant in the high-tech sector, in which Chinese investment of venture capital (VC) doubled from \$500 million in 2014 to \$1 billion in 2016. Israeli tech startups received Chinese investment of \$325 million in the first three quarters of 2018, up 37 percent from a year earlier.¹

This exploratory research is a deep dive into an issue—the security implications of Chinese investments in Israeli technology and infrastructure—raised in a 2018 RAND Corporation report on evolving Israeli-Chinese ties.² The analysis here benefitted from U.S. Depart-

¹ Reuters reported numbers assessed by the Israel Venture Capital Research Center; see “Israeli Minister Reassures U.S. over Chinese Telecoms Investment,” Reuters, January 18, 2019.

² Shira Efron, Howard J. Shatz, Arthur Chan, Emily Haskel, Lyle J. Morris, and Andrew Scobell, *The Evolving Israel-China Relationship*, Santa Monica, Calif.: RAND Corporation, RR-2641-RC, 2019.

ment of Defense (DoD) research support funds, but it was not directed by the U.S. government and does not reflect its opinions.

This study was conducted with a mixed-method approach. We drew on academic literature and original reporting in Hebrew, Chinese, and English, as well as on open-source materials reporting on 92 investment and construction deals between 2007 and 2018. We also held off-the-record discussions with over a dozen Israeli and U.S. current and former government officials, subject-matter experts, and business executives.

We first examine China's outbound investment strategy, discuss how Israel fits within China's broader policy goals, consider how Israel benefits from increased economic engagement with China, and survey a range of Chinese investments in Israel. We then discuss potential risk to U.S. and Israeli interests from these investments, including broader security concerns, and conclude with some additional questions that warrant further investigation.

China's Outbound Investment Strategy

Although Chinese companies have their own economic motivations, their decisions to invest abroad are strongly influenced by China's policies, which incentivize investment in certain industries. Since 2000, Chinese policy on outbound foreign investment has shifted from restrictive to encouraging, particularly in sectors that China considers important for domestic development. The focus of China's overseas investment has shifted from energy, mining, and manufacturing to such high-tech industries as artificial intelligence (AI), robotics, and information and telecommunications technology.

In 2013, China announced the BRI, its key foreign policy strategy to increase engagement with countries in Asia, the Middle East, and Europe. The BRI centers on infrastructure construction projects in these countries and includes an important investment policy.

Chinese Technology Goals

China wants to become a world leader in cutting-edge technologies, both for commercial and military purposes, and has myriad national plans intended to spur the development of its technology sector, including the National Long- and Medium-Term Plan for Science and Technology Development (2006–2020), Made in China 2025 (MIC 2025), and Internet Plus. The Chinese government also issues various industry-specific plans, such as the Next-Generation Artificial Intelligence Development Plan, released in July 2017.

MIC 2025, issued by the State Council in May 2015, provides a roadmap for turning China into a global leader in high-tech manufacturing. The plan names ten sectors that are priorities for development, including new-generation information technology, high-end numerical control machinery and robotics, and maritime engineering equipment and high-tech shipping.³ MIC 2025 also encourages deeper civil-military integration in science and technology development and promotes the development of dual-use technologies.⁴

How Israel Fits in with China's Policy Goals

Compared with other countries that receive Chinese investment, Israel is unique, as it aligns with the BRI as well as with Chinese goals to improve its domestic high-tech sector. This combination means that the Chinese government incentivizes companies to engage in both construction and technology investments in Israel. Moreover, engagement with Israel advances China's broader, long-term goals of increasing its presence and role in the Middle East and connecting to Europe.

The BRI is a major part of China's push in the Middle East, where China seeks to sustain friendships with all governments in the region,

³ State Council, 中国制造2025 [Made in China 2025], May 8, 2015a, Section 3(6). The other seven priority sectors are aviation and aerospace equipment, advanced rail transport equipment, energy-saving and new energy vehicles, electrical equipment, agricultural machinery and equipment, new materials, and biomedical and high-performance medical equipment.

⁴ State Council, 2015a, Sections 2(1), 3(1), and 3(3).

including those of Iran, Saudi Arabia, the Palestinian Authority, and Israel. Improved ties with Israel can serve to offset China's historically closer ties with other countries in the region, including Iran and Israel's Arab neighbors; these ties are primarily motivated by China's energy dependence. Israel has the potential to be a small but important stop on the 21st Century Maritime Silk Road, connecting the Indian Ocean and the Mediterranean Sea through the Gulf of Suez. The construction of a new port in Ashdod by a Chinese company, and the possible construction of a railway line from Eilat to Ashdod (pending approval by the Israeli government) by another Chinese engineering firm, serve as prime examples of such architecture. In addition, construction in Israel might act as a springboard to help Chinese infrastructure companies enter European or U.S. markets.

On the technology front, Israel is particularly attractive for Chinese investment because of its reputation as a “start-up nation.” China views Israel as a model for quickly creating an innovation hub, which matches well with China's goal of developing its own indigenous innovation capabilities.⁵ Moreover, Chinese investors face fewer barriers in Israel compared with markets in the United States and other advanced economies, helping Chinese companies diversify their investments.

Foreign Investment and Regulatory Policies in Israel

Foreign investments in Israel's technology sector are not new, but such investments have recently started drawing more attention because of increased investment in assets that are considered “vital” to the nation's security,⁶ particularly in the absence of a comprehensive and trans-

⁵ Conversation with manager at an Israeli VC company, October 2017; Fan Jida, 以色列如何成为创新驱动型国家 [“How Israel Became an Innovation-Driven Nation”], *Journal of Theory Guidance*, December 2016.

⁶ The term “vital infrastructure” alludes to infrastructure that if damaged, could lead to substantial economic, social and environmental losses and even lead to casualties. Such infrastructures also regularly serve the military and thus any damage to them means strategic damage to national security. See Eldar Haber and Tal Zarsky, “Protecting Critical Infrastructure from Cyberattacks [Hebrew],” *Mishpat U'Mimshal*, 2017.

parent mechanism for screening foreign investments in the country.⁷ Since 2013, the government of Prime Minister Benjamin Netanyahu has been eager to expand ties with China and has openly welcomed Chinese infrastructure projects. The key motivation is to expand Israel's diplomatic and economic relations with the world's fastest-growing major economy and diversify its export markets and sources of investments away from its traditional partners: the United States and Europe. Government Resolution 251 in 2013 called for expanding Israeli-Chinese cooperation,⁸ and it was quickly followed by additional government directives, including incentives for different ministries to cooperate with Chinese companies.⁹ While not the focus of this report, clearly, economic ties with China offer Israel important opportunities.

Increased Chinese activity in Israel has been enabled by a relatively permissive investment environment that only regulates foreign investment in Israeli companies that produce strictly military or dual-use goods and services; however, the line between purely civilian and dual-use technologies is becoming increasingly blurry, especially in such areas as cyber technologies. Regulation of commercial entities has generally focused on financial aspects, not political or security concerns. Until early 2020, Israel had not had an overarching mandated review mechanism similar to the U.S. Committee on Foreign Investment in the United States (CFIUS), which reviews the acquisition of U.S. companies by foreign entities to screen for potential threats to national security. On October 30, 2019, the Israeli cabinet announced that it would form a new advisory committee panel that would help screen foreign investments in the country; the committee supposedly began working in January 2020.¹⁰ This is a step in the right direction.

⁷ On October 30, 2019, the Israeli cabinet announced that it would set up a new advisory committee panel to help screen foreign investments in the country. However, at the time of writing, it is unclear how this decision is being implemented and how effective the committee will be.

⁸ Prime Minister's Office, Government Decision #251, "Strengthening Economic Cooperation with China [Hebrew]," May 19, 2013.

⁹ Prime Minister Office's, Government Decision #251, 2013.

¹⁰ Prime Minister's Office, "Security Cabinet Statement," press release, October 30, 2019.

However, based on the few details in the announcement, the committee will likely have legal and structural challenges. In practice, the committee might not fundamentally change the regulation environment.¹¹ The committee was established by a caretaker government; although a future government is unlikely to dissolve the committee, it is not fully established through legislation, and proper implementation could take time.

In addition, the Israeli committee is not as far-ranging as the U.S. CFIUS.¹² Per the 2018 Foreign Investment Risk Review Modernization Act (FIRRMA),¹³ CFIUS might now review transactions related to various technologies that are defined as “critical, emerging and foundational.”¹⁴ Including biotechnology; artificial intelligence (AI) and machine learning technology; position, navigation, and timing technology; data analytics technology; robotics; and microprocessors.¹⁵ Most of the Chinese investments in Israel in the last decade were in areas that FIRRMA covers, yet these areas are not included in the new committee’s areas of responsibility, which exclude the tech sector.¹⁶

In designing the committee, the Israeli government sought to “find the appropriate balance between the need to encourage foreign investments in Israel and ensure continued economic prosperity, and

¹¹ According to a U.S. official, the committee “will likely change nothing” (telephone conversation, November 15, 2019).

¹² Doron Ella, “A Regulatory Mechanism to Oversee Foreign Investment in Israel: Security Ramifications,” Institute for National Security Studies, Insight No. 1229, November 19, 2019b.

¹³ Public Law 115-232, Foreign Investment Risk Review Modernization Act, August 13, 2018; White and Case, “CFIUS Reform Becomes Law: What FIRRMA Means for Industry,” August 13, 2018.

¹⁴ U.S. Department of the Treasury, Office of Public Affairs, “Fact Sheet: Proposed CFIUS Regulations to Implement FIRRMA,” September 17, 2019.

¹⁵ White and Case, “Department of Commerce Review of Export Controls on Emerging Technologies,” November 28, 2018b.

¹⁶ Doron Ella, “Regulation of Foreign Investments and Acquisitions: China as a Case Study,” in Assaf Orion and Galia Lavi, eds., *Israel-China Relations: Opportunities and Challenges*, Tel Aviv: Institute for National Security Studies, August 2019a.

considerations of national security.”¹⁷ The decision followed months of deliberations during which different actors espoused different opinions on the issue. Economists and business-minded stakeholders contended that the Israeli business environment was already cumbersome and that a screening mechanism that is clearly focused on China would upset Beijing, cool diplomatic ties, and scuttle Chinese investment in Israel; security-minded Israeli stakeholders were pushing for more draconian regulations to mitigate risks. It is too early to fully assess the effectiveness of the new committee; however, given its narrow mandate and uncertain future, Israel’s screening of foreign investments could remain lacking in the near future.

Chinese Investment and Construction in Israel

Chinese companies have been increasingly active in Israel in terms of both investment and construction. We utilized and expanded upon a dataset of 92 business deals in Israel by Chinese companies between 2011 and 2018 (87 investments and five construction projects).¹⁸ 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). This list is not necessarily exhaustive, as data on Chinese investment in Israel are not collected systematically.

We examined the key Chinese companies known to have invested in Israeli technology or to have built infrastructure in Israel during this time period, and identified 11 that raise potential concerns for Israel or the United States. These concerns include connections with the Chinese military or government; issues related to security, privacy, and censorship; and business activities involving Israel’s adversaries, such as Iran. A key concern is the nature of the ties that Chinese companies investing or building major infrastructure projects in Israel have with Chinese

¹⁷ Prime Minister’s Office, 2019.

¹⁸ Ella, 2019a.

government or military entities, particularly if a company has ties to military intelligence or to Chinese operations in the South China Sea.

We found that Chinese companies, all of which are state-owned, have been involved in building and operating four major infrastructure projects in Israel; these projects are worth more than \$4 billion in total. All four projects are related to transportation infrastructure: the expansion of the Ashdod port, partial construction and operation of a new terminal by the Haifa port, construction and operation of the Tel Aviv light rail, and the digging of the Carmel Tunnels (road tunnels in Haifa).¹⁹ In addition, we examined the proposed rail line between Eilat and the Mediterranean, which, if approved, would likely be completed by a Chinese state-owned enterprise at an estimated cost of a little less than \$2 billion.²⁰ Of the Chinese companies working on these infrastructure projects, China Communications Construction Company and its subsidiaries, including the China Harbor Engineering Company, are noteworthy for having completed work for the Chinese armed forces.

Among the Chinese technology companies investing in Israel, telecommunications companies Huawei Technologies and ZTE Corporation have come under significant scrutiny in the United States for their less-than-transparent connections to the Chinese government and military. Other potential concerns include other Chinese companies receiving direct support from the government to develop dual-use technologies and company executives holding government positions or having personal connections with high-ranking officials or their relations (“princelings”). Security vulnerabilities have also been identified in the products of many Chinese technology companies investing in Israel.

¹⁹ Avi Bar-Eli, “Carmelton, Chinese Firm Reach Compromise on Tunnels Project,” *Haaretz*, November 3, 2008; Amiram Barkat, “Eilat Railway Hits Financing Buffer,” *Globes*, May 21, 2014; Angela Yu, “Chinese Port Operator Signs Deal to Run Israel’s Haifa Port,” *JOC.com*, June 2, 2015; David Shamah, “China Firm to Build New Ashdod ‘Union Buster’ Port,” *Times of Israel*, September 23, 2014; Hedy Cohen, “Arison, Chinese Co Win TA Light Rail Underground Tender,” *Globes*, May 19, 2015; China Railway Construction Corporation Ltd., “CCECC Signes [sic] Israel’s First Light Rail Operation Maintenance Contract,” November 16, 2017.

²⁰ Barkat, 2014.

Some Chinese companies investing or building infrastructure in Israel also conduct business with Israel's adversaries, such as Iran. Although companies from other countries that Israel does business with might also work in Iran, many Chinese companies active in Israel are state-owned and thus are heavily influenced by China's overall strategic goals rather than purely by business motivations. Of the 33 Chinese companies we examined, ZTE and China Railway Tunnel Group are known to have conducted business in Iran.

Through VC or other tools, Chinese investment in Israeli companies that develop sensitive, dual-use, or "emerging" technologies might also present security risks for either Israel or the United States. Chinese investment in companies developing semiconductors, AI, satellite communications, and other such products raises concerns about the potential for transfers of sensitive technology. In addition, China's weak enforcement of intellectual property (IP) rights means that Israeli companies could suffer theft of their IP, and even that Israel could lose its competitive advantage in the technology industry.

Security Risks for Israel and the United States

We took a closer look at four categories of security risks for Israel and the United States.

Government or Military Connections of Chinese Companies Doing Business in Israel

Most Chinese companies are linked with the Chinese government, the People's Liberation Army (PLA), Chinese princelings,²¹ or the Chinese Communist Party. The close relationship between Chinese companies and the state suggests that commercial activities are not motivated solely by economic considerations but also by China's strategic motivations. Official Chinese involvement in business operations allows

²¹ The term "princelings" refers to relations, particularly descendants, of high-ranking former Chinese Communist Party officials. Princelings are often perceived to receive preferential treatment from this status. Many princelings also hold high-level positions in government or business.

China to leverage its economic power to advance its geostrategic interests. China has also been able to affect the behaviors of private, non-Chinese companies.

China has developed its own network of lobbyists to do its bidding and has placed a number of Israeli individuals to encourage sales to China or to advocate for policies or tenders on China's behalf. One former Israeli official stated that Israel might be cautious to express criticism of China or discuss the potential threat posed by China to Israel's security, because the high-level political support for the Israel-China relationship comes directly from the prime minister's office.²²

Cyber and Intelligence Threats Arising from Chinese Investments and Construction Activities

Although the Israeli technology sector is mostly oriented westward, Chinese investment in technologies, including sensitive ones, and the construction and operation of key infrastructure present a number of cyber- and intelligence-related potential problems for both Israel and the United States. A key issue concerns China's interest in acquiring technologies that can be used for both commercial and military purposes. Through MIC 2025, the Chinese government has created both a strategy and a roadmap to help guide China toward the development of dual-use technologies and the two-way transfer of technology between the military and civilian sectors.²³ Although Israel regulates exports of dual-use technologies, it does not regulate exports and foreign investments in technologies that are considered purely commercial—but it is becoming increasingly hard to distinguish between technologies that can be considered commercial and those that are clearly of dual-use nature.²⁴ Based on FIRMA's list of emerging and foundational technologies, it is clear that the dual-use definition that Israel adheres to is simply too narrow in today's world, as it does not account for the dual uses of the future.²⁵

²² Conversation with a former Israeli official, Tel Aviv, October 22, 2018.

²³ State Council, 2015, Sections 2(1), 3(1), and 3(3).

²⁴ Conversation with an Israeli official, Tel Aviv, October 23, 2019.

²⁵ Conversation with a U.S. official, October 30, 2019.

Cyber espionage is another chief risk. According to the National Counterintelligence and Security Center (NCSC), China, along with Russia and Iran, is the most active foreign power engaged in the illegal acquisition of U.S. technology.²⁶ China's investment in Israeli cybersecurity companies creates risks for Israel and the DoD; the transfer of proprietary information used to develop these cybersecurity capabilities might be either used by China to bolster its own cyber defenses or reverse-engineered to identify software vulnerabilities. Additionally, China's human intelligence-gathering efforts certainly aid in the identification of desirable technologies and information, and these efforts likely will grow as China sends more personnel abroad to oversee and take part in construction projects and investments, as well as more students and academics.²⁷

Chinese investment and construction activities also create numerous opportunities for cyber-enabled and open-source intelligence collection. For example, the Shanghai International Port Group has secured a contract to operate a new terminal port next to the port of Haifa for 25 years, beginning in 2021. The physical location of Chinese construction workers and operators, combined with the possible ability of Chinese companies to exploit weaknesses regarding use of domestically sourced communications equipment and access to sensitive sites like industrial control systems, might provide Chinese workers with high levels of access to potentially sensitive commercial or military information. The port contract is accompanied by a classified appendix that includes limitations on the Chinese operator and workers and specifies what types of data, and via which means, are to be shared with Israel's General Security Service (the Shin Bet);²⁸ however, experts we

²⁶ NCSC, *Foreign Economic Espionage in Cyberspace*, Washington, D.C., 2018.

²⁷ Israeli Council for Higher Education, "Academic Cooperation with China and India—General Information," webpage, undated; Sarah Levi, "Chinese Enrollment at Israeli Universities Skyrockets," *Jerusalem Post*, August 14, 2017.

²⁸ Parts of the security appendix were shared with the authors. The appendix includes several directives including that personnel in certain roles will be Israeli nationals holding security clearances; that the operator has to comply with instructions of any authorized authority, including the Israel Defense Forces, the General Security Services (Shin Bet), the Israeli Police, the Home Front Command, and the Fire Department; and that the Shin Bet

spoke with admit there are risks and question the ability to enforce all these limitations in practice.²⁹

China might also use various forms of cyber and electronic collection to gain information about Israeli and U.S. commercial and naval operations. According to the NCSC, “China uses front companies to obscure the hand of the Chinese government.”³⁰ Chinese intelligence services, using connections to state-owned construction companies, could insinuate themselves into these companies’ operations and use their access to conduct espionage. For example, when a U.S. Navy ship comes into port, China might be able to identify its electronic warfare capabilities, what signatures the ship is emitting, or what kinds of radars are on board. There are numerous ways an adversary could hack into naval vessels and port infrastructure, including inserting USB drives loaded with malicious software, infecting diagnostic and maintenance equipment with malicious software, and installing network equipment to provide direct, persistent remote access. Of course, an adversary does not necessarily need to control a port to conduct such nefarious activities, as there are other means to hack into maritime vessels and insert malicious hardware into infrastructure; however, operating a port provides additional and beneficial opportunities.

Incompatibility Between Israeli and Chinese Interests in the Middle East

Despite the positive views of the China-Israel relationship within both commercial industries and government, Israel faces the potential for conflict in its relations with China because of the incompatibility between the countries’ interests in the Middle East. China’s coupling of its economic levers with geostrategic interests could have dangerous implications for Israel for two reasons. First, China’s positions and priorities in the Middle East are often contradictory to Israel’s, especially

will receive data on people and goods and have the ability to connect to systems that monitor and track movement by people and goods.

²⁹ Conversations with former defense official, an Israeli expert on China, and an Israeli cyber expert, October 20–21, 2018.

³⁰ NCSC, 2018.

China's close ties with Iran. Second, given the trade war between the United States and China, Israel could risk finding itself on opposing sides with Washington—its most important security, diplomatic, and economic patron.

In addition, Chinese companies have access to immense financial resources provided by the government, and could crowd out non-Chinese competitors without such access, increasing the risk for substantial concentration of assets in the hands of Chinese entities at the expense of local and other foreign businesses.

Effect on the Israel-U.S. Relationship

In addition to cyber and intelligence threats and traditional “hard power” concerns, China appears to be using its investment and other “soft power” activities to help achieve its economic, political, and security goals throughout the world, with important implications for the United States. From a geostrategic perspective, Chinese investment activities in Israeli infrastructure, including such vital infrastructure as ports and rail, is of concern to some experts in both Israel and the United States. Haifa port is the largest of Israel's three ports, the base for Israel's submarines, and a strategic port of call for the U.S. Navy's 6th Fleet. The U.S. Navy 6th Fleet docks at least once a year at Haifa port to participate in a biennial naval exercise and to support ballistic missile defense (BMD).³¹ At any given time, there is always a U.S. ship in or near the eastern Mediterranean to bolster Israel's land-based ballistic missile defenses by providing sea-based BMD support. For that reason, some argue that the Haifa port has become an emotional and contentious issue between Israel and the United States.³² However, there could also be actual risks. If—and that is an open question—a Chinese presence in port affords China unique information collection capabilities, the United States might need to balance its interests in the

³¹ U.S. Navy, “NMCB 11 Prepares for Juniper Cobra 18 in Israel,” press release, March 12, 2018.

³² Discussion with U.S. naval expert, by phone, September 14, 2019.

area with its concern about Chinese collection on U.S. military operations and possible cyber risks to naval ships.³³

The Haifa port issue has attracted most press and become a symbol of the tension between Israel and the United States over Israel's ties with China. However, the United States is more concerned about Chinese investment in Israeli technology. The United States is worried about transfers of U.S. technology or about any technologies that give China a military and economic edge. In recent years, former and current security officials, as well as several lawmakers in Israel, have expressed concerns about taking money from China, fearing that doing so would impact relations with the United States.³⁴ Israel relies on the United States for security, economic ties, and geopolitical assistance, and the China-U.S. relationship has grown increasingly tense in recent years. Since early 2019, U.S. officials have warned Israel publicly about its connections with China. Israeli press reported that during their March 2019 meeting, U.S. President Donald Trump told Israeli Prime Minister Benjamin Netanyahu that unless Israel limits its ties with Beijing, the U.S.–Israeli security relationship could be impaired.³⁵ The same month, U.S. Secretary of State Mike Pompeo said that continued Chinese investment in Israel could hamper intelligence sharing between Israel and the United States.³⁶ This U.S. pressure resulted in the establishment of the foreign investment screening mechanism announced in October 2019. However, given the presumable limitations of the committee, tensions with the United States over this issue

³³ Conversation with U.S. naval warfare expert, California, September 19, 2018.

³⁴ Multiple discussions with former Israeli officials, Tel Aviv, October 21–23, 2018; see also Ben Caspit, “Does China Endanger Israel’s Security?” *Al-Monitor*, January 11, 2019; and Yossi Melman, “Cause for Concern? Chinese Investment and Israel’s National Security,” *Jerusalem Post*, April 7, 2018.

³⁵ Barak Ravid, “Trump Le’Netanyahu: Tsanen Ha’Keshet Im Sin o She’Hayachasim Imanu Alolim Lehipaga [Trump to Netanyahu: Cool Down Connection With China Otherwise Our Ties Could Cool Down],” *Channel 13*, April 4, 2019.

³⁶ “Pompeo Warns U.S. Could Curb Security Ties with Israel over China Relations,” *Times of Israel*, March 21, 2019.

might continue,³⁷ indicating that Israel needs to play a balancing act as it moves its relations with China forward.

Conclusion

As Israel continues its economic engagement with China, Chinese investment activities will likely continue to have security repercussions, including across multiple facets of the U.S.-Israel-China relationship. Israel might be able to take specific and appropriate actions to mitigate the potential threats of doing business with China.

Follow-On Questions

This study has identified five areas that warrant additional research. We summarize a few of these here:

- **The first issue relates to assessment of the security risks to both Israel and the United States that are associated with Chinese penetration into Israel.** Data on Chinese investments in Israeli technology and infrastructure are not systematically collected, and further research is needed to capture the full extent of Chinese access, including bids in which Chinese companies are presently competing. Such data collection should extend into the classified domain to allow better analysis of pending questions. For example, what type of risks are borne out of Chinese presence in the new Bayport terminal in Haifa versus Chinese agents watching the port from a nearby location or from other instances where U.S. and Chinese maritime vessels interact at sea? Could China obtain technology from Israel that it cannot obtain from other countries, and what risks could these technologies pose to U.S. economic and security interests? More generally, once data are available, does China's investment in Israel help Beijing achieve its broader outbound investment strategic objectives?

³⁷ Conversation with U.S. State Department official, October 30, 2019.

- **A second area for further investigation relates to the effectiveness of existing regulatory bodies that monitor foreign investment and acquisition of sensitive or future dual-use technologies.** From the U.S. perspective, how effective are existing U.S. laws and procedures regarding foreign investment if China is able to acquire similar technologies or capabilities from countries such as Israel, which have regulatory mechanisms that are not as robust or as strict? Could alternative regulatory models or structures mitigate China's acquisition of sensitive technologies more effectively than CFIUS? What lessons can the United States learn from other countries' oversight mechanisms to better protect U.S. and allied interests, including those of Israel? Further investigation is needed into the mechanism that Israel has decided to create in late October 2019 and how effective it will likely be.
- **A third set of questions relates to U.S. security and defense interests in the Middle East.** How might China exercise its increasing social and political influence in Israel, both in the short and long term, and what implications would this have for the United States? How does China's presence affect BMD as a strategic resource for the United States? From a geostrategic perspective, how might China's presence in the Middle East affect other countries vying for influence throughout the region—primarily Russia and Iran? And how does China's presence in and operation of the civilian port in Haifa and Ashdod affects U.S. risk assessments, including counterintelligence risk?
- **The fourth issue relates to the threat of the transfer of sensitive, including emerging and foundational, civilian technologies and dual-use capabilities to China.** What exactly is the nature of the threat to the United States posed by Chinese acquisition of such technologies from U.S. allies, including, but not limited to, Israel? Which specific technologies provide the greatest advances to China's military capabilities or otherwise pose a threat to U.S. interests and security? How can the United States effectively communicate to its partners its concerns regarding Chinese investments in such technologies? If other U.S. allies share U.S. concerns about Chinese investments in technology and vital

or critical infrastructure, what existing mechanisms or oversight bodies can the United States and its partners use to create a comprehensive, partner-oriented response to these shared concerns? What kind of collaborations in the areas of technology and innovation can the United States develop with its allies to better prepare in those areas?

- **The final issue is what types of security risks are associated with growing Israeli-Chinese academic cooperation and the increase in the number of Chinese students in Israel.** In what areas do Israeli and Chinese academics collaborate? What do these partnerships entail? Will more academics and students be used as human intelligence to aid China's efforts to identify desirable technologies and sensitive information? Could deeper academic cooperation increase knowledge transfer from Israel to China—against Israeli and U.S. interests? Could enhanced Israeli-Chinese academic collaboration undermine Israeli-U.S. cooperation?

Acknowledgments

The authors thank our formal peer reviewers Courtney Weinbaum and Larry Hanauer, who provided instrumental feedback on this report. In addition, we thank the many individuals who helped enhance our understating of the nature of Chinese investments into Israeli technology and infrastructure and their security implications, including Doron Ella, Brig. Gen. (ret.) Assaf Orion, and Galia Lavi of the Institute for National Security Studies, Yoram Evron, assistant professor and head of the Business in Asia program at the University of Haifa, and the former and current U.S. and Israeli officials and experts who chose to remain anonymous.

We also thank the RAND Corporation's Cyber and Intelligence Policy Center for funding this study, especially director Richard Girven, associate director Sina Beaghley, and former acting associate director Javed Ali for supporting this project.

Abbreviations

AI	artificial intelligence
BMD	ballistic missile defense
BRI	Belt and Road Initiative
CBC	China Broadband Capital Partners
CCCC	China Communications Construction Company
CEO	chief executive officer
CFIUS	Committee on Foreign Investment in the United States
CHEC	China Harbor Engineering Company
FIRRMA	Foreign Investment Risk Review Modernization Act
IDF	Israel Defense Forces
INSS	Institute for National Security Studies
IP	intellectual property
IT	information technology
MIC 2025	Made in China 2025
MOD	Ministry of Defense
MOFCOM	State Council and Ministry of Commerce
NCSC	National Counterintelligence and Security Center

NDRC	National Development and Reform Commission
NEC	National Economic Council
NPC	National People's Congress
NSC	National Security Council
PLA	People's Liberation Army
PLAAF	People's Liberation Army Air Force
PMEC	Pan-Mediterranean Engineering
UAV	unmanned aerial vehicle
VC	venture capital

Introduction

Bilateral ties between Israel and China began in 1950, but recently the two countries have substantially expanded their relationship. China is interested in Israeli advanced technology, wants to learn from Israel's success in innovation, and considers Israel an important player within the Middle East and a useful node in its ambitious Belt and Road Initiative (BRI)—China's attempt to connect Eurasia and Africa via land and sea. Israel seeks to diversify its relationships beyond its traditional partners, the United States and Europe, and wants to benefit from enhanced ties with the world's fastest-growing major economy.

Since 2013, Chinese companies have become increasingly involved in purchasing Israeli companies and successfully bidding on construction projects for key Israeli infrastructure. Such activity has been significant in the high-tech sector. Chinese venture capital (VC) investment in the Israeli high-tech sector increased from \$500 million in 2014 to \$1 billion in 2016.¹ Chinese investment in Israeli tech start-ups was \$325 million in the first three quarters of 2018, up 37 percent from a year earlier.²

¹ Ferry Biedermann, "China Is Increasingly Becoming Key for Israel's High-Tech Industry," *CNBC*, July 18, 2017.

² Reuters reported numbers assessed by the Israel Venture Capital Research Center; see "Israeli Minister Reassures U.S. over Chinese Telecoms Investment," Reuters, January 18, 2019.

This report, which was born out of a comprehensive RAND Corporation assessment of Israeli-Chinese ties,³ analyzes the security implications of Chinese investments in Israeli technology and infrastructure. Although economic ties with China offer Israel important opportunities, these are outside of the scope of this study. As we will explain in detail in this report, Chinese investment in these sectors could lead to friction between Israel and the United States. In addition, Chinese investment in Israeli technology companies and in VC firms investing in dual-use and other sensitive technologies, as well as Chinese involvement in building and operating strategic infrastructure, could be used for surveillance and intelligence purposes, raising important security concerns for both Israel and the United States.⁴

In the remainder of this introduction, we briefly describe the evolution of Israeli-Chinese defense ties and discuss the approach used in this study.

Evolution of Israeli-Chinese Defense Ties

Israel was the first country in the Middle East to recognize the People's Republic of China in January 1950. Still, the two countries were divided by the Cold War and pressured by different parties—Israel by the United States and China by the Arab countries—which hindered the establishment of formal diplomatic relations until 1992.⁵ However, even without open ties, in 1979, Israel and China began secret contacts; these mostly involved the transfer of defense technology from Israel to China.⁶ Over the next two decades, more than 60 military technol-

³ Shira Efron, Howard J. Shatz, Arthur Chan, Emily Haskel, Lyle J. Morris, and Andrew Scobell, *The Evolving Israel-China Relationship*. Santa Monica, Calif.: RAND Corporation, RR-2641-RC, 2019.

⁴ “Too Open for Business? Israel’s Ties with China Are Raising Security Concerns,” *The Economist*, October 11, 2018.

⁵ Yitzhak Shichor, “Hide and Seek: Sino-Israeli Relations in Perspective,” *Israel Affairs*, Vol. 1, No. 2, 1994, pp. 188–208.

⁶ Yaakov Katz and Amir Bohbot, “How Israel Used Weapons and Technology to Become an Ally of China,” *Newsweek*, May 11, 2017.

ogy transactions between Israel and China occurred, totaling \$1–2 billion. These transfers allegedly included technology to upgrade Chinese tanks, night vision systems, electronic warfare systems, Python-3 air-to-air missiles, fighter aircraft technology, unmanned aerial vehicle technology, and more.⁷

However, the United States continued to exert influence on Israeli ties with China. The relationship suffered two major blows in the late 1990s and early 2000s as a result of U.S. objection to such transactions. In 1999, the United States opposed the sale of the PHALCON advanced airborne radar system on surveillance planes to the People's Liberation Army Air Force (PLAAF).⁸ This opposition stemmed from worries that such early warning capabilities would enable China to gain greater control of airspace in the event of conflict.⁹ The U.S. government worked to block the sale, arguing that the PHALCON employed U.S.-origin technology, which would require U.S. permission to re-export to China.¹⁰ Israel tried to lobby Congress directly for permission to export the technology to China, but that strategy failed, and Israel was forced to cancel the deal.¹¹ Israel compensated China at \$350 million in damages, including repayment of \$190 million that China had

⁷ Yoram Evron, "Between Beijing and Washington: Israel's Technology Transfers to China," *Journal of East Asian Studies*, Vol. 13, No. 3, December 2013, pp. 503–528.

⁸ P. R. Kumaraswamy, "Israel-China Relations and the Phalcon Controversy," *Middle East Policy*, Vol. 12, No. 2, Winter 1996, pp. 93–103. It is worth noting that even before the PHALCON sale, Israel's transfer of defense technologies to China created tension in its relationship with the United States. The United States alleged that Israel transferred Patriot missile technology to China without U.S. approval, and it further alleged that Israel transferred U.S.-origin technology that was used in Israel's U.S.-funded Lavi fighter jet.

⁹ Suzanne Goldenberg, "Israel and US Clash over Spy Plane Sale to China," *The Guardian*, April 9, 2000; conversation with former U.S. official who worked on defense issues related to Israel in the late 1990s and early 2000s, August 2017.

¹⁰ Conversation with former U.S. official, August 2017. Despite the U.S. claim, Israeli officials contend to this day that the technology was originated in Israel. See No Man's Land, "Ha'Kiboosh Ha'Sini: Haim Hadirat Ha'Maatzama Ha'Sinit Le'Yisrael Sakana Bitchonit? [Chinese Occupation: Is the Penetration of the Chinese Superpower to Israel a Security Risk?]," *Kan 11*, March 11, 2019.

¹¹ Conversation with former U.S. official, August 2017.

paid in advance.¹² This incident led to greater U.S. scrutiny of and suspicion about Israeli transfers to third parties.¹³

In 2005, a second incident occurred after Israel agreed to upgrade HARPY unmanned aerial vehicles (UAVs) that it had sold to China a decade earlier.¹⁴ Washington accused Israel of deception¹⁵ and stopped cooperation with Israel on the F-35 joint strike fighter program. A former senior official at the U.S. National Security Council said that the HARPY incident put the “special relationship with Israel” at risk.¹⁶ Consequently, Israel not only cancelled the HARPY deal but also forced senior Ministry of Defense officials to resign and agree that all defense transfers and dual-use exports to China would be subject to U.S. approval.¹⁷ This essentially cut off Israel-China technology relations.¹⁸ In 2007, as a result of the HARPY crisis, Israel passed the Export Control Law, which placed further restrictions on exports of arms and dual-use technology.¹⁹

Although Israel has been extremely cautious not to sell military or what is defined explicitly as dual-use technology to China since 2005, a new area of concern has since emerged. In recent years, Chinese companies have increased their investments in Israeli high-tech companies and VC firms in the technology sector and have successfully bid on construction of infrastructure projects. This activity, as discussed in Chapter Five, could both create surveillance and intelli-

¹² Amnon Barzilai, “Israel, China Agree on Compensation for Cancelled Phalcon Deal,” *Haaretz*, March 13, 2002.

¹³ Conversation with former U.S. official, August 2017.

¹⁴ Ran Dagoni, “Harpy UAV Compromise with US: No Upgrades for China,” *Globes*, May 25, 2005.

¹⁵ Yitzhad Shichor, “The U.S. Factor in Israel’s Military Relations with China,” *China Brief*, Vol. 5, No. 12, May 24, 2005.

¹⁶ Conversation with a former U.S. National Security Council senior official, Washington, D.C., May 2017.

¹⁷ Evron, 2013.

¹⁸ Yoram Evron, “Israel’s Response to China’s Rise: A Dependent State’s Dilemma,” *Asian Survey*, Vol. 56, No. 2, March–April 2016, pp. 392–414.

¹⁹ Evron, 2013.

gence risks, as well as more broader security risks, and thus raises concerns among Israeli and U.S. security officials.²⁰ It also could stir up new tensions with the United States over investments in technologies that the United States would consider “emerging” and “foundational” and therefore merit further oversight.²¹ Other risks include connections between Chinese companies and the Chinese government; Chinese commercial activities might seek to advance China’s strategic motivations—which are not always aligned with Israel’s interests. There is also the risk of a foreign entity controlling infrastructure, including infrastructure that is vital to Israeli security.²² Chinese support for the Palestinians in international forums and links with Iran pose other diplomatic challenges,²³ as explained in Chapters Four and Five.

Data Collection and Methods

In this exploratory study, we used a mixed-method approach. First, we drew on academic literature (mostly about Israeli-Chinese ties)²⁴ and Israeli regulation of foreign investment. We also collected and analyzed original news and business reporting (in Hebrew, Chinese, and English) and examined analysis by other think tanks. We primarily focused our searches on reports from the last decade that provided insights into the evolution of Israeli-Chinese relations and U.S. response to these developing ties. We also briefly analyzed Chinese, Israeli, and U.S. official

²⁰ “Too Open for Business? Israel’s Ties with China Are Raising Security Concerns,” 2018.

²¹ The Foreign Investment Risk Review Modernization Act (FIRRMA), which Congress passed in August 2018 to reform the Committee on Foreign Investment in the United States (CFIUS) process, covers a wider variety of transactions, including investments that would give a foreign investor access to “sensitive” technologies. See Public Law 115-232, Foreign Investment Risk Review Modernization Act, August 13, 2018.

²² Yossi Melman, “Cause for Concern? Chinese Investment and Israel’s National Security,” *Jerusalem Post*, April 7, 2018.

²³ An official with the Israeli Ministry of Foreign Affairs explained that Israel does not anticipate China voting in its favor in the UN anytime soon (in Jerusalem, July 19, 2017).

²⁴ This report benefitted from an extensive literature review on this subject that was conducted while writing Efron et al., 2019.

government documents to better understand these countries' policies on different issues, including China's technology goals, Israel's regulatory frameworks, and the U.S. approach toward China. All information was derived from publicly available documents.

To gather information about Chinese investment in Israeli technology and infrastructure projects, we used open-source materials that reported on 92 such investment and construction deals between 2007 and 2018. This list, which is an expansion of a dataset developed primarily by Doron Ella of the Institute for National Security Studies (INSS), is not necessarily exhaustive, as data on Chinese investment in Israel are not collected systematically. We used multiple open-source materials, including U.S. government reports; data sets on investment and construction; websites of Chinese and Israeli companies; news articles; and technology and financial websites. We sorted through these data and characterized investment profiles. We identified a subset of Chinese companies that raise potential security concerns for Israel or the United States because of their links with the Chinese military or government; track record of problems related to security, privacy, or censorship; business activities with Iran; and implications of involvement in major infrastructure, including ports and rail adjacent to military bases. We also identified a subset of Israeli companies that received investment, concentrating on those that produce sensitive technology or that receive investments from Chinese companies that experts estimate to potentially pose security risks to Israel or the United States. Finally, we held off-the-record interviews with more than a dozen Israeli and U.S. current and former officials, subject-matter experts, and executives from the Israeli tech sector. Interviewees included relevant current and former officials and experts from both the United States and Israel in the areas of intelligence, cyber technology, business, and defense. Israeli experts represented by the interview population came from various governmental ministries and agencies, academia, think tanks, and VC organizations. Example U.S. organizations represented are the State Department, Congress (through congressional staff), the U.S. Navy, and think tanks. Off-the-record discussions with these experts provided insights into issues that are not often publicly discussed—for example, the challenges of enforcing regulation.

We recognize the limitations of these methods, particularly relying only on information in the public domain and holding discussions with a small, nonrepresentative group of experts, which could both limit the analysis and introduce bias. This was an exploratory effort rather than a comprehensive research endeavor. Our primary goals were to determine the key issues associated with Chinese investment in technology and involvement in infrastructure in Israel and identify questions that warrant further study.

Organization of this Report

Chapter Two examines Chinese policies on outbound investment and technology and explains how Israel fits in with China's broader policy goals. Chapter Three contains an explanation of how Israel benefits from increased economic engagement with China and briefly discusses Israeli regulations on foreign investments, including those involving China. Chapter Four provides an overview of Chinese investments in Israel from 2007 to 2018, as well as major construction projects undertaken by Chinese companies in Israel over the same time period. In addition, we discuss concerns presented by several Chinese technology companies investing in Israel, as well as Israeli technology companies that have received Chinese investments. We also elaborate on potential risks to U.S. and Israeli interests as they relate to specific companies, investments, and construction projects. Chapter Five analyzes broader concerns related to Chinese investment in Israel, focusing on (1) the relationship of Chinese companies to the Chinese government, military, Chinese "princelings," or the Chinese Communist Party;²⁵ (2) cyber and intelligence threats posed by Chinese investments and construction activities; (3) the risk that Israel's ties with China could undermine its ties with the United States; and (4) the incompatibility between Israel and China's interests in the Middle East. Chapter Six

²⁵ The term "princelings" refers to relations, particularly descendants, of high-ranking former Chinese Communist Party officials. Princelings are often perceived to receive preferential treatment from this status. Many princelings also hold high-level positions in government or business.

concludes the study and identifies outstanding questions that warrant additional research. An appendix provides more-specific information about Chinese investments in Israel.

China's Outbound Investment Strategy

Since 2000, Chinese policy on outbound foreign investment has shifted from restrictive to encouraging, particularly for sectors that China considers important for domestic development. During this period, the focus of China's overseas investment shifted from energy, mining, and manufacturing to such high-tech industries as artificial intelligence (AI), robotics, and information and telecommunications technology. In 2013, China announced the BRI, its key foreign policy strategy to increase engagement with countries in Asia, the Middle East, and Europe. The BRI emphasizes infrastructure construction projects in these countries and includes an important investment component.

To contextualize Chinese investment and construction activity in Israel, this chapter examines Chinese policies on outbound investment and technology. All research in this chapter comes from publicly available sources—primarily Chinese and U.S. government documents, journal articles and think tank analysis, and several conversations with experts. After discussing China's general policies, we look specifically at how Israel might fit into China's broader goals.

Background: Evolution of China's Policy on Outbound Foreign Investment

Beginning in the early 2000s, China started a policy known as "Going Out," which encouraged companies to pursue activities abroad. Although overseas investment was still highly regulated, prior approval from the State Council and Ministry of Commerce (MOFCOM) was

no longer required for all outbound direct investments, and additional policies followed in the coming decade that further loosened regulatory restrictions on overseas investment.¹ This policy shift was driven by the Chinese government's realization that investing abroad was needed to continue funding the country's high-paced growth, foster the competitiveness of Chinese businesses, and obtain resources that were not abundant domestically.² Before the implementation of the "Going Out" policy, outbound investment was primarily undertaken by state-owned enterprises; the shift in policy allowed larger numbers of private companies to seek higher returns by investing abroad. The advent of the "Going Out" era led to a huge surge in Chinese outbound investment, which increased from \$2.7 billion in 2002 to \$196.2 billion in 2016, with an average annual growth rate of 35.8 percent over the same period.³

¹ For more information on China's "Going Out" policy and other related policies regulating outbound investment, see Huang Wenbin and Andreas Wilkes, *Analysis of China's Overseas Investment Policies*, Bogor, Indonesia: Center for International Forestry Research, Working Paper 79, 2011; Karl P. Sauvants and Victor Z. Chen, "China's Regulatory Framework for Outward Foreign Direct Investment," *China Economic Journal*, Vol. 7, No. 1, 2014, pp. 141–163; Thilo Hanemann and Daniel H. Rosen, "Chinese Investment in the United States: Recent Trends and the Policy Agenda," *Rhodium Group*, December 9, 2016; 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. Although "Going Out" was announced in 2000, it was formalized in the 2004 State Council "Decision on Reforming the Investment Systems." Regulations on outbound investment were further loosened several times in the following decade by measures such as MOFCOM's 2009 Administrative Measures for Overseas Investment (revised in 2014), the National Development and Reform Commission's (NDRC) 2011 Notice on the Decentralization and Approval of Overseas Investment Projects, and NDRC's 2014 Measures for the Administration of Approval and Registration of Overseas Investment Projects. These policies simplified and decentralized approval processes, and by 2014 most investments only needed to be registered rather than approved. In 2016, the trend toward loosening investment regulations reversed: The Chinese government began to worry about currency depreciation and cracked down on what it described as "irrational investments" in real estate, hotels, and the entertainment industry. New measures were issued in late 2017 that restrict these investments, while still encouraging overseas investments in desired sectors.

² Hanemann and Rosen, 2016; Wenbin and Wilkes, 2011; Sauvants and Chen, 2014.

³ Bijun Wang and Kailin Gao, 2018.

In 2013, President Xi Jinping announced the BRI, a major foreign policy program to increase engagement and connectivity across Asia and the Middle East to Europe. Infrastructure construction projects in BRI countries, carried out by Chinese state-owned enterprises, are a cornerstone of the policy. Although the BRI is much broader than investment, it is a key initiative for Xi and is therefore reflected in various aspects of foreign policy, including investment policy. For example, the Guiding Opinions on Further Guiding and Regulating the Direction of Outbound Investment, issued in August 2017, specifically encourage investment projects that are conducive to BRI construction.⁴

The Guiding Opinions also urge outbound investment in certain sectors, especially in the high-tech and advanced manufacturing industries, and encourage the establishment of overseas research and development centers.⁵ For investments in priority areas, the Guiding Opinions stipulate that the government will provide preferential services in taxation, currency exchange, insurance, customs, and information services.⁶

Although Chinese companies have their own economic motivations, their decisions to invest abroad are strongly influenced by Chinese government policies, which incentivize investment in certain industries. According to a 2011 survey of Chinese firms (both private and state-owned), 55 percent of firms engaged in overseas investment identified the “Going Out” policy as an “important” or “very important” factor in their decisionmaking process (as important as “host country market size and potential” and more important than “host country legal system”).⁷

Moreover, it is worth noting that the distinction between Chinese state-owned enterprises and private companies has become increasingly

⁴ State Council, 关于进一步引导和规范境外投资方向的指导意见 [Guiding Opinions on Further Guiding and Regulating the Direction of Outbound Investment], August 4, 2017b.

⁵ State Council, 2017b.

⁶ For more information on some of the mechanisms through which the Chinese government provides support for overseas investment priorities, see Sauvants and Chen, 2014, section 2.1.2.

⁷ Sauvants and Chen, 2014.

blurred, meaning that the degree of state influence over private companies is unclear. According to a study of Chinese state capitalism, the ownership structure of a Chinese company “provides relatively little information about the degree of autonomy the firm enjoys from the state.”⁸ In one case, a member of the Chinese Political Consultative Conference, a legislative advisory body, noted that state-owned enterprises were increasingly encountering difficulties investing abroad and suggested that state-owned enterprises and private companies cooperate to “evade the risks of political approval in the foreign mergers and acquisitions process.”⁹ The security implications of the links between Chinese companies and the Chinese government are discussed further in Chapter Five.

Chinese Technology Goals

In addition to the economic benefit for Chinese companies and for China’s economy overall, overseas investment can also help China achieve its goals for its domestic technology sector. China wants to become a world leader in cutting-edge technologies, both for commercial and military purposes, and has myriad national plans intended to spur the development of its technology sector. Key plans and policies include the National Long- and Medium-Term Plan for Science and Technology Development (2006–2020), Made in China 2025 (MIC 2025), and Internet Plus. The Chinese government also issues various industry-specific plans, such as the Next-Generation Artificial Intelligence Development Plan, released in July 2017.

The main goal of the National Long- and Medium-Term Plan for Science and Technology Development is to develop China’s capabilities for indigenous innovation. According to a 2005 lecture by a

⁸ Curtis J. Milhaupt and Wentong Zheng, “Beyond Ownership: State Capitalism and the Chinese Firm,” *Georgetown Law Journal*, Vol. 103, No. 3, March 2015.

⁹ Sina Finance, 政协委员张宏伟: 建议海外能源投资方式多元化 [“Zhang Hongwei (CPPCC) Suggests Diversifying the Method of Overseas Investment on Energy”], March 8, 2010.

senior official in the Chinese Ministry of Science and Technology, the plan's major targets for 2020 include ensuring that China's advanced technologies come from indigenous innovation; reducing reliance on foreign technologies; making high-tech manufacturing and knowledge-based services the dominant industries of China's economy; and supporting several Chinese high-tech companies in becoming world-class innovators.¹⁰

The MIC 2025 and Internet Plus policies supplement this main science and technology plan, promoting innovation in the manufacturing and internet industries. MIC 2025, issued by the State Council in May 2015, provides a roadmap for turning China into a global leader in high-tech manufacturing. The plan names ten sectors that are priorities for development, including new-generation information technology, high-end numerical control machinery and robotics, and maritime engineering equipment and high-tech shipping.¹¹ MIC 2025 also encourages deeper civil-military integration in science and technology development and promotes the development of dual-use technologies, as well as the two-way transfer of technology between the military and civilian sectors.¹² The U.S. Chamber of Commerce notes that a key feature of MIC 2025 is preferential treatment and financial incentives for Chinese companies in these key sectors, in which the Chinese government seeks to "leverage China's legal and regulatory systems to favor domestic companies over foreign ones" and provide financing "that could substantially distort domestic and global markets."¹³

Shortly after unveiling MIC 2025, China also released an action plan for implementing Internet Plus. Internet Plus seeks to promote the

¹⁰ Shang Yong, "An Introduction to China's Science and Technology Policy," briefing delivered at the Kennedy School of Government, Cambridge, Mass., December 15th, 2005.

¹¹ State Council, 中国制造2025 [Made in China 2025], May 8, 2015a, Section 3(6). The other seven priority sectors are: aviation and aerospace equipment, advanced rail transport equipment, energy-saving and new energy vehicles, electrical equipment, agricultural machinery and equipment, new materials, and biomedical and high-performance medical equipment.

¹² State Council, 2015a, Sections 2(1), 3(1), and 3(3).

¹³ U.S. Chamber of Commerce, *Made in China 2025: Global Ambitions Built on Local Protections*, Washington, D.C., 2017.

integration of internet technologies—including next-generation mobile technologies, cloud computing, the internet of things, and robotics—into the manufacturing industry, as well as into such industries as agriculture, finance, and e-commerce.¹⁴ The policy also includes the goal of accelerating technological breakthroughs in AI, including cultivating companies and innovation teams to be global leaders in AI. Moreover, the action plan states that government agencies should encourage competitive internet companies to join companies in the manufacturing, financial, and information and communications sectors in “going out” through overseas acquisitions, joint ventures, and the establishment of subsidiaries.¹⁵

Industry-specific development plans follow the lead of the broader technology policies in setting targets for industry development, emphasizing indigenous innovation, and promoting development by looking abroad. For example, the Next-Generation Artificial Intelligence Development Plan has the goal of making China a world leader in AI by 2025, and encourages Chinese AI companies to “go out,” using such methods as overseas mergers and acquisitions, equity investments, VC, and the establishment of overseas research and development centers. Further risks associated with these policies are explained in more detail in Chapter Five.

How Overseas Investment Contributes to China’s Technology Goals

In addition to encouraging and incentivizing research and development domestically in these areas, both overt and covert technology transfer through overseas acquisitions and investment provides another means for China to accomplish its technology goals. The Mercator Institute for China Studies asserted in a 2016 report that Chinese companies are using overseas investments “to speed up China’s technological catch-up and to leapfrog stages of technological development,” which, although

¹⁴ State Council, 关于积极推进“互联网+”行动的指导意见 [“Guiding Opinions on Actively Advancing ‘Internet Plus’ Actions”], July 4, 2015b.

¹⁵ State Council, 2015b. The agencies specifically tasked with this item were the NDRC, the Ministry of Foreign Affairs, Ministry of Industry and Information Technology, MOFCOM, and the State Internet Information Office (also known as the Cyberspace Administration of China).

not problematic by itself, is objectionable because this activity is “partly supported and guided by the state” as part of “an overarching political” program that aims to “generate large-scale technology transfer.”¹⁶

The MIC 2025 policy includes an outward-looking component that promotes investment in advanced technologies. In 2016, as part of MIC 2025 implementation, the Ministry of Industry and Information Technology created three categories of “project library” and indicated that projects included in these libraries would be eligible for financial support. One of the categories was “industry and communications companies ‘Going Out’ projects,” and projects in this category would additionally be eligible for diplomatic support.¹⁷

The Rhodium Group, a research firm that monitors Chinese investments in the United States, cited the semiconductor industry as a clear example of “the nexus of industrial policy and outbound [foreign direct investment]” in China.¹⁸ Following the announcement of a new national policy encouraging the development of China’s domestic semiconductor industry, Chinese companies “embarked on an unprecedented buying spree of assets along the semiconductor supply chain in Asia, Europe, and North America.”¹⁹ The transfer of semiconductor technology to China is of particular concern to the United States because of its dual-use nature: semiconductors have applications for weapons systems as well as for smartphones.²⁰ The dual-use application of many technologies targeted by Chinese outbound foreign direct investment is of particular concern for the United States and Israel.

¹⁶ Jost Wübbeke, Mirjam Meissner, Max J. Zenglein, Jaqueline Ives, and Björn Conrad, *Made in China 2025: The Making of a High-Tech Superpower and Consequences For Industrial Countries*, Berlin: Mercator Institute for China Studies, December 2016.

¹⁷ U.S. Chamber of Commerce, 2017.

¹⁸ Hanemann and Rosen, 2016.

¹⁹ Hanemann and Rosen, 2016.

²⁰ In September 2017, based on the recommendation of the CFIUS, President Donald Trump blocked Chinese-government-backed Canyon Bridge Capital Partners from buying U.S.-based Lattice Semiconductor on national security grounds, citing in part the use of Lattice products by the U.S. government (Kate O’Keeffe, “Trump Blocks China-Backed Fund from Buying Lattice Semiconductor,” *Wall Street Journal*, September 13, 2017).

Other Elements in China's Efforts to Use Technology Transfer to Meet These Goals

Overseas investments form just one piece of a broader strategy of using technology transfer to achieve China's industrial and technology policy goals.²¹ Other tools China uses to meet these goals include forced technology transfer in exchange for market access, as well as cyber espionage.²²

Restrictions on foreign investment in China are designed such that foreign companies are often pressured to transfer their technology to Chinese companies as a condition for conducting business in the Chinese market. In certain industries, including those that draw Chinese investment in Israel, foreign companies operating in China are required to partner with a Chinese entity; in some cases, the Chinese company must be the controlling shareholder. These restrictions apply in several of the priority industries in MIC 2025, including auto manufacturing, civil aviation, telecommunications, ship building, and railway equipment.²³ In a statement on the investment climate in China, the U.S. State Department noted that, in addition to the existence of such mandatory joint venture structures, the lack of transparency in the approval process "foster[s] an environment where government authorities can impose deal-specific conditions beyond written legal requirements, often with the intent to force technology transfer as a condition of market access or to support industrial policies and the

²¹ For a more thorough investigation of the various methods China uses to achieve technology transfer, see 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*, Washington, D.C., March 2018. The report examines policy tools including foreign ownership restrictions, technology licensing, systematic foreign investment and acquisition, and cyber intrusions.

²² See Daniel R. Coats, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*, testimony before the Senate Select Committee on Intelligence, January 29, 2019. See also Fred Plan, Nalani Fraser, Jacqueline O'Leary, Vincent Cannon and Ben Read, "ATP40: Examining a China-Nexus Espionage Actor," *FireEye Threat Research*, March 4, 2019.

²³ Office of the United States Trade Representative, 2018; U.S. Chamber of Commerce, 2017.

interests of local competitors.”²⁴ In addition to forming local partnerships that could result in technology transfer, foreign companies are often required to disclose unreasonable amounts of sensitive technical information during the approval process.²⁵

Cyber espionage is another tool that the Chinese government uses to achieve technology transfer. An investigation into China's technology transfer practices by the Office of the United States Trade Representative concluded that “documented incidents of China's cyber intrusions against U.S. commercial entities align closely with China's industrial policy objectives.”²⁶ Chinese state-sponsored cyber actors have also targeted Israeli technology and defense companies, including Israeli companies involved in the development of the Iron Dome missile defense system.²⁷ This specific incident, as well as a more in-depth discussion regarding Chinese cyber espionage, will be discussed in Chapter Five.

How Israel Fits with China's Policy Goals

Israel is unique among countries that receive Chinese investment, as it aligns both with the BRI and Chinese goals to improve its domestic high-tech sector. This combination means that the Chinese government incentivizes both construction and technology companies to engage in Israel. Moreover, engagement with Israel advances China's broader long-term goals of increasing its presence and role in the Middle East and connecting to Europe.

China sees Israel as an important node in the BRI. The BRI is a major part of China's push to take a more active role in the Middle East, and improved ties with Israel can serve to offset China's historically closer ties with other countries in the region, including Iran and

²⁴ U.S. Department of State, “2015 Investment Climate Statement—China,” May 2015.

²⁵ Office of the United States Trade Representative, 2018.

²⁶ See Coats, 2019, and Office of the United States Trade Representative, 2018.

²⁷ Zachary Keck, “Chinese Hackers Target Israel's Iron Dome,” *The Diplomat*, August 2, 2014.

Israel's Arab neighbors. A Chinese academic wrote that Israel was particularly important in the BRI because it could "lend credibility to Chinese soft power in the region" as it would counterbalance the region's Arab states.²⁸ In addition, the author noted that Israel's "well-endowed human capital," "developed economy and high technology base," and "stable society and government business environment" further increased the country's appeal as a key piece of the BRI.²⁹

Moreover, Israel has the potential to be a small but important stop on the 21st Century Maritime Silk Road connecting the Indian Ocean and the Mediterranean Sea through the Gulf of Suez. The possible construction of a railway line from Eilat to Ashdod (pending approval by the Israeli government) and the construction of a new port in Ashdod—both to be built by government-owned Chinese firms—serve as prime examples of such an architecture.³⁰

Furthermore, construction in Israel might help Chinese infrastructure companies get a foot in the door in Europe or the United States. Most of the other BRI countries in which Chinese companies complete infrastructure are low- and middle-income countries. The ability of Chinese companies to successfully build infrastructure in Israel, a highly developed country, improves their image and lends legitimacy to their operations, potentially leading to additional projects in other developed countries.³¹

On the technology front, Israel is particularly attractive as a destination for Chinese investment in technology because of its reputation as a "start-up nation." China views Israel as a model for creating an innovation hub quickly, which matches well with China's goal of devel-

²⁸ Xiao Xian, 一带一路视角下的中国与以色列关系 ["The Role of 'One Belt One Road' Within Sino-Israeli Relations"], *Journal of Southwest Asia and Africa*, Vol. 2, 2016.

²⁹ Xiao Xian, 2016.

³⁰ Dubi Ben-Gedalyahu, "China to Be Israel's Biggest Infrastructure Partner," *Globes*, April 29, 2015; Niv Elis, "Private Ashdod Port Building Ahead of Schedule, Says Ports Company," *Jerusalem Post*, April 12, 2016.

³¹ Conversation with former senior government official, Tel Aviv, October 23, 2018.

oping its own indigenous innovation capabilities.³² After returning from a visit to China in 2013, Israeli Prime Minister Benjamin Netanyahu said China was interested in “three things: Israeli technology, Israeli technology, and Israeli technology.”³³ During Netanyahu’s visit to Beijing in March 2017, Netanyahu and Xi announced the establishment of a “comprehensive partnership” for innovation between Israel and China, which would include “closer exchanges among young technological personnel” as well as a “global technology transfer center.”³⁴ Xi said the two countries would “steadily advance major cooperative projects within the framework of jointly building the Silk Road Economic Belt and the 21st Century Maritime Silk Road.”³⁵

Moreover, compared to markets in the United States and other advanced economies, there are fewer barriers to entry in Israel for Chinese investors. In the United States, the CFIUS reviews the acquisition of U.S. companies by foreign entities to screen for potential threats to national security. In August 2018, Congress passed the FIRRMA to reform the CFIUS process to cover a wider variety of transactions, including investments (short of purchasing a controlling stake) that would give a foreign investor access to sensitive technologies. FIRRMA suggests that the committee consider in its deliberations if a transaction “involves a country of special concern that has a demonstrated or declared strategic goal of acquiring a type of critical technology or critical infrastructure.”³⁶ Although CFIUS and FIRRMA cover foreign acquisitions and investment from any country, Chinese investments are

³² Conversation with an executive at an Israeli VC company, October 23, 2018; Fan Jida, 以色列如何成为创新驱动型国家 [“How Israel Became an Innovation-Driven Nation”], *Journal of Theory Guidance*, December 2016.

³³ Prime Minister’s Office, “PM Netanyahu’s Remarks at Israeli Presidential Conference,” press release, June 20, 2013.

³⁴ “China, Israel Announce Innovative Comprehensive Partnership,” *Xinhua*, March 21, 2017.

³⁵ Liu Hua, “Xi Jinping Meets With Israeli Prime Minister Netanyahu,” *Xinhua*, March 21, 2017.

³⁶ Pub. L. 115-232, 2018.

a major focus. Canada and Australia also have review mechanisms;³⁷ in late 2018, the European Union has adopted a Europe-wide policy to screen foreign investments in strategic technologies and infrastructure,³⁸ and individual European countries have adopted their own policies, including Germany's revision of its Foreign Trade Regulation in July 2017 to allow the government to screen and block foreign takeovers.³⁹ Up until late October 2019, including the period in which research was conducted, Israel has had no formal mechanism to screen foreign investment, providing a more permissive operating environment for Chinese firms. The mechanism that was announced in October is discussed in more detail in Chapter Three. Even though it has not yet been implemented during the time of writing, its description by the government implies that it will be associated with worrying shortcomings including failure to oversee investments in the technology sector. This could pose serious concerns for the United States, which closely partners with Israel on advanced technology and defense projects.

³⁷ Foreign Investment Review Board, "About FIRB," webpage, undated; Foreign Investment Review Board, *Annual Report 2016-17*, Canberra: Commonwealth of Australia, 2018; Government of Canada, "Investment Canada Act," webpage, April 6, 2018; Innovation, Science, and Economic Development Canada, *Annual Report: Investment Canada Act 2016-17*, Ottawa, 2017.

³⁸ Phillip Blenkinsop, "EU Countries Back Investment Screening Plan with China in Mind," Reuters, December 5, 2018.

³⁹ Philip Blenkinsop, "EU Promises Tough Line on U.S., China While Pushing for Free Trade," Reuters, June 23, 2017; Slaughter and May, "Foreign Investment in the EU: A Tale of Competing Tensions," July 26, 2017.

Foreign Investment and Regulatory Policies in Israel

In recent years, Chinese entities have increased investments in Israeli technology and infrastructure (alongside other areas, including agriculture, cellular and medical companies). Chapter Four will provide specific examples of such investments. Although the Israeli economy, especially the technology sector, has benefitted substantially from foreign investment (including Chinese investment), involvement in assets that are considered vital to national security has drawn attention to the absence of a *comprehensive* mechanism in Israel for screening foreign investments in the country. The Israeli government announced the establishment of such a mechanism in October 2019, but at the time of writing, this mechanism had not started operating. This chapter contains a brief explanation of how Israel benefits from increased economic engagement with China. It then discusses the current state of foreign investment and cyber regulation in Israel and describes ongoing discussions about potential forthcoming screening mechanisms in this area.

Why Engagement with China Is Attractive to Israel

Although defense technology transfers were the bedrock of Israeli-Chinese ties until the mid-2000s, Israel's current chief interest in promoting its relations with China is economic, even though political and

defense ties have been steadily improving.¹ Since 2013, Netanyahu has been eager to expand ties with China and has openly welcomed Chinese infrastructure projects. Israel hopes to access the large Chinese market and diversify its export markets and foreign investments outside of the United States and Europe, its traditional partners.² In 2013, the Ministry of Economy opened offices in China (while it was closing economic attaché offices in the United States and Europe).³ Upon Netanyahu's return from Beijing that year, the Knesset passed Government Resolution 251, calling for expansion of Israeli-Chinese cooperation.⁴ Other government decisions followed suit, including incentives to cooperate with Chinese companies.⁵ Ministers of Finance and Housing worked to bring Chinese construction companies and workers to Israel, and the Ministry of Transportation started promoting tenders to Chinese companies.⁶ Although some Israeli officials had previously stated their openness to easing the stringent restrictions on dual-use and defense technology exports to China that were established after the 2005 HARP incident,⁷ the Ministry of Defense protested these calls, fearing Washington's reaction.⁸ Israel indeed does not sell China military or explicit dual-use technology; however, it is becoming increasingly difficult to distinguish between commercial and dual-use technology,

¹ Gregory Noddin Poulin, "Sino-Israeli Economic Ties Blossoming," *The Diplomat*, December 1, 2014; Liu Zhen, "Free Trade and Top Tech: What China Wants from Israel," *South China Morning Post*, March 21, 2017.

² Poulin, 2014; Zhen, 2017.

³ Yuval Azulay, "Rotsim La'avod Be'chul: 2,200 Muamadim al 12 Misrot Nispachim Mischariyim [Want to Work Abroad: 2,200 Candidates for 12 Commercial Attaché Positions]," *Globes*, December 2, 2013.

⁴ Prime Minister's Office, "Tochnit Le'kidum Ve'harchavat Ha'ksharim Ha'kalkaliyim Bein Israel V'sin [A Plan to Promote and Expand the Economic Relations Between Israel and China]," press release, June 5, 2014.

⁵ Prime Minister's Office, 2014.

⁶ Discussion with a former government official, Tel Aviv, October 23, 2018.

⁷ Ora Coren, "Washington Obstructing Israeli High-Tech Exports to China," *Haaretz*, January 22, 2014.

⁸ Coren, 2014.

and the United States is worried about the future dual-use nature of technology on which Israel and China do collaborate.⁹

During his 2017 visit to China, Netanyahu remarked that “the Israeli side is ready to actively participate in infrastructure and other cooperation under the framework of the [BRI].”¹⁰ Chinese state-owned enterprises are able to put forward very competitive bids for various infrastructure projects and also have a good track record in Israel for speedy project completion.¹¹ For some projects, such as digging or underground rail, Chinese companies have proven experience, unlike Israeli bidders.¹² Moreover, Israel’s infrastructure sectors, particularly its ports, have powerful unions, and port workers have gone on numerous strikes in recent years; using Chinese companies bypasses the difficulties of dealing with labor unions.¹³ When the deal was announced for a Chinese company to build a new port in Ashdod, Israeli officials claimed that it was the “government’s response to what [it] called the excesses of the port workers’ unions.”¹⁴ However, some in Israel contend that these motivations are insufficient to justify Chinese involvement in important infrastructure, and that short-term interests are bound to entail long-term costs, including Chinese political leverage and a possible rift with the United States.¹⁵

Israeli Regulation on Foreign Investment

Increased Chinese activity in Israel has been enabled by a relatively lax regulatory environment for foreign investments. Based on our research, as of December 2019, Israel does not have an *overarching* screening

⁹ Conversation with a U.S. State Department official, October 30, 2019.

¹⁰ Liu Hua, 2017.

¹¹ Discussion with an Israeli academic specializing in China, Tel Aviv, October 21, 2018.

¹² Discussion with former defense official, Tel Aviv, October 21, 2018.

¹³ Discussion with former defense official, Tel Aviv, October 21, 2018.

¹⁴ David Shamah, “China Firm to Build New Ashdod ‘Union Buster’ Port,” *Times of Israel*, September 23, 2014.

¹⁵ Discussion with an Israeli academic specializing in China, Tel Aviv, October 21, 2018; discussion with former Israel Defense Forces (IDF) official, Tel Aviv, April 29, 2019.

mechanism similar to CFIUS that evaluates investments' potential national security impact and that is empowered to block deals. On October 30, 2019, the government announced its decision to establish a committee that would oversee foreign investments in different sectors;¹⁶ however, the decision has yet to be formally implemented at the time of writing. In addition, the government's announcement suggests that this committee could be quite different from its parallels in other advanced economies, limiting its ability to monitor investments effectively.

First, the committee's establishment is not anchored in legislation.¹⁷ Moreover, it is designed to advise regulators, not senior political leaders (as in other countries).¹⁸ More importantly, the committee is defined as "advisory." The committee's advice is nonbinding—regulators can choose whether to heed the committee's advice.¹⁹ Furthermore, the committee does not distinguish between private companies and entities that are controlled by foreign governments. In addition, the committee advises only on investments in the areas of "finance, communications, infrastructure, transportation, and energy."²⁰ These are indeed important areas—ones for which regulators already exist, but in which regulators might not yet incorporate national security considerations into deliberations. However, the high-tech sector is missing, especially the "foundational" and "emerging" technologies on the United States' FIRRMA list, which includes biotechnology; artificial intelligence (AI) and machine learning technology; position, navigation, and timing technology; data analytics technology; robotics; and microprocessors.²¹ Most of the investments that Chinese companies have made in Israel in the last decade—the vast majority of which were within the

¹⁶ Prime Minister's Office, "Security Cabinet Statement," press release, October 30, 2019.

¹⁷ Doron Ella, "A Regulatory Mechanism to Oversee Foreign Investment in Israel: Security Ramifications," Institute for National Security Studies, Insight No. 1229, November 19, 2019b.

¹⁸ Ella, 2019b.

¹⁹ Ella, 2019b.

²⁰ Prime Minister's Office, 2019.

²¹ White and Case, "Department of Commerce Review of Export Controls on Emerging Technologies," November 28, 2018b.

tech sector—would fall under the FIRMA list, but they would not be included in the new committee's areas of responsibility.²²

Finally, the committee will consist of “senior representatives” from the ministries of finance, defense, and the National Security Council, with “observers” from the foreign ministry, the ministry of labor and industry, and the National Economic Council.²³ Notwithstanding these officials' expertise, their understanding of China is lacking. The INSS in Tel Aviv found that Israel's China expert bench is extremely thin. This gap is understandable because of Israel's traditional national security focus on the Middle East. The outcome, however, is that very few professionals specializing in modern China are employed by the government. Only a handful of modern China academics exist, and they are not systematically integrated into policymaking.²⁴ This is in contrast to CFIUS, for example, whose members include the Director of National Intelligence. Thus, discussing the security considerations associated with Chinese investment in Israel could be hindered because of a gap in expertise. Time will tell whether the committee, once it becomes operational, will effectively monitor foreign investment into Israel. Its formation is definitely an important step in the right direction; however, at least based on the few details available during the time of writing, it is likely to be associated with legal, structural and staffing challenges.

The general regulatory environment in Israel has been fractured into different sectors and government ministries, each with their own regulators, and this situation will continue at least until the decision to establish the committee is fully implemented. There has been a clear difference in regulation concerning investment in companies that produce strictly military or dual-use goods and services, and business entities in sectors that could be considered sensitive.

²² Doron Ella, “Regulation of Foreign Investments and Acquisitions: China as a Case Study,” in Assaf Orion and Galia Lavi, eds., *Israel-China Relations: Opportunities and Challenges*, Tel Aviv: Institute for National Security Studies, August 2019a.

²³ Prime Minister's Office, 2019.

²⁴ Assaf Orion, “Challenges to Israel's Policy on China,” in Assaf Orion and Galia Lavi, eds., *Israel-China Relations: Opportunities and Challenges*, Tel Aviv: Institute for National Security Studies, August 2019.

Foreign purchases of military, defense and dual-use technologies are regulated by the Israeli Defense Export Controls Agency, which was established in 2006 in response to the PHALCON and HARPY incidents and which operates within the Ministry of Defense (MOD). Companies producing defense and military equipment have regularly complained that Israeli export control laws, which the Israeli Defense Export Controls Agency oversees, hinder the ability of Israeli businesses to compete in international markets.²⁵ However, according to a former defense official intimately familiar with the matter, the MOD prefers to be very careful in the hope of avoiding another confrontation with the United States.²⁶

Exports by companies producing dual-use technologies, including cyber applications, are monitored and regulated according to the Wassenaar Arrangement, “whose 42 members exchange information on transfers of conventional weapons and dual-use goods and technologies.”²⁷ Israel is not a member of the agreement, but is compliant with its definitions.²⁸ The issue is that the line between civil and military technology is becoming increasingly blurry.²⁹ In addition, it is hard to define the concrete negative consequences that foreign investments could entail in terms of access to technology.³⁰ The Ministry of Economy, overseeing such companies, cooperates on these decisions with the Ministry of Foreign Affairs and the Ministry of Defense, and usually heeds the advice of the latter.³¹

Israeli government-owned companies have specific regulation on investment and stock purchases. This regulation aims at protecting

²⁵ Gil Rosen, “Israel: Israeli Defense Export Control Regulations Amended,” *Advoc*, May 8, 2015.

²⁶ Conversation with a former Israeli senior defense official, Tel Aviv, October 21, 2018.

²⁷ Arms Control Association, “The Wassenaar Arrangement at a Glance,” webpage, December 2017.

²⁸ Conversation with an Israeli government official, Jerusalem, October 21, 2018.

²⁹ Conversation with an Israeli official, Tel Aviv, October 23, 2018.

³⁰ Conversation with an Israeli official, Tel Aviv, October 23, 2018.

³¹ Conversation with an Israeli government official, Jerusalem, October 21, 2018.

national vital interests, including (1) ensuring continuity of activities essential to security, foreign affairs, or to public provision of essential services; (2) promoting market competition; (3) preventing elements that could undermine national security and foreign affairs from gaining influential positions; and (4) preventing the release of classified information.³² However, Chinese investments in Israeli technology and key infrastructure have not always been subject to such scrutiny because they involve non-government-owned companies.

More broadly, the purchase of or an investment in commercial public and private entities is not subject to extensive scrutiny.³³ Regulation of business entities in Israel generally has focused on financial aspects, not on political or security concerns—the concerns that the new committee supposedly will incorporate. Commercial companies are required to report to the Israeli Securities Authority on any discussions pertaining to possible purchase of assets (or acquisition granting control). The authority then examines the prospective purchasing entity's corporate structure and finances,³⁴ but unlike in many other Western countries (including the United States, Canada, and Australia) prospective purchases of local companies by foreign entities have not been scrutinized more broadly.

Regulation that is concerned with financial aspects of local and foreign investments in specific sectors is administered by three key bodies: the Capital Markets Commissioner, which oversees the Capital Markets, Insurance, and Savings Authority; Israel's Securities Authority, which oversees stock markets; and the Bank of Israel, where the Banking Supervision Department regulates commercial banks in Israel. Each of these regulators operates under different rules, according to their respective areas of responsibility.

³² Government of Israel, *Hok Ha'Havarot Ha'Memshaltiyot* [Law of Governmental Companies], 1975.

³³ Ella, 2018.

³⁴ Government of Israel, "Haraot Le'Giluy Be'Hitkashrut Le'Rechishat Nechasim [Instructions for Disclosing Communication Regarding the Purchase of Assets]," section 36A of the Securities Law, 1968.

Although these regulators focus on financial aspects, in one famous example, the Capital Markets Commissioner blocked a Chinese attempt to purchase an Israeli company. Specifically, the commissioner placed hurdles on Fosun's bid to purchase one of Israel's largest insurance firms, the Phoenix, which also manages substantial parts of the Israeli public's pension funds. During the approval process, the chairman of Fosun disappeared, and reports suggested that he might have been arrested by the Chinese police.³⁵ This incident raised red flags and the deal was blocked.³⁶ Notwithstanding this incident, according to our research, Chinese purchases and investments in Israeli technology companies (e.g., Huawei's purchase of Israeli cyber security startup HexaTier) and Chinese bids to build vital infrastructure (including rail) might have not been subject to such scrutiny.³⁷

Cyber Regulation Is Advanced but Implementation Might Be Lacking

Given the cyber and intelligence risks that could be associated with Chinese investments and involvement in Israeli technology and infrastructure, it is important to briefly explain the status of cyber regulation in Israel. In their 2019 book *Regulation in Cyberspace*, Gabi Siboni and Ido Sivan Sevilla of the INSS describe Israel's cyber regulation framework in detail. Based on their research, Israel's approach to cyber protections is advanced and combines characteristics from both the European and U.S. approaches, merging between binding state regulation and market forces, depending on the sector.³⁸ According to a serving government official, Israeli risk management framework for cybersecurity infrastructures "is exceptionally mature by international

³⁵ Michael Forsythe, "Fosun Group's Chairman Is Said to Be Missing in China," *New York Times*, December 10, 2015.

³⁶ Assa Sasson, "Reports in China: Chairman of Fosun—Purchaser of Phoenix—Disappeared [Hebrew]," *The Marker*, December 10, 2015.

³⁷ Conversation with former senior official, Tel Aviv, October 22, 2018; conversation with former government official, Tel Aviv, October 23, 2018.

³⁸ Gabi Siboni and Ido Sivan Sevilla, "Regulation in Cyberspace," Tel Aviv: Institute for National Security Studies, Memorandum No. 190, April 2019.

standards.” Yet Siboni and Sevilla and Israel’s State Comptroller found flaws in Israel’s cyber defenses.

The main security services—the IDF, the General Security Service (known as the Shin Bet), and Mossad—are not subject to external cybersecurity regulations and instead protect themselves. The Director of Security of the Defense Establishment oversees cybersecurity for sensitive facilities and the defense industries. Otherwise, cyber regulation in Israel is centralized within the National Cyber Directorate within the Prime Minister’s Office.³⁹ The approach is largely sectoral, and different ministries are tasked with protecting their own areas of responsibility. Different cybersecurity guidelines are applied to different commercial entities, depending on how they are characterized.

Businesses operating in areas of infrastructure that the state defines as “vital,” which include telecommunications, water, electricity, and transportation, are subject to binding state intervention issued by the Shin Bet and the National Cyber Directorate. The directives themselves are then applied and enforced by the relevant ministry or authority.⁴⁰ Private-sector companies that operate in areas that are not classified as “vital” but that the state considers strategically important, such as banks, the capital market, and healthcare, are subject to sector-specific supervision that is managed by the appropriate ministries.⁴¹ Cybersecurity in the rest of the private sector, however, is not regulated by the state. The exception is the Privacy Protection Law, which requires organizations that own, manage or store databases of personal information that contain more than 10,000 records to implement cybersecurity measures (which vary by the size of the database).⁴²

Even though the Israeli cybersecurity framework is relatively thorough, Siboni and Sevilla conclude their research by pointing out that

³⁹ Siboni and Sevilla, 2019.

⁴⁰ For example, privately owned water and electricity infrastructures are supervised by a private company that the Ministry of Energy subcontracted for this task (Siboni and Sevilla, 2019).

⁴¹ An example that Siboni and Sevilla provide is that the Ministry of Health supervises hospitals; Siboni and Sevilla, 2019.

⁴² Government of Israel, *Hok Haganat Ha’Pratiyut* [Privacy Protection Law], 1981.

“major organizations [are] not subject to supervision, despite their substantial impact on Israel’s national resilience in cyberspace.” Further, they explain that the sectoral monitoring division does not address the need for developing a comprehensive approach to supervise the private sector.⁴³

In May 2019, Israel’s state comptroller published an abridged and unclassified criticism of the state of cybersecurity in which he found that “[g]overnment ministries are ineffective, and the private sector lacks guidance.”⁴⁴ The state comptroller investigated three vital infrastructure entities (which were unnamed in the public version) and found that despite binding directives, implementation of security measures was lacking. In addition, the State Comptroller found that the government ministries tasked with instructing and guiding their respective sectors

are finding it difficult to work at the necessary pace, and to take effective measures. The civilian sector will find it hard to meet the cyber defense challenge without instruction and guidance. There is concern that without suitable government leadership, the economy will be left exposed to cyberattacks.⁴⁵

It is important to mention that the Israeli parliament is likely to pass a draft bill on cyber regulations that would provide the government, and especially the National Cyber Directorate, very broad powers to get into companies’ systems and grant them leverage to examine foreign investments in technology and cyber.⁴⁶

⁴³ Siboni and Sevilla, 2019.

⁴⁴ Joseph Shapira, “Mevaker Ha’Medina, HeArchut Gufim Hiyuniyim Le’Haganat Ha’Syber [Cyber Security Preparation of Essential Bodies],” May 6, 2019.

⁴⁵ Shapira, 2019.

⁴⁶ Conversation with cyber experts, Tel Aviv, October 23, 2018.

Increased Chinese Investment in Israeli Technology and Key Infrastructure Highlights Need for Regulation

Although Israeli regulations on foreign investment have been lacking in general, Chinese involvement has led to recent discussions in Israel about the need for an orderly process that guarantees scrutiny and intervention if needed. The reason, as will be elaborated upon in Chapters Four and Five, is the concern that Chinese investments pose unique challenges to advanced economies in general, and to Israel in particular, including the risk of a rift with Washington. It is clear that since 2017, and even more so since late 2018, that Israeli thinking about China has been evolving to consider the challenges of the relationship, in addition to the opportunities.

In 2017, several former and current Israeli Knesset members and officials started raising concerns about China, such as cyber espionage, corruption allegations, the links between Chinese companies and China's government, and the issue of having a foreign entity control major infrastructure.⁴⁷ In March 2018, four Knesset members, representing parties across the political spectrum, initiated a discussion in the Knesset Foreign Affairs and Security Committee titled, "Israel's Policy vis-à-vis the Entrance of Chinese Entities to Strategic Areas in Israel," which concentrated on political and security risks.⁴⁸ In July 2018, for the first time, a classified discussion was held by the committee.⁴⁹ During the discussion, the prime minister's economic adviser reportedly indicated that the government might form a new "body or team that would vet foreign investments, a move largely seen [as] aimed at China"⁵⁰—in stark con-

⁴⁷ Melman, 2018.

⁴⁸ Melman, 2018.

⁴⁹ Conversations with former senior government official, Tel Aviv, July 17, 2018; and an Israeli think tank team, Tel Aviv, July 19, 2018. Reference to the hearing was also included in Barak Ravid, "Scoop: Netanyahu's Economic Adviser Backs Trump's Trade War with China," *Axios*, July 12, 2018.

⁵⁰ Hagai Amit, "In Turnaround, Israel May Form Body to Vet Foreign Investment," *Haaretz*, July 16, 2018.

trast to the Israeli government's policy since 2013, which has encouraged foreign investment from China overseen directly by the council.⁵¹

Since January 2019, leading security experts in Israel have voiced concerns over deepening Chinese involvement in Israel's infrastructure and technology sectors, including the head of Shin Bet, who called for instituting a mechanism for screening foreign investments.⁵² Subsequently, Israel was planning to bar Chinese and Turkish companies from competing in a tender process for construction of a new international airport because of concerns about Chinese espionage and diplomatic tensions with Turkey. China was not targeted exclusively, but the tender was limited to companies from member countries of the North Atlantic Treaty Organization.⁵³ Then, in late October 2019, the caretaker government announced the formation of a committee to monitor foreign investments. The decision to design the committee as is was a result of tension between Israel's National Security Council (NSC) and the National Economic Council (NEC), who differed in their approaches on this matter, as explained in meetings with Israeli government officials in October 2018. The NEC has proposed to rely on existing regulators and design a voluntary mechanism in which companies seeking foreign investments or issuing tenders would elect to seek advice from a regulatory committee, which would examine the deal's possible security implications. The Israeli NSC, on the other hand, has proposed a mandatory process for screening all foreign

⁵¹ The Prime Minister's Office Israel-China task force was led by the National Economic Council. In 2015, then-National Economic Council and Israel-China Task Force Chairman Eugene Kandel said,

the expansion of bilateral economic ties will have far-reaching macro-economic effects on the Israeli economy. . . . Ties between Israeli and Chinese companies, encouraged and supported by both governments, is of decisive importance for Israel at a time when the global economy as a whole is moving eastward (Israeli Ministry of Foreign Affairs, "Israel-China Task Force to be Launched," March 30, 2015).

⁵² "Chinese Investments in Israel Could Pose Security Threat, Shin Bet Chief Warns," *Haaretz*, January 9, 2019.

⁵³ "Israel Said to Bar China, Turkey from Bidding for \$40 Million Airport Tender," *Times of Israel*, January 25, 2019.

investment.⁵⁴ These two approaches represented the main divide in Israel on this issue: Economists and business-minded stakeholders contend that the Israeli business environment is already cumbersome and bureaucratic,⁵⁵ and security-minded stakeholders, including the NSC, MOD, and Shin Bet, were pushing for more draconian regulations to mitigate risks. Based on the government's announcement, the NEC's approach gained the upper hand eventually.

During the discussions on the committee and subsequently after it was announced, some experts expressed fear that it would be insufficient to adequately mitigate risks.⁵⁶

⁵⁴ Conversation with Israeli government official, Jerusalem, October 21, 2018.

⁵⁵ Conversation with an expert on Israeli-Chinese ties, February 2018.

⁵⁶ Conversation with former government official, March 6, 2019; conversation with U.S. State Department official, March 6, 2019; conversation with U.S. State Department official, October 30, 2019.

Chinese Technology Investment and Construction in Israel

Chinese companies have been increasingly active in both investment and construction in Israel. This chapter provides an overview of Chinese investments in Israel from 2007 to 2018, as well as major construction projects undertaken by Chinese companies in Israel over the same period. First, we provide an overview of the extent of these activities, including estimates of the total dollar amount, as well as the scope of these investments and other economic activity across different sectors. We also examine several construction projects and investments in technology companies in greater detail, with a focus on investments and infrastructure that could have national security implications for Israel and the United States. We discuss the risks of Chinese technology companies' investments in Israel and of Israeli technology companies that have received Chinese investment. We also elaborate on potential risks to U.S. and Israeli interests as they relate to specific companies, investments, and construction projects. The risks of Chinese investment and construction activity more broadly are addressed in Chapter Five.

Overview of Chinese Investment and Construction Activity

Chinese investment generally flows to *developed* countries, Chinese construction typically occurs in *developing* countries.¹ Israel is an exception

¹ Derek Scissors, "Private Data, Not Private Firms: The Real Issues in Chinese Investment," *American Enterprise Institute*, January 10, 2018.

to this rule: It is both a developed country with a sizable advanced technology sector as well as a participant in China's BRI program, which emphasizes Chinese construction of major infrastructure projects—most of which are built in low- and middle-income countries.

We compiled a dataset of 92 deals between China and Israel: five construction project deals made between 2007 and 2018 and 87 investments made between 2011 and 2018 (see Appendix A). The data were collected from several primary sources, including an analysis conducted by Doron Ella in his article “Regulation of Foreign Investments and Acquisitions,” which was published in the INSS report *Israel-China Relations: Opportunities and Challenges* in Hebrew.² In addition, we drew on publicly available sources. Data on VC investments were drawn from the VC companies' websites. According to data collected, investment totaled \$12.9 billion and infrastructure construction and operation contracts amounted to more than \$4 billion.

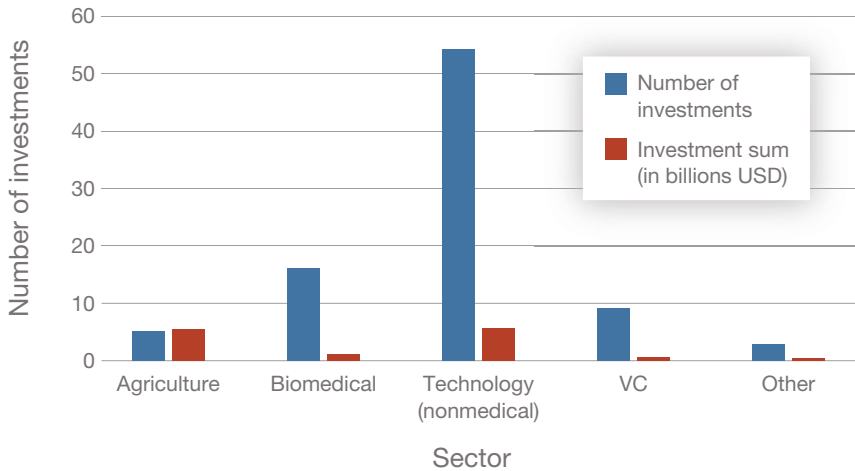
In terms of technology investment, the potential for transfer of sensitive technologies presents the greatest risk. Intelligence collection, whether through cyber or traditional espionage, is a major risk when it comes to construction and operation of such infrastructure as rail or ports. Chinese activity in Israel also gives rise to the risk that Beijing could use its increasing economic, political, and social influence in Israel in ways that are contrary to U.S. interests. Subsequent sections focus on these risks as they relate to specific investments and infrastructure projects; the broader implications of this activity are discussed further in Chapter Five.

Investment

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; see Figure 4.1). The agricultural sector received the second-largest amount of investment (\$5.3 billion). Investment in agriculture was driven primarily by ChemChina's acquisition of Adama (previously known as Machteshim-

² Ella, 2019a.

Figure 4.1
Known Chinese Investment in Israel, 2007–2018



SOURCE: Ella, 2019a, and authors' assessments from sources described in the methodology section.

Agan) for \$3.8 billion.³ We also tracked VC as a separate category, even though most Israeli VC companies that received Chinese funding have portfolios that consist primarily of technology or biotechnology companies. Although some of the values include the total investment amount in funding rounds in which the Chinese companies were not the sole participants, this overestimation might be balanced out by the fact that other investment amounts were undisclosed, and our compilation of investments might not be exhaustive.

Construction and Operation of Infrastructure

Because of the potential cyber and espionage risks or for the transfer of sensitive technologies, we focused our research on construction of major infrastructure, concentrating on ports and rail. Based on news reports, Chinese companies are also participating in tenders for other projects, some in sectors that are defined as “vital” infrastructure (e.g.,

³ Yoram Gabison, “IDB Selling Remaining 40% Stake in Adama to ChemChina for \$1.4 Billion,” *Haaretz*, July 18, 2016.

water and electricity).⁴ We do not discuss these deals because they have yet to be finalized.

We identified four major infrastructure projects in Israel that are being completed by state-owned Chinese companies; two of the projects also involve infrastructure operation. The four projects are all related to transportation infrastructure:

1. the expansion of the Ashdod port
2. partial construction of a new terminal by the Haifa port (with operation rights for 25 years)
3. construction and operation of the Tel Aviv light rail (two Chinese companies are involved in building different sections)
4. and the digging of the Carmel Tunnels (a Chinese company is a subcontractor).⁵

The total estimated cost of these projects is more than \$4 billion. In addition, we looked at the proposed rail line between Eilat and the Mediterranean, which, if approved, would likely be completed by a Chinese state-owned enterprise at an estimated cost of a little less than \$2 billion.⁶ It is worth noting that Ashdod and Haifa are Israel's two important ports on the Mediterranean Sea. Additionally, portions of

⁴ These attempts include bids by two Chinese companies—Pan-Mediterranean Engineering (PMEC), a subsidiary of China Harbor Engineering Company, and Hutchison—for a new desalination plant in the Sorek area. PMEC was reportedly disqualified, but Hutchison advanced to the next stage, despite protests by the Ministry of Defense. PMEC has also been attempting to buy the Alon Tavor electric power station, which is currently owned by Israel Electric Corporation. See Amos Harel, "With Its National Security at Stake, Israel Takes Sides in U.S.-China Trade War," *Haaretz*, May 26, 2019; "Israel Received Bids to Build World's Biggest Desalination Plant," *Reuters*, October 7, 2018; Lior Gutman, "China's PMEC Looking to Buy Israeli Electricity Power Station," *Calcalist*, January 20, 2019.

⁵ Avi Bar-Eli, "Carmelton, Chinese Firm Reach Compromise on Tunnels Project," *Haaretz*, November 3, 2008; Amiram Barkat, "Eilat Railways Hits Financing Buffer," *Globes*, May 21, 2014; Angela Yu, "Chinese Port Operator Signs Deal to Run Israel's Haifa Port," *JOC.com*, June 2, 2015; Shamah, 2014; Hedy Cohen, "Arison, Chinese Co Win TA Light Rail Underground Tender," *Globes*, May 19, 2015; China Railway Construction Corporation Ltd., "CCECC Signes [sic] Israel's First Light Rail Operation Maintenance Contract," November 16, 2017.

⁶ Barkat, 2014.

the Tel Aviv light rail run close to the Kirya area in Tel Aviv, where the Israeli Defense Forces are headquartered, offering China opportunities to conduct surveillance.⁷ Protective cyber measures are employed, but they might not be sufficient in the future to offset such risk.⁸ Concerns regarding the involvement of Chinese state-owned companies in developing these two ports as well as building other key infrastructure in Israel are discussed further in Chapter Five.

Chinese Entities

We examined all the Chinese companies known to have invested in Israeli technology or to have built infrastructure in Israel and identified 11 that pose potential risks to Israel or the United States. We have not examined Chinese entities that have bid on yet-to-be-finalized projects. These risks include connections with the Chinese military or government, as well as issues related to security, privacy, or censorship. We also noted if any of these companies conducted business activities with Israel's adversaries, such as Iran, and whether any of the companies are alleged to have conducted nefarious activities in other countries. Table 4.1 presents an overview of the 11 companies we identified and the areas of possible risk.⁹

Military and Government Connections

A key risk is the nature of the ties that Chinese companies investing or building major infrastructure projects in Israel have with Chinese government or military entities, particularly if a company has ties to military intelligence or to Chinese operations in the South China Sea, meaning that its operations could be motivated by

⁷ Conversations with a former senior Israeli defense official and a former government official, Tel Aviv, October 23, 2018.

⁸ Conversations with cyber experts, Tel Aviv, October 21, 2018, and with government officials, Tel Aviv, October 23, 2018. According to cyber experts, these measures include air gapping (isolating a computer from outside networks).

⁹ For more detail on these companies and the concerns they present, see Efron et al., 2019.

Table 4.1
Overview of Chinese Companies That Have Invested or Built Infrastructure in Israel

Chinese Entity	Company Information	Ownership	Activity	Israeli Entities or Projects	Area of Risk
Alibaba	E-commerce and internet services company; investments include eight Israeli technology or VC companies	Public	Investment	Visualead, Thetaray, Twiggle, Lumus, Jerusalem Venture Partners, Infinity Augmented Reality, SQream Technologies	Security issues: browsers made by Tencent, Alibaba, and Baidu all contained “strikingly similar security vulnerabilities” that left user data open to potential surveillance and to malicious attackers; ^a censorship concerns related to purchase of Hong Kong newspaper South China Morning Post
Baidu	Web services company that is also doing artificial intelligence research and developing autonomous cars; investments include five Israeli technology companies or VC funds	Public	Investment	Pixellot, Tonara, Taboola, Dynamic Yield, Carmel Ventures	Government connections: national lab for artificial intelligence Security issues: browsers made by Tencent, Alibaba, and Baidu all contained “strikingly similar security vulnerabilities” that left user data open to potential surveillance and to malicious attackers ^a

Table 4.1—Continued

Chinese Entity	Company Information	Ownership	Activity	Israeli Entities or Projects	Area of Risk
China Broadband Capital Partners (CBC)	Technology, media, and telecommunications investment company	Private	Investment	IronSource Ltd.	Princeling connections: Chairman of CBC served as the chief executive officer (CEO) of China Netcom, a state-owned telecommunications provider that was backed by the son of former Chinese President Jiang Zemin and appears to have enjoyed preferential treatment because of this connection ^b
Huawei Technologies Co., Ltd.	Network and telecommunications equipment company; Huawei's investment in Israeli company Toga Networks was initially disguised and unreported, and the exact nature of their relationship remains unclear ^c	Private	Investment	Toga Networks, HexaTier	Ties to Chinese government and military: the U.S. House of Representatives Permanent Select Committee on Intelligence has expressed concerns about the threat of economic espionage or intelligence collection because of the potential influence of the Chinese government in Huawei's business operations

Table 4.1—Continued

Chinese Entity	Company Information	Ownership	Activity	Israeli Entities or Projects	Area of Risk
Lenovo	Personal computers and electronics company	Public	Investment	Neura, Canaan Partners Israel	Government connections: founder served as National People's Congress (NPC) delegate Security issues: pattern of including unnecessary and vulnerable preinstalled software on its devices ^d
Kuang Chi	Technology conglomerate, with expertise in areas from materials technology to aerospace; Kuang Chi plans to establish an "International Innovation Headquarters" in Tel Aviv and invest \$300 million in Israel through its Global Community of Innovation Fund, of which it has already invested \$50 million ^e	Private	Investment	eyeSight, AgentVI, Beyond Verbal	Government connections: first company Xi visited as head of the Chinese Communist Party; ^f one of several technology companies chosen by the government to participate in a mixed-ownership pilot to introduce private sector innovation into China Unicom ^g

Table 4.1—Continued

Chinese Entity	Company Information	Ownership	Activity	Israeli Entities or Projects	Area of Risk
Tencent	Internet company: maker of WeChat, a social media application with more than 900 million monthly active users	Public	Investment	Contacts+, Singulariteam	Government connections: CEO served as NPC delegate Security and censorship issues: browsers made by Tencent, Alibaba, and Baidu all contained “strikingly similar security vulnerabilities” that left user data open to potential surveillance and to malicious attackers ^a
Xiaomi	Smartphone and electronics company	Private	Investment	Pebbles Interfaces	Government connections: received government support to develop semiconductor technology, founder served as NPC delegate Security issues: Xiaomi’s devices were reported in 2014 to send user data to servers in China, including collecting address book data without permission

Table 4.1—Continued

Chinese Entity	Company Information	Ownership	Activity	Israeli Entities or Projects	Area of Risk
ZTE Corporation	Network and telecommunications equipment company	Public	Investment	Rainbow Medical	Ties to Chinese government and military: a 2012 report for the U.S.-China Economic and Security Review Commission concluded that ZTE has a relationship with the People's Liberation Army (PLA) that involves collaborative research with military and civilian universities, satellite navigation, data link jamming techniques, training active-duty PLA personnel; it is a regular exhibitor and presenter at PLA-sponsored defense industry expositions^h Business in Iran: sold surveillance and other equipment to Iran in violation of sanctions
China Communications Construction Company (CCCC) and subsidiaries, such as China Harbour Engineering Company (CHEC)	Infrastructure projects worldwide, including Gwadar Port in Pakistan and Colombo Port City in Sri Lanka	State-owned	Construction	Construction of Ashdod port, proposed Eilat-Mediterranean rail line	Military construction projects: CHEC built a satellite ground station for the PLA in Argentina that is suspected of being an intelligence collection site; CCCC Dredging has allegedly been involved in China's island reclamation efforts in the South China Sea

Table 4.1—Continued

Chinese Entity	Company Information	Ownership	Activity	Israeli Entities or Projects	Area of Risk
China Railway Tunnel Group	Infrastructure projects in 80+ countries	State-owned	Construction	Portion of the Tel Aviv light rail	Conducts business in Iran

NOTES:

^a Jeffrey Knockel, Adam Senft, and Ron Deibert, "WUP! There It Is: Privacy and Security Issues in QQ Browser," *The Citizen Lab*, March 28, 2016.

^b John Pomfret, "Lines Crossed in China; State-Owned Firms Bully Customers, One Another in Fight for Telecom Turf," *Washington Post*, August 17, 2002.

^c Orr Hirschauge, "China's Huawei Is Coy On Ties to Israeli Firm," *Wall Street Journal*, June 2, 2016.

^d Paul Ducklin, "Lenovo 'Superfish' Controversy—What You Need to Know," *Naked Security by Sophos*, February 20, 2015.

^e "Gesture Tech Firm Eyesight Nabs \$20 Million Chinese Investment," *Times of Israel*, May 15, 2016; Shoshanna Solomon, "China's Kuang-Chi to Set Up Tel Aviv Base, Eyes Larger Firms," *Times of Israel*, January 12, 2017.

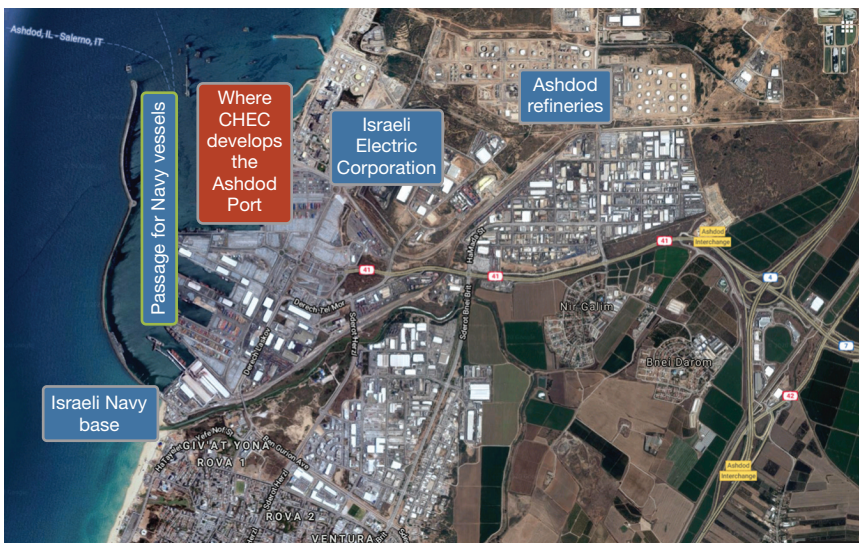
^f Yang Jingru, 习近平考察深圳光启研究院: 国家应择天下英才而用 ["Xi Jinping Observes Shenzhen Kuang Chi Research Center: The Nation Should Select And Use The Most Outstanding Talent"], *China News*, December 14, 2012.

^g Bien Perez, "China Taps Nation's Who's Who of Technology to Anchor Ownership Shakeup at Unicom's Parent," *South China Morning Post*, August 16, 2017.

^h Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, Falls Church, Va.: Northrop Grumman, March 12, 2012, p. 71.

broader strategic considerations. The degree to which Chinese security entities exercise control over state-owned companies operating abroad is unclear; based on the activities of such companies in other countries, we are flagging these companies as possible risks. Of the Chinese companies working on infrastructure projects in Israel, CCCC Dredging and its subsidiaries, including CHEC, are noteworthy for having completed work for the Chinese armed forces. CHEC is developing Israel's Ashdod port (Figure 4.2), one of Israel's two major ports on the Mediterranean and sited adjacent to an IDF naval base; CHEC also built a suspected intelligence collection site in Argentina. Despite Chinese denials that the site has military applications, the 50-year long lease, the terms of the contract (under which Argentinian government is not permitted to "interrupt" the station's activities), and the rule of Chinese, not Argentinian, law over station staff (many of whom are PLA members) have raised suspicions that the site is really designed to observe

Figure 4.2
Aerial Image of the Ashdod Port Area



SOURCE: Google Maps and consultations with Israeli experts; see Efron et al., 2019.

NOTE: Locations are not exact.

and track satellites over the Western Hemisphere.¹⁰ CCCC Dredging is slated to construct the Eilat-Ashdod rail line, if the project is approved; this company allegedly participated in land reclamation in the South China Sea.¹¹

Among the technology companies investing in Israel, telecommunications companies Huawei Technologies Co., Ltd. and ZTE Corporation in particular have come under significant scrutiny in the United States for their less-than-transparent connections to the Chinese government and military. The U.S. House of Representatives Permanent Select Committee on Intelligence released a report on these connections in 2012, outlining concerns about the possibility of the Chinese government's involvement in these companies' business operations and the potential that these companies would provide access to telecommunications networks for intelligence-gathering.¹² ZTE invested \$5 million in Israeli company Rainbow Medical in 2015, and Huawei has invested in Israeli technology companies Toga Networks and HexaTier. Huawei has an investment center in Israel and has invested (along with Samsung, Western Digital, Lenovo, Cisco and Dell Technologies¹³) \$16 million in Elastifile, a cloud storage company.¹⁴ Huawei's acquisition of Toga Networks, which it allegedly acquired for \$150 million in

¹⁰ Jana Robinson, "Deterring Chinese and Russian Space Hybrid Warfare by Economic And Financial Means," *Space Review*, September 18, 2017.

¹¹ Victor Robert Lee, "China Builds Space-Monitoring Base in the Americas," *The Diplomat*, May 24, 2016; Shamah, 2014; Laura Zhou, "Chinese Island-Building Firm Wins Contract with South China Sea Rival Claimant, the Philippines," *South China Morning Post*, October 26, 2016, updated October 27, 2016.

¹² Mike Rogers and C.A. Dutch Ruppertsberger, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, Permanent Select Committee on Intelligence, U.S. House of Representatives, October 8, 2012. For more information on Huawei's and ZTE's government and military connections, see Bill Gertz, "Chinese Telecom Firm Tied to Spy Ministry," *Washington Times*, October 11, 2011; Cai Ye, 见证华为任正非和孙亚芳历史不得不说的事情 ["Evidence from the Histories of Huawei's Ren Zhengfei and Sun Yafang that Must Be Spoken"], *Sina Blog of Cai Ye*, April 19, 2012; Krekel, Adams, and Bakos, 2012.

¹³ Meir Orbach, "Western Digital, Huawei, Invest in Cloud Storage Company," *Calcalist*, September 6, 2017.

¹⁴ Discussion with an Israeli think tank expert on China, Tel Aviv, May 30, 2019.

2016, was of particular concern because the deal was initially undisclosed; the nature of the relationship between the two companies is still unclear.¹⁵ A senior Israeli official disclosed that Toga had since moved part of its research and development operations to the United Kingdom, potentially to circumvent Israel's strict export control regulations.¹⁶ This activity raises concerns about Chinese investment contributing to technology transfer, with the possibility of China more easily obtaining sensitive technologies or Israel losing its competitive advantage.

Given the heated debate in the United States and in other countries about whether the presence of Huawei or ZTE equipment in nascent 5G networks could threaten the security and integrity of communications, it is important to address the use of such equipment in Israeli networks, although this represents Chinese sales of technology to Israel rather than Chinese investments in Israeli technology. It is especially relevant after U.S. officials raised this issue in discussions with their Israeli counterparts, including former National Security Adviser John Bolton, who according to press reports raised concerns about Israel using Chinese telecoms equipment during his January 2019 visit to Israel.¹⁷ In summer 2019, Israel announced that it would issue a tender for a 5G network.¹⁸ Based on media reports that contend that the Shin Bet does not approve Chinese-originated communication infrastructure¹⁹ and expert assessments citing security concerns, neither Huawei nor ZTE will successfully bid for this project.²⁰ The Israeli Ministry of

¹⁵ Hirschauge, 2016.

¹⁶ Conversation with senior Israeli official, October 2018.

¹⁷ Barak Ravid, "Trump Le'Netanyahu: Tsanen Ha'Kesher Im Sin O She'Hayachasim Imanu Aloolim Lehipaga [Cool Down Connection With China Otherwise Our Ties Could Cool Down]," *Channel 13*, April 4, 2019.

¹⁸ Steven Scheer, "Israel Holds 5G Mobile Network Tender, Aims for 2020 Launch," *Reuters*, July 14, 2019.

¹⁹ Amitai Ziv, "'Ha'Shabac Lo Yeasher:' Ha'Sod al Hevrot Ha'Tikshoret M'eSin Ve'Rusia She'Rotsot Lipfol Be'Yisrael ['The Shin Bet will Not Approve:' The Secret about Companies from China and Russia that Want to Operate in Israel]," *The Marker*, September 26, 2019.

²⁰ Discussion with an Israeli think tank expert on China, Tel Aviv, May 30, 2019.

Communications, according to press, is consulting with security services on whether these companies will even be allowed to compete.²¹

Other potential concerns related to Chinese technology companies' government connections include companies receiving direct support from the Chinese government to develop dual-use technologies and Chinese company executives holding government positions or having personal connections with high-ranking officials or their relations ("princelings"). For example, major mobile phone and smart appliance developer Xiaomi received government support to develop its own smartphone processor. Although the amount of funding Xiaomi received is unknown, a company representative claimed that "assistance extended beyond cash to include research and development."²² In addition, the Chinese National Development and Reform Commission designated web services giant Baidu as a national lab for deep learning in February 2017; the lab will also include several universities, including Beihang, which is known for military research. These partnerships with Xiaomi and Baidu are part of China's efforts to develop its domestic semiconductor industry and artificial intelligence expertise.

In terms of the government connections of company leadership, many executives from private or publicly traded Chinese companies that are investing in Israel, including those from Tencent, Xiaomi, and Lenovo, have served as delegates to the NPC.²³ In addition, leaders from Tencent, Alibaba, Lenovo, and Baidu accompanied Xi during

²¹ Yaakov Lappin, "Security Concerns Prompts Israel to Review China's Huawei 5G Network," *Breaking Israel News*, March 15, 2019.

²² Rogers and Ruppertsberger, 2012.

²³ The NPC is China's official main legislative body, although it wields very little real power, primarily acting as a rubber stamp in passing measures handed down from the Party or State Council. The NPC's nearly 3,000 delegates include many of China's most influential businesspeople, providing some degree of political protection to their companies and giving them a platform to raise issues of concern, so it is not surprising or necessarily concerning that the executives whose companies are investing in Israel are members. However, inviting businesspeople to participate in the NPC might serve to engender Party loyalty. For more information on the NPC, see Austin Ramzy, "Q. and A.: How China's National People's Congress Works," *New York Times*, March 4, 2016.

his first state visit to the United States in 2015.²⁴ Alibaba founder and executive chairman Jack Ma also accompanied Chinese Vice President Wang Qishan at the opening ceremony of the Israel Innovation Center in October 2018.²⁵ The degree of Chinese state influence over Chinese companies is still uncertain, but such close ties between companies' leadership and the government officials and institutions could mean that these companies are influenced by Chinese state motivations and interests, which are not necessarily aligned with those of Israel or the United States.²⁶

Security and Censorship Concerns

Security vulnerabilities have been identified in the products of many Chinese technology companies investing in Israel. For example, browsers made by Chinese technology giants Tencent, Alibaba, and Baidu were found to transmit such personal data as GPS coordinates, URLs visited, Wi-Fi access points, and unique device identifiers with either weak or no encryption.²⁷ Both Tencent's and Baidu's browsers also contained vulnerabilities that could be exploited to install malicious code on users' devices. In addition, Xiaomi's devices sent user data to servers in China without permission, including address book data, which

²⁴ "What's in a Picture? The Unspoken Messages in Xi Jinping's Group Portrait with CEO's and Senior Executives During His First State Visit to the US," *South China Morning Post*, September 24, 2015.

²⁵ Yasmin Yablonko, "Chinese Take Growing Slice of Israeli Tech Investment," *Globes*, October 30, 2018.

²⁶ This concern was raised in Israeli press by Harel Menashri, head of the cyber department at the Holon Institute of Technology and a former official in the Shin Bet. He said that, "Israeli leaders have to understand that there is no real private sector in China. Though many companies defined themselves as 'private,' practically all of them are directly or indirectly controlled by the centralized government, which is ruled by the Communist Party. All Chinese businessmen, investors and companies play along the party lines and its prevailing spirit." See Melman, 2018.

²⁷ Jeffrey Knockel, Sarah McKune, and Adam Senft, "Baidu's and Don'ts: Privacy and Security Issues in Baidu Browser," *The Citizen Lab*, February 23, 2016; Knockel, Senft, and Deibert, 2016.

prompted an investigation by the Taiwanese government.²⁸ Storage of user data on servers in the Chinese mainland is a potential concern for Taiwan given legal requirements to share such data with the Chinese government if requested. The extent to which the above security issues reflect simple sloppiness rather than intentional efforts to enable government surveillance is unknown—and while this is not necessarily a concern for Israel, it is for the United States.

In addition, Chinese internet companies are required to comply with government censorship directives and must turn over user data to the Chinese government upon request if the data are stored on Chinese servers. Tencent's popular WeChat app, which has more than 938 million monthly active users, has frequently faced scrutiny for its censorship of sensitive terms and images in both group and one-on-one private messages.²⁹ China's 2017 National Intelligence Law placed new security obligations on Chinese citizens and companies as well as their foreign partners. The law stipulates that Chinese, and often foreign citizens and companies operating in China, are required to provide access, cooperation, and support for the Chinese state's intelligence gathering.³⁰ The law, combined with other legislation and regulation, such as the Cybersecurity Law, could grant the Chinese government access to corporate networks, including "business and personal data, proprietary codes, and other intellectual property."³¹

The implication for Israeli companies, as for other Western companies, is that data, including IP, source code, private user data, and other information that renders protection, could be monitored by the Chi-

²⁸ Michael Gold, "Taiwan Government Investigates Xiaomi on Potential Cyber Security Concerns," Reuters, September 24, 2014.

²⁹ Scott Cendrowski, "China's WeChat Is a Censorship Juggernaut," *Fortune*, April 14, 2017; Jordan Novet, "China's WeChat Captures Almost 30% of the Country's Mobile App Usage: Meeker Report," *CNBC*, May 31, 2017.

³⁰ Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," *Lawfare*, July 20, 2017.

³¹ Tanner, 2017.

nese government.³² Data could be collected either through investment in technology companies or through the construction and operation of infrastructure such as roads and tunnels (e.g., the Mount Carmel tunnels), rail (the light rail in Tel Aviv), and ports in Haifa and Ashdod,³³ that collect and use private data from Israeli citizens.³⁴ Israel's Privacy Protection Law mandates that every organization that maintains, stores, and manages a database of more than 10,000 entries employ cybersecurity measures, but these measures might not be foolproof.³⁵

Censorship could also be problematic. According to a profile of Tencent, "Chinese Internet companies, Tencent included, employ hundreds if not thousands of their own censors."³⁶ Alibaba's 2016 purchase of the *South China Morning Post*, a Hong Kong-based newspaper that is blocked in mainland China, also gave rise to censorship concerns. According to the *New York Times*, "Alibaba said the deal was fueled by a desire to improve China's image and offer an alternative to what it calls the biased lens of Western news outlets," rhetoric that matches closely with language commonly used by the Chinese government regarding coverage of China.³⁷ A *South China Morning Post* July 2016 interview with a detained Chinese activist in which the activist expressed regret and repentance led many observers to believe the interview was forced.³⁸

Although not necessarily a security risk to Israel, Chinese censorship could pose ethical problems for Israeli companies if they directly or indirectly enable the Chinese government to collect information

³² Israel Kanner and Doron Ella, "China's New Cybersecurity Law and the Implications for Israel," *Israel Defense*, April 4, 2017.

³³ Melman, 2018.

³⁴ Discussion with former defense officials, Tel Aviv, April 30, 2019.

³⁵ Shapira, 2019.

³⁶ Dorinda Elliott, "Tencent
 The Secretive, Chinese Tech Giant That Can Rival Facebook and Amazon," *Fast Company*, April 17, 2014.

³⁷ David Barboza, "Alibaba Buying South China Morning Post, Aiming to Influence Media," *New York Times*, December 11, 2015.

³⁸ Tom Phillips, "Mysterious Confession Fuels Fears of Beijing's Influence on Hong Kong's Top Newspaper," *The Guardian*, July 25, 2016.

that could be used against Chinese citizens.³⁹ Furthermore, these companies' investments abroad give rise to the possibility that these capabilities will be used against foreign citizens as well. In addition, technology companies that want to expand into the Chinese market are often pressured to comply with government censorship requirements, and a desire to succeed in the Chinese market can result in companies self-censoring. These issues are discussed further in Chapter Five.

Chinese Business in Iran

Some Chinese companies investing or building infrastructure in Israel also conduct business with Israel's adversaries, such as Iran.⁴⁰ One risk is that the Chinese government might require Chinese companies doing business in Israel to share insights with the Iranian government in order to win friends and influence in Tehran. Another risk is that Beijing could use the fact that the same companies build major infrastructure both in Israel and in Iran to create political leverage on Israel (e.g., to support China's positions in the South China Sea).⁴¹ According to Harel Menashri, head of the cyber department at the Holon Institute of Technology and a former official in the Shin Bet, if Israel seeks to strike Iran, China could damage infrastructure operations in Israel to signal to Israel that it should not attack.⁴² Such a fear is likely overstated, but Israeli experts think that Israel should not provide a foreign governmental entity such leverage.⁴³

Although companies from other countries that Israel does business with might also work in Iran, a key difference concerns the influence of the Chinese state: Many Chinese companies active in Israel are state-owned, and the Chinese government even has significant reach into private companies. Of the 33 Chinese companies we examined,

³⁹ Kanner and Ella, 2017.

⁴⁰ For more detail, see Andrew Scobell and Alireza Nader, *China in the Middle East: The Reluctant Dragon*, Santa Monica, Calif.: RAND Corporation, RR-1229-A, 2016, Chapter Four.

⁴¹ Discussion with former defense officials, Tel Aviv, April 30, 2019.

⁴² No Man's Land, 2019.

⁴³ Discussion with former Israeli defense officials, Tel Aviv, April 30, 2019.

ZTE and China Railway Tunnel Group are known to have conducted business in Iran. Moreover, ZTE violated U.S. sanctions on Iran, selling \$130.6 million worth of network and surveillance equipment to the government-controlled Telecommunication Company of Iran in 2010.⁴⁴ This sale included equipment that originated in the United States, leading the U.S. government to fine ZTE nearly \$900 million for export control violations.⁴⁵

The parent company of China Railway Tunnel Group has a \$2 billion contract to build a high-speed rail link between Tehran and Isfahan.⁴⁶ In May 2015, three months after the launch of the Iran project, the China Railway Tunnel Group won an \$800 million contract to build a portion of the Tel Aviv light rail.⁴⁷ China Railway Tunnel Group is building the red line of the rail, operating right by the Kirya area (Figure 4.3). Yehuda Bar-On, CEO of NTA, the Israeli governmental company that manages the construction of the light rail in the Tel Aviv area, said publicly that Israeli security services are providing guiding principles both on cyber and other security measures but that no formal government body in Israel has told them that working with Chinese companies could be an issue.⁴⁸ According to cyber experts interviewed in Israel, these measures include air gapping. However, air gapping might be insufficient protection in the medium term; therefore, it would be safer to prevent a Chinese company with ties to the Chinese government operate such a vital infrastructure in such close proximity to one of Israel's most sensitive facilities.⁴⁹

⁴⁴ Steve Stecklow, "Special Report: Chinese Firm Helps Iran Spy on Citizens," Reuters, March 22, 2012.

⁴⁵ U.S. Department of Justice, "ZTE Corporation Agrees to Plead Guilty and Pay over \$430.4 Million for Violating U.S. Sanctions by Sending U.S.-Origin Items to Iran," Office of Public Affairs, Washington, D.C., March 7, 2017.

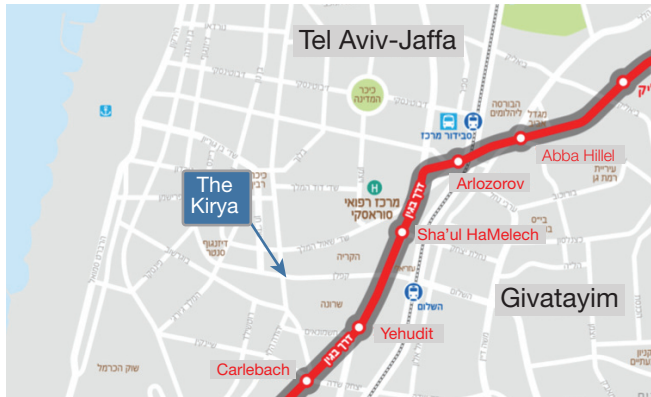
⁴⁶ "Iran Finalizes €2.2b Rail Deal with China's CMC—Exclusive," Financial Tribune, May 21, 2017; "Iran Launches \$2.7bn High-Speed Rail Project," *Trade Arabia*, February 26, 2015.

⁴⁷ "Chinese Company Connects Tel Aviv Rail, Tehran," *Times of Israel*, July 6, 2015.

⁴⁸ No Man's Land, 2019.

⁴⁹ Conversation with cyber experts, Tel Aviv, October 22, 2019.

Figure 4.3
Map of the Red Line of the Tel Aviv Rail Built by China
Railway Tunnel Group



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

Israeli Companies

Chinese investment in Israeli companies that develop sensitive technologies might present security concerns for either Israel or the United States. As discussed in Chapter Two, Chinese investment in overseas technology companies forms part of a larger pattern of technology transfer to develop China's domestic industries, and investment in Israel is no exception. In addition to the possibility that China could use acquired technologies to develop military and cyber capabilities that could be employed against the United States, a large-scale transfer of technology from Israel to China could potentially erode Israel's competitive advantage in the technology industry in the future.

In Table 4.2, we present a subset of Israeli technology companies that were the targets of Chinese investment, all of which are involved in developing sensitive technologies that, according to U.S. officials, could become the dual-use technologies of the future.⁵⁰

⁵⁰ Conversation with U.S. State Department official, December 1, 2019.

Table 4.2
Overview of Israeli Technology Deals

Israeli Entity	Company Information	Chinese Investors	Area of Risk
ThetaRay	Cybersecurity company that specializes in detection and prevention of advanced persistent threats, which are high-level cyber actors, usually nation states ^a	Alibaba	ThetaRay's products aim to detect and prevent cyber intrusions from Chinese government actors.
Kaymera	Cybersecurity start-up focused on mobile devices ^b	GoCapital	Kaymera's security products are marketed toward governments as well as businesses; Kaymera's founders have military security backgrounds. ^b
Toga Networks	IT and telecommunications company; the nature of Huawei's relationship with Toga is unclear ^c	Huawei	Potentially sensitive technologies; investment by Huawei, a company with suspect ties to the Chinese military and government.
HexaTier	Database security company; according to Reuters, "Huawei will use HexaTier to set up a research and development center in Israel for databases in the cloud" ^d	Huawei	Potentially sensitive technologies; investment by Huawei, a company with suspect ties to the Chinese military and government.

Table 4.2—Continued

Israeli Entity	Company Information	Chinese Investors	Area of Risk
Copyleaks	Company's product uses artificial intelligence to identify plagiarism	Identity unknown	Copyleaks' founders were formerly programmers in the 8200 unit in the Israeli Defense Forces, which is responsible for signals intelligence and is comparable to the National Security Agency in the United States. ^e

NOTES:

- ^a David Penn, "ThetaRay Lands \$5 Million Investment from Alibaba, Partners with PwC," Finovate Blog, December 4, 2015.
- ^b Gedalyah Reback, "Kaymera Nabs \$10 Million for its Super Secure Mobile OS," Geektime, February 1, 2016.
- ^c Hirschauge, 2016.
- ^d Tova Cohen and Catherine Cadell, "Huawei in Talks to Buy Israeli Cyber Company HexaTier: Sources," Reuters, December 20, 2016.
- ^e "AI Plagiarism Detection Co Copyleaks Raises \$1.1m," Globes, March 29, 2018.

Our concerns about Chinese investment in or acquisition of Israeli technology companies center on potential transfers of sensitive technology and China's weak IP rights enforcement. Chinese investment in companies developing semiconductors, AI, satellite communications, and other technologies that could have dual-use applications falls into the first category, even though the Israeli companies might not be working directly on military applications. China's weak enforcement of IP rights means that Israeli companies could suffer IP theft and that Israel could lose its competitive advantage in the technology industry.⁵¹

However, some Israeli officials and experts we talked with believe that these threats are exaggerated, especially with regard to Israel's cyberindustry. One current official noted that there are "natural barriers" to Chinese investment in the cyber sector: The main market for Israeli cybersecurity products and services is Western, which leads many companies to be wary of working with China, and China's data residency laws make many foreign companies hesitant to do business there.⁵² In terms of Israel potentially losing its competitive edge, an executive in an Israeli VC company believes that, although the Israeli market could do better in terms of anticipating long-term trends, Israel will continue to be competitive because of a cultural propensity for entrepreneurship as well as the continued flow of a high-skilled workforce, including software engineers, from the military.⁵³

Venture Capital

In addition to investing directly in Israeli companies, Chinese entities have been active in investing in Israeli VC firms, many of which invest heavily in other Israeli technology companies working in areas such as cybersecurity, AI, robotics, and other advanced fields. Table 4.3 provides a profile of several Israeli VC firms that have received Chinese funding and that invest in companies developing sensitive technologies.

⁵¹ Discussion with Israeli security experts, Tel Aviv, April 29–30, 2019.

⁵² Conversation with an Israeli government official, Tel Aviv, October 23, 2018.

⁵³ Conversation with an executive at an Israeli VC company, Tel Aviv, October 23, 2018.

Table 4.3
Overview of Israeli Venture Capital Deals

Israeli Entity	Company Information	Chinese Investors	Area of Risk
Singulariteam	VC fund that aims to “focus investments into new areas like machine learning, artificial intelligence and robotics” ^a	Tencent Holdings, Renren	Potential for dual-use technology; Singulariteam also raised funds from an “unnamed Russian investor.” ^a
Viola Ventures (formerly Carmel Ventures)	VC fund that invests in “Enterprise Software/ [Software as a Service], AI, Cloud Infrastructure, FinTech, Frontier Technologies (automotive, [internet of things], [Augmented Reality/Virtual Reality], drones), Big Data, Digital Media, Consumer Services, Semiconductors and more” ^b	Baidu, Ping-an, Qihoo, and Shengjing 360	Investments in potentially sensitive or dual-use technologies.
Canaan Partners	VC fund that invests in the following sectors: [software as a service]/ enterprise, mobile computing, and internet infrastructure ^c	Lenovo, Shengjing 360	Investments in internet infrastructure.
Catalyst (Catalyst CEL China Israel Fund)	Catalyst is a private equity firm that launched the first Israeli-Chinese fund with an investment of \$200 million from Chinese Everbright Ltd.; invests in technology and innovation companies, including SatixFyLtd, an Israeli provider of satellite communication ^d	China Everbright Ltd.	Investments in potentially sensitive or dual-use technologies; Conflict of interest: Catalyst head Yair Shamir is also the chair of NTA, the Israeli governmental company building the light rail in the Tel Aviv area. ^d

Table 4.3—Continued

Israeli Entity	Company Information	Chinese Investors	Area of Risk
OurCrowd	Small VC firm; portfolio includes cyber threat intelligence companies Thetaray and Kenna Security, AI companies Vayavision and Magisto, and robotics company Memic, among others ^e	Identity unknown	Investments in potentially dual-use or sensitive technologies; the identity of the Chinese investor is unknown, although an OurCrowd representative claimed the company received funding in its C round from “China’s most well-known internet company.” ^f
Pitango	One of Israel’s largest VC funds; has invested in 250 companies worldwide; portfolio includes semiconductor companies Anobit and Sckipio, text analytics company ClearForest facial recognition protection company D-ID, and cybersecurity companies ForeScout and Skycure, among many others ^g	Yongjin Group	Investments in potentially sensitive or dual-use technologies.
Jerusalem Venture Partners	VC firm focusing on cybersecurity (12 companies in its active portfolio), big data/predictive analytics (eight companies), media/next-generation tech (11 companies), and cloud and enterprise software (11 companies) ^h	Alibaba, Yongjin Group	Investments in potentially sensitive or dual-use technologies.

Table 4.3—Continued

Israeli Entity	Company Information	Chinese Investors	Area of Risk
MizMaa Ventures	Chinese-funded VC firm based in Israel, and investing only in Israeli companies; invests in artificial intelligence/machine learning, mobility (autonomous vehicles), cybersecurity, fintech/blockchain, and cloud/storage/server-less computing ⁱ	Identity unknown: three wealthy Chinese families ^j	Investments in potentially sensitive or dual-use technologies; MizMaa's four-person team includes a former employee of the U.S. Department of Defense and current member of the Board of Trustees for the National Defense University's Institute for National Strategic Studies, as well as an Israeli Air Force veteran who worked on the deployment of new aviation technologies ⁱ

NOTES:

^a Ingrid Lunden, "Israel VC Singulariteam Raises 2nd Fund, \$102M Backed by Tencent, Renren Founders," Techcrunch, January 28, 2015.

^b Viola Ventures, "Empowering Early-Stage Technology Companies to Become Global Category Leaders," webpage, 2017.

^c Canaan, homepage, undated.

^d Tali Heruti-Sever, "Yair Shamir Metsig: Ha'Malatim HaTsarfatiyim, Hakronot Hasiniyim, Hayoets Hamefukpak, Ve'Nigudei Hainyanim [Yair Shamir Present: The French UAVs, the Chinese Cars, the Shady Consultant, and the Conflicts of Interests]," *The Marker*, January 30, 2017.

^e OurCrowd, "Foreign Portfolio," webpage, 2018.

^f Zhang Feifei, 以色列热的冷思考 ["Cool Reflections on 'Israel Fever'"], *Economic Observer Online*, October 22, 2016.

^g Pitango Venture Capital, "About," webpage, undated; Pitango Venture Capital, "Our Portfolio Companies," webpage, undated.

^h Jerusalem Venture Partners, "Companies," webpage, undated.

ⁱ MizMaa, homepage, 2018.

^j Idan Rabi, "Chinese Fund MizMaa to Invest \$100m in Israeli Startups," *Globes*, June 13, 2017.

Although VC does not provide direct access to a company's technology, an investor might have access a company's technical roadmap for their development; the company's intellectual property; information about how competitive the company might be in the market; insight into business decisions, budgets, and human resources; and the company's plan for conquering the market.⁵⁴ A company might fear that its Chinese investors are politically influenced as opposed to making decisions based purely on business motivations.⁵⁵ Another risk could be that if an Israeli company were to develop something unique or particularly sensitive, a Chinese investor could have knowledge of the company's customers, including whether the product is used by government organizations.⁵⁶

Conclusion

Chinese investment in Israel's technology sector creates risks for potential transfer of sensitive technologies that could help China develop military and cyber capabilities contrary to U.S. interests, and could erode Israeli and U.S. competitive advantage in a key sector of their economies. The construction and operation of Israeli vital infrastructure, including Israel's only two ports on the Mediterranean, by Chinese state-owned companies present cyber and espionage risks that could have implications for U.S. as well as Israeli national security. The following chapter discusses the risks and implications in greater depth.

⁵⁴ Conversation with an executive at an Israeli VC company, Tel Aviv, October 23, 2018.

⁵⁵ Conversation with an executive at an Israeli VC company, Tel Aviv, October 23, 2018.

⁵⁶ Conversation with an executive at an Israeli VC company, Tel Aviv, October 23, 2018.

Security Risks for Israel and the United States

In previous chapters, we touched on some of the security risks created by China's investments in sensitive technologies and vital infrastructure projects in Israel. In this chapter, we look more closely at four categories of risk:

1. government or military connections of Chinese companies doing business in Israel
2. cyber and intelligence threats arising from Chinese investments and construction activities, including sensitive technologies, cyber espionage, and vital infrastructure vulnerabilities
3. the incompatibility between Israel and China's interests in the Middle East
4. threats to U.S. interests and the impact of Israel's dealings with China on its relationship with the United States.

Government or Military Connections of Chinese Companies Doing Business in Israel

It is widely accepted that most Chinese companies are linked with the Chinese government, the People's Liberation Army (PLA), Chinese princelings, or the Communist Party. The degree of control that the government can exercise differs between companies, but the Chinese state still has considerable influence over decisions relating to business

personnel, investments, and activities at home and abroad.¹ The close relationship between Chinese companies and the state suggests that commercial activities are not motivated solely by economic considerations, like other private, profit-seeking businesses, but also by China's strategic motivations.

Official Chinese involvement in business operations allows the country to leverage its economic power to advance its geostrategic interests. For example, in 2013, China reportedly conditioned Netanyahu's visit to China on Israel ending its involvement in a New York federal court case against the state-owned Bank of China, which had been accused of laundering Iranian money for the terrorist groups Hamas and Palestinian Islamic Jihad.² Involvement by Israeli defense officials had been a critical component of the case. Under Chinese pressure, Netanyahu allegedly guaranteed that senior defense officials would refrain from testifying in court; a lack of expert witnesses led to dismissal of the case.³ This case led to increased tensions between the Israeli government and the White House, Congress, and U.S.-based

¹ Scott Cendrowski, "China's Global 500 Companies Are Bigger than Ever—and Mostly State-Owned," *Fortune*, July 22, 2015; Sherisse Pham, "Why China's Tech Giants Are Cozying Up to the Communist Party," *CNN Business*, November 4, 2018.

² In 2008, the family of Daniel Wultz, a 16-year-old (and a relative of Representative Eric Cantor, former House Majority Leader) who died in a suicide terror attack in Tel Aviv in 2006, launched legal action against the Bank of China. The case represented the families of 20 families of American victims of terror attacks that took place in Israel in from 2003 to 2008. They sued the Bank of China's branch in Guangzhou for funneling Iranian money to Palestinian terrorist organizations that backed the attacks that killed Daniel Wultz and the other victims. Israel reportedly urged the family to start legal proceedings and promised to provide them with evidence, including expert witnesses, one of whom was a former counterterrorism official named Uzi Shaya, who had tracked the bank of China case and pressed it to close the problematic accounts, to no avail. In 2013, however, as Netanyahu's visit to China was approaching, Shaya told the Wultz family he was threatened by Israeli officials not to testify in the case. The Wultz lawyers subpoenaed him to force the testimony but Israel answered on his behalf by filing a petition against the Wultz family, arguing that any testimony could harm Israeli security by revealing state secrets. More details are available in Roger Cohen, "Did Israel Put Money over Justice?" *New York Times*, February 28, 2015.

³ Yonah Jeremy Bob, "Exclusive: Historic Case Against Bank of China for Millions in Terror Financing Dismissed," *Jerusalem Post*, November 8, 2015.

Jewish organizations, which accused Netanyahu of caving in to Chinese pressure.⁴

China has also been able to affect the behaviors of non-Chinese private companies, which has implications for the independence of Israeli firms. In February 2018, the car company Daimler bowed to Chinese pressure and apologized for a quote attributed to the Dalai Lama posted on the company's Facebook page. China is Mercedes-Benz's largest car market and accounts for approximately one-quarter of the company's sales.⁵ Israeli companies might also be vulnerable to similar mechanisms through which China can exert its power and control.⁶

Through its investment and construction activities, China has developed its own network of lobbyists to do its bidding and has placed a number of individuals in Israel to encourage sales to China or to advocate for policies or tenders on China's behalf. Because Israel sees China as a key partner contributing to the Israeli economy, one former Israeli official stated that Israel might avoid expressing criticism of China or discussing the potential threat posed by China to Israel's security because of high-level political support for the Israel-China relationship.⁷ Interviews with multiple Israeli officials confirm that China generally is viewed in a positive light; Israelis feel that Chinese investment brings more benefits than it does risks.⁸ This positive message resonates within Israel's commercial industry and is echoed through Israel's government, except among defense officials. Nonetheless, U.S. pressure and growing coverage of the issue in Israeli press has raised awareness of the risks associated with growing Chinese investment in Israel.

⁴ Shimon Shiffer, "U.S. Outraged After Israel Backs Out of Terror Suit," *Ynet News*, May 15, 2013.

⁵ Sui-Lee Wee, "Mercedes-Benz Quotes the Dalai Lama. China Notices. Apology Follows," *New York Times*, February 6, 2018; Paul Mozur, "China Presses Its Internet Censorship Efforts Across the Globe," *New York Times*, March 2, 2018.

⁶ Discussion with Israeli and U.S. security experts, Tel Aviv, April 29, 2019.

⁷ Conversation with former Israeli official, Tel Aviv, October 22, 2018.

⁸ Conversation with current and former Israeli officials, October 21–23, 2018.

Cyber and Intelligence Threats Arising from Chinese Investments and Construction Activities

Chinese investment in sensitive technologies and the construction and operation of vital infrastructure present a number of cyber- and intelligence-related risks for both Israel and the United States.

Sensitive Technologies

One issue concerns China's interest in acquiring technologies that can be used for both commercial and military purposes. Whether China is striving to be *a* global power or *the* global power, it makes sense that China would want to acquire the technologies and establish the infrastructure needed to defend its growing investments and its interests abroad. Therefore, one can reasonably assume that China's technology acquisitions likely will be used by its military and defense establishment, much in the same way the United States relies on proprietary and sensitive technologies to project power and influence and secure its global interests. Douglas Feith, the director at the Center for National Security Strategies at the Hudson Institute, accurately notes that many civilian cyber-defense technologies used for commercial purposes are "the top of the line that militaries should adapt and use for their own purposes."⁹ As China continues to expand its reach throughout the globe, it only makes sense that China's military will be close behind as it works to defend China's growing backyard.

Through MIC 2025, the Chinese government has created both a strategy and a roadmap to help guide China toward the development of dual-use technologies and the two-way transfer of technology between the military and civilian sectors.¹⁰ The plan names ten sectors that are priorities for development, including new generation information technology, high-end numerical control machinery and robotics, and maritime engineering equipment and high-tech ship-

⁹ Anna Ahronheim, "Naval Experts Concerned over China's Increasing Presence in Mediterranean," *Jerusalem Post*, August 23, 2018.

¹⁰ State Council, 2015a, Sections 2(1), 3(1), and 3(3).

ping, all of which are considered dual use.¹¹ Moreover, China's effort to become a global power and a world leader in technological innovation is associated with risks. As part of MIC 2025, China uses government subsidies, mobilizes state-owned enterprises, and acquires intellectual property to eventually surpass technological knowhow in advanced industries.¹² Consequently, investment in Israeli companies focusing on cyber security, AI, facial-recognition, 3-D printing, virtual reality, maritime engineering equipment and high-tech shipping, and autonomous vehicles¹³—again, all not currently defined as dual-use but potentially so in the future—is particularly worrisome.¹⁴

Cyber Espionage and Theft of Intellectual Property

Cyber espionage has had a devastating impact on U.S. economic and security interests, especially as a mechanism to enable the transfer of sensitive technology. Reportedly, China is the most active foreign power engaged in the illegal acquisition of American technology.¹⁵ To cite one example related to Israel, between 2011 and 2012, alleged Chinese cyber hackers stole sensitive information relating to Israel's Iron Dome, the antimissile defense system that intercepts and destroys incoming rockets. According to Cyber Engineering Services, the company that conducted the forensic analysis of the attack, hackers not only used sophisticated cyber tools similar to those used by known Chinese hackers but also targeted two Israeli defense contractors, Israeli Aerospace

¹¹ State Council, 2015a, Section 3(6). The other seven priority sectors are: aviation and aerospace equipment, advanced rail transport equipment, energy-saving and new energy vehicles, electrical equipment, agricultural machinery and equipment, new materials, and biomedical and high-performance medical equipment.

¹² James McBride and Andrew Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?" *Council on Foreign Relations*, August 2, 2018.

¹³ It is important to note that the Israeli tech market is primarily geared toward Western countries but, as noted earlier, Chinese investment in companies that produce sensitive technologies and VC companies that invest in such technologies has been on the rise.

¹⁴ Paul Mozur and Jane Perlez, "China Tech Investment Flying Under the Radar, Pentagon Warns," *New York Times*, April 7, 2017.

¹⁵ Jack Murphy, "Here's What Sets China's International Espionage Apart from Everyone Else," *Business Insider*, July 11, 2015.

industries and Rafael Advanced Defense Systems, compromising their civilian unclassified networks and stealing intellectual property related to Arrow III missiles, unmanned aerial vehicles, and ballistic rockets.¹⁶ In addition to the concerns raised by China's cyber espionage activity, some of the information stolen contained IP data that was controlled by U.S. government International Traffic in Arms regulations.¹⁷ Most of the Arrow III technology was designed by Boeing and other U.S. defense contractors, not Israel—so China's exfiltration of Israeli-held technical data possibly compromised U.S. military systems as well.

The illegal transfer of sensitive technological data through cyber-enabled commercial espionage, as well as traditional open-source collection, is a serious risk for Israel and the United States. China's investment in Israeli cybersecurity companies could create particular issues for the United States, given that the transfer of proprietary information used to develop these cybersecurity capabilities might be either used by China to bolster its own cyber defenses or reverse-engineered to identify zero-day vulnerabilities within the software that China might later exploit. Chinese companies have invested in such Israeli cyber startups as Kaymera, which provides mobile device security solutions to governments as well as businesses, and Thetaray, which aims to guard against intrusions by nation-state cyber actors.¹⁸ Chinese VC companies MizMaa Ventures and China Everbright Ltd. also have several cybersecurity companies in their portfolios.¹⁹

Additionally, China's human intelligence gathering efforts certainly aid in the identification of desirable technologies and information and likely will grow as China sends more and more personnel abroad to oversee and take part in the many construction projects and investments in other countries' key infrastructure and sensitive technologies, including in Israel. Academic cooperation and student and

¹⁶ Keck, 2014.

¹⁷ Joe Miller, "Israeli Iron Dome Firms 'Infiltrated By Chinese Hackers', *BBC News*, July 31, 2014. See also Brian Krebs, "Hackers Plundered Israeli Defense Firms that Built 'Iron Dome' Missile Defense System," *KrebsOnSecurity*, July 28, 2014.

¹⁸ Reback, 2016; Penn, 2015.

¹⁹ MizMaa, 2018; Catalyst Fund, homepage, undated.

faculty exchanges are important in this context. The openness of academic environments means that foreign nationals, including Chinese nationals, might have access to research funded by the U.S. military and gain access to sensitive research.

Beginning in the past decade, Israel and China have substantially expanded academic cooperation. Israel has four academic institutions in China. Israeli institutions in China include the XIN Center, a “joint center for innovative research and education to be funded by government and private enterprise”²⁰ and Guangdong Technion Israel Institute of Technology in Shantou,²¹ the first Israeli university in China.²² Although China does not have academic institutions in Israel, it has expanded its cultural presence on campuses through Confucius Institutes at Tel Aviv University and the Hebrew University of Jerusalem;²³ these cultural institutions are formally designed to promote Chinese language and culture.²⁴ However, the U.S. Senate’s Permanent Subcommittee on Investigations Senate concluded in February 2019 that Confucius Institutes are tightly controlled arms of the Chinese government, whose employees might, under U.S. law, need to register as foreign agents.²⁵

Vital Infrastructure Vulnerabilities

Chinese investment and construction activities also create numerous opportunities for cyber-enabled and open-source intelligence collec-

²⁰ Tova Cohen, “Tel Aviv, Tsinghua Universities Set Up \$300 Mln Research Center,” Reuters, May 19, 2014.

²¹ Ellie Bothwell, “Israel Looks to Asia,” *Inside Higher Ed*, July 14, 2017.

²² Technion Israel Institute of Technology, “Launch of First Israeli University in China,” press release, December 19, 2017; Avi Blizovski, “Machon Chadash: Ha’Sinim Yilmedu Chadshanut Meha’Yisraelim [New Institute: The Chinese Will Learn Innovation from the Israelis],” *PC Anashim U’Mechasvim*, December 26, 2017.

²³ Confucius Institute Headquarters, “About Confucius Institute/Classrooms,” webpage, 2014.

²⁴ Confucius Institute Headquarters, 2014.

²⁵ Patricia Zengerle, “Senate Panel Wants Chinese-Funded Institutes to Change or Leave U.S.,” Reuters, February 27, 2019.

tion. Using the Port of Haifa as an example, the Shanghai International Port Group secured a contract to operate a portion of the port for 25 years, beginning in 2021. The contract included a classified security appendix that, according to the parts we have seen, specifies limitation on the Chinese company and defines the authority of the Shin Bet in regards to the port.²⁶ However, some experts are concerned that implementation of the security appendix in practice could be lacking, meaning that the physical location of Chinese construction workers and operators, combined with the ability of Chinese companies to exploit weaknesses regarding use of domestically sourced communications equipment and access to sensitive sites like industrial control systems, might provide Chinese workers with high levels of access to potentially sensitive information.²⁷ From a commercial perspective, Chinese workers can collect information about day-to-day operations to try to gain a competitive advantage for Chinese companies in the markets. From a military perspective, workers can also monitor activities like increases in operational tempo by Israel, the United States, or other nations; how Israel or the United States moves materiel on and off ships; and how Israeli and U.S. ships replenish themselves. During the construction phase, Chinese companies could use their own hardware and software to monitor the activities of the nearby military port or enable cyber accesses into Israeli industrial control systems.²⁸

²⁶ Conversation with a U.S. State Department official, March 6, 2019. The security appendix reportedly includes several directives including that personnel in certain roles will be Israeli nationals holding security clearances; that the operator has to comply with instructions of any authorized authority including the Israeli Defense Forces, General Security Services (Shin Bet), Israeli Police, Home Front Command, and Fire Department; and that the Shin Bet will receive data on people and goods, as well as be able to connect to systems that monitor and track movement by people and goods.

²⁷ The security appendix and the division of labor on the port between the Chinese and Israeli operators should (in theory) prevent a situation in which China could deny the use of Haifa port by the U.S. military during a crisis (Conversation with a U.S. State Department official, March 6, 2019; conversation with Israeli and U.S. security experts, Tel Aviv, April 29–30, 2019).

²⁸ Conversation with U.S. naval warfare expert, September 19, 2018; Harel Menashri, head of the cyber department at the Holon Institute of Technology and a former official in the

Through its construction and operation of Israeli vital infrastructure, China might also use various forms of cyber and electronic collection to gain information about U.S. commercial and naval operations. For example, when a U.S. Navy ship comes into port, China might be able to identify its electronic warfare capabilities, what signatures the ship is emitting, or what kinds of radars are on board. In addition, the ships themselves are increasingly exposed to more interference and thus more cyber risk. Of course, an adversary can gather this information through other means, but the operation of a port creates additional and beneficial opportunities to do so.²⁹

Finally, there are numerous ways an adversary could hack into naval vessels and port infrastructure: inserting USB drives loaded with malicious software; infecting diagnostic and maintenance equipment with malicious software; stealing information or sabotaging systems via malicious insiders; installing network equipment to provide direct, persistent remote access; infecting equipment through the supply chain prior to delivery; as well as numerous other attack vectors into allegedly “closed” and “air gapped” systems of naval vessels and port operations. Of course, foreign agents can pursue such nefarious activities without having to operate a port. Moreover, security protections as described in the classified appendix of the port contract are designed to address such concerns. However, experts contend that risks would remain, especially when considering the friendly and open character of Israel, who might grant Chinese port employees access to which they are officially denied.³⁰

As major corporations—including U.S. defense manufacturers—gain greater understanding of the threats posed by poor supply chain management, it is understandable that the United States would be wary of Chinese-funded foreign, including Israeli, products. A small tech firm based in Portland, Oregon, had unknowingly been using

Shin Bet, spoke on television about his concerns for Israel in the naval domain (see No Man’s Land, 2019).

²⁹ Amber Corrin, “Can the Navy Protect This Ship from Hackers?” *Fifth Domain*, April 30, 2018.

³⁰ Conversation with former government officials, Tel Aviv, October 22, 2018.

hardware inserted by China. Amazon Web Services, in coordination with another third-party security company, found microchips that had been secretly embedded in the motherboards of Elemental's servers.³¹ The purposes of these microchips have not yet been disclosed, but the striking concerns created by the discovery of China's covert corruption of Elemental's supply chain resonated far beyond the walls of these companies and serves as just one example of the risks associated with Chinese investment in and acquisition of sensitive technologies.

Although Israel can take steps to mitigate some of these risks, it is not clear how many of these steps have been taken. Israeli officials argue that the ports of Haifa and Ashdod are protected against potential cyber intrusions through their classification as "vital" infrastructure, which affords extra protections to the operating mechanisms or component systems of the ports that have been defined this way.³² However, any equipment installed prior to the designation of port infrastructure—or any other type of infrastructure—as "vital" is not subject to increased scrutiny and does not receive additional protections. Also, much of the existing infrastructure is out of date and not likely to be replaced, which increases the likelihood that an adversary could maintain persistent and remote access into vital operating infrastructure.³³ In addition, in light of the State Comptroller's May 2019 report that severely criticized cybersecurity in three vital infrastructure facilities, despite the proper designation, ports might not be as well protected.³⁴

Although much attention has been devoted in the press to the issue of the Haifa Port, the construction of portions of the Tel Aviv light rail near IDF headquarters also offers China surveillance opportunities and perhaps leverage. Former National Security Advisor Yaakov Amidror stated that in the worst-case scenario, a Chinese company could leave a "red button" that would enable Beijing to stop the light

³¹ Jordan Robertson and Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," *Bloomberg*, October 4 2018.

³² Conversation with an Israeli official, Tel Aviv, October 23, 2018.

³³ Conversation with an Israeli official, Tel Aviv, October 23, 2018.

³⁴ Shapira, 2019.

rail if it wishes to do so. He said, “Even if China does so, the State of Israel would not collapse. Rather, Israel would switch to a non-Chinese system within a year. But if China does something like that, Beijing would lose the international market because no country will continue to buy from it.”³⁵ However, former Mossad head Efraim Halevy has argued that the Chinese are too strong and would not be affected substantially even if they are caught doing something wrong.³⁶ Therefore, this threat might not be a sufficient deterrent.

Incompatibility Between Israeli and Chinese Interests in the Middle East

Despite the positive views of the China-Israel relationship within both commercial industries and the nonsecurity parts of the government, Israel faces the potential for conflict in its relations with China because of the incompatibility between the countries’ interests in the Middle East. China’s interests in the region are motivated primarily by its energy dependence, which demands good relations with countries in the Arab world and Iran. China’s positions and activities in the region and in international organizations conflict with Israel’s. China has frequently opposed any military actions against Iran and does not consider the Iranian-backed Lebanese Hezbollah to be a terrorist organization.³⁷ The same Chinese companies that are working in Iran are also involved in Israel, including in construction of strategic infrastructure. China has also supplied hundreds of millions of dollars of weapons to Iran since 2000,³⁸ and it has a long history of cooperation with Iran’s missile and nuclear programs.³⁹ China also supports the Palestinian

³⁵ No Man’s Land, 2019.

³⁶ No Man’s Land, 2019.

³⁷ Scobell and Nader, 2016.

³⁸ Scobell and Nader, 2016.

³⁹ John Garver, “China-Iran Relations: Cautious Friendship with America’s Nemesis,” *China Report*, Vol. 49, No. 1, 2013, p. 84.

position in international fora⁴⁰ and consistently votes against Israel in the UN.⁴¹ Some Israeli security experts contend that given Chinese regional priorities, Israel might need to think a bit more about the extent to which it helps Beijing strengthen its position with access to Israeli technology and infrastructure.⁴² In addition, given the rivalry between the United States and China, Israel could risk finding itself on opposing sides with Washington—its most important security, diplomatic, and economic patron. We discuss the latter issue in more detail later in this chapter.

MIC 2025 poses unique challenges to Israel. The plan prioritizes ten high-tech industries, including agricultural technology, biomedicine, next-generation information technology (IT) and telecommunications, advanced robotics, and AI⁴³—areas of Israeli dominance. The implication is that China should not be seen only as a customer, investor, or partner in the development of Israeli technology, but rather as a direct competitor that benefits from adoption, improvement, and adaptation of technologies originated in Israel.⁴⁴

Chinese companies have access to immense government financial resources, and could crowd out non-Chinese competitors without such access, increasing the risk for substantial concentration of assets in the hands of Chinese entities at the expense of local and other foreign businesses.⁴⁵ This issue is particularly worrisome in Israel, a small and concentrated economy.⁴⁶ For example, Israel's Construction Association, which represents all organizations, corporations, and entities in

⁴⁰ Charlotte Gao, "What's China's Stance on Trump's Jerusalem Decision?" *The Diplomat*, December 7, 2017.

⁴¹ Conversation with a senior Israeli government official, Jerusalem, July 2017.

⁴² Conversation with Israeli security experts, Tel Aviv, April 30, 2019.

⁴³ "Made in China 2025' Plan Revealed," *Xinhua*, May 19, 2018.

⁴⁴ Ella, 2019a.

⁴⁵ The term *crowding out* is used to describe a situation when a government outspends the private sector, making it impossible for the private sector to compete and removes any impetus for the private sector to invest. In the long run, crowding out creates systemic inefficiencies because it eliminates competition and hampers innovation.

⁴⁶ Conversation with an Israeli former official, Tel Aviv, October 23, 2018.

the construction and infrastructure sectors, has formally petitioned to designate Chinese construction and infrastructure companies working in Israel as having excessive market power and violating antitrust restrictions. The association argues that Israeli companies cannot compete with the deep pockets of Chinese companies, especially as tenders prioritize low cost over other considerations.⁴⁷

Impact on the Israel-U.S. Relationship

In addition to cyber and intelligence threats and traditional hard power concerns, China appears to be using its investment and other soft power activities to help achieve its economic, political, and security goals throughout the world, with important implications for the United States.

Chinese state-owned companies now control two ports in Asia—one in Sri Lanka, the other in Pakistan—with one in Myanmar and one in Bangladesh on the way.⁴⁸ These countries lie on one of the most heavily trafficked waterways on earth, lending credibility to assertions that such infrastructure projects help China secure both its economic and maritime security interests through a “string of pearls” concept, connecting China with ports throughout Southeast Asia and stretching into Africa. Although these four ports currently are only used for civilian purposes, in 2017, China opened its first overseas military base in Djibouti. China plans to build its second offshore naval base on the Jiwani Peninsula, near the Iranian border and the existing civilian port of Gwadar in Pakistan.⁴⁹ Figure 5.1 highlights current and possible “dual-use” ports.

⁴⁷ Sonia Gorodisky, “Hachrizu al Chevrot Ha’Bniya Ha’Siniyot Be’Yisrael Kegorem Rikuzi [Declare Chinese Construction Companies in Israel as Concentration Element],” *Globes*, July 26, 2017.

⁴⁸ Peter S. Goodman and Jane Perlez, “Money and Muscle Pave China’s Way to Global Power,” *New York Times*, November 25, 2018.

⁴⁹ Minnie Chan, “First Djibouti . . . Now Pakistan Port Earmarked for a Chinese Overseas Naval Base, Sources Say,” *South China Morning Post*, January 5, 2018. See also “Gwadar Port About China’s Interests, Not Pakistan’s: US Think-Tank,” *Economic Times*, February 9, 2018.

Not surprisingly, Chinese infrastructure projects have been focused on strategic maritime traffic ways, such as the Strait of Malacca, the Strait of Hormuz, the Bab al-Mandab, and the Suez Canal.⁵⁰ Several of these maritime corridors are in areas of current instability, where the U.S. Navy has historically patrolled to ensure freedom of navigation, necessitating a degree of friendly relations between China and the United States. With growing Chinese diplomatic and commercial investments in these countries, however, China is liberating itself from

Figure 5.1
China's Dual-Use Ports



SOURCE: Kyngé et al., 2017.

NOTE: *Dual use* is defined as Chinese owned or invested ports confirmed, or proposed, as engaging in both commerce and military use.

*China has not invested in a port, but its navy uses Seychelles' facilities in anti-piracy operations in the Indian Ocean.

**The United States has expressed concern over the possible use of Chinese-owned Darwin port for military purposes.

⁵⁰ "Strait of Malacca Key Chokepoint for Oil Trade," *Maritime Executive*, August 27, 2018; Aldo Premoli, "The Evolving Role of Maritime Straits," *Global Risk Insights*, December 13, 2016; James Kyngé, Chris Campbell, Amy Kazmin, and Farhan Bokhari, "Beijing's Global Power Play: How China Rules the Waves," *Financial Times*, January 12, 2017.

a reliance on the U.S. Navy, expanding its economic and geopolitical influence, and quietly moving toward replacing the United States as the dominant power. One security risk is that China's navy might seek opportunities to exert itself against the U.S. Navy, leading to increased opportunities for hostilities between the two countries' navies as they both vie to police the same tense waterways.

From a geostrategic perspective, Chinese investment activities in Israeli vital infrastructure are of concern to some in both Israel and the United States. Using the Haifa port as an example again, the U.S. Navy 6th Fleet docks at least once a year at Haifa port for two primary reasons: first, to participate in a biennial naval exercise known as "JUNIPER COBRA", and second, to support ballistic missile defense (BMD).⁵¹ At any given time, there is always a U.S. ship in or near the eastern Mediterranean to bolster Israel's land-based ballistic missile defenses by providing sea-based BMD support. For that reason, some argue that the Haifa port has become an emotional and contentious issue between Israel and the United States. However, there are also actual possible risks.⁵² If there is real concern that Chinese presence in Israeli ports would offer unique information collection capabilities, the United States might have to weigh its interests in the region against the risks. As a result, additional analysis on the effects of Chinese port operations on U.S. strategy in the region warrant consideration and further research.

Although the geostrategic nature of China's commercial activities is well documented, many of the Israeli officials that we talked with did not view China's activities as a threat per se, let alone part of a broader Chinese objective to posture itself—both economically and militarily—around the globe. However, most of them expressed concerns about taking money from China because doing so could impact relations with the United States. According to Israeli researchers interviewed for this project, China understands the U.S. restrictions placed on military technology, so they work to acquire sensitive technologies

⁵¹ U.S. Navy, "NMCB 11 Prepares for Juniper Cobra 18 in Israel," press release, March 12, 2018.

⁵² Discussion with U.S. naval expert, by phone, September 14, 2019.

that could have dual-use applications through the commercial market instead.⁵³ Because of this, some in Israel are concerned that the United States would stop buying technology from Israel if they feared that Chinese money potentially provides China with control over or backdoors into such technologies. In addition, given the tenuous U.S.-Chinese relations, some Israeli security experts we interviewed raised the question—why would Israel help Beijing strengthen its capabilities and grasp in the Middle East, and indirectly weaken Washington, Israel’s most important strategic ally?⁵⁴

Israeli officials we talked with believe that Israel’s relationship with China has the potential to negatively affect its close ties to the United States. Israel relies on the United States for security, economic ties, and geopolitical assistance, and the China-U.S. relationship has grown increasingly tense in recent years. The U.S. government is concerned about transfers of U.S. technology or about any technologies that give China a military edge. Since early 2019, U.S. officials have begun warning Israel *publicly* about Chinese involvement in Israeli technology and infrastructure. Israeli press reported in March 2019 that President Trump warned Netanyahu that continued deepening Israeli ties with Beijing could strain the U.S.–Israeli security relationship.⁵⁵ In the same month, U.S. Secretary of State Mike Pompeo said that Chinese investment in Israel could strain sharing and other security cooperation with Washington.⁵⁶ Secretary of Energy Dan Brouillette issued a similar warning in January, saying that continued Chinese investment in Israel could limit intelligence-sharing with its allies.⁵⁷ As a result of mounting U.S. pressure, on October 30, 2019, the Israeli government announced the formation of a new advisory committee to help screen foreign investments in the coun-

⁵³ Conversation with Israeli academic researchers, Tel Aviv, October 21, 2018.

⁵⁴ Conversation with Israeli security experts, Tel Aviv, April 30, 2019.

⁵⁵ Ravid, 2019.

⁵⁶ “Pompeo Warns U.S. Could Curb Security Ties with Israel over China Relations,” *Times of Israel*, March 21, 2019.

⁵⁷ “Israeli Minister Reassures U.S. over Chinese Telecoms Investment,” 2019.

try. Despite the limitations of the committee, which we based on the cabinet's announcement as explained in Chapter Three, its mere existence and the discussions about U.S. alarm over Chinese involvement in Israeli technology and investment indicate that, as with the Phalcon and HARPY incidents, Israel understands that it should continue to play a balancing act as it moves its relations with China forward.

Conclusion

The interconnectedness of China's economic, political, and security policies is important to consider when assessing Chinese investment in Israeli technology. China's intelligence apparatus is directly linked to its internal foreign policy, national security, and economic decision-making processes. Although many countries rely on intelligence gathering services to inform their defense and foreign policies, China is unique in the way in which it views its economic and security strategies as one in the same. As a result, it is extremely difficult to assess the motives behind China's actions because the same motives drive China's economic and commercial activity, political and diplomatic policies, and actions taken to support China's national security. Nevertheless, Israeli officials interviewed for this study noted that Chinese investment in technologies and vital infrastructure is often pursued "under the guise of maintaining a trade route from the Indian Ocean via the Suez Canal to Europe."⁵⁸

As Israel continues expanding its ties with Beijing, it is important that it views Chinese investment activities as multifaceted and takes appropriate actions to mitigate against the potential threats that they might create.

⁵⁸ Amos Harel, "Israel Is Giving China the Keys to Its Largest Port—and the U.S. Navy May Abandon Israel," *Haaretz*, September 17, 2018; Conversation with former Israeli official, October 2018.

Concluding Thoughts and Research Gaps for Further Study

On October 30, 2019, the caretaker Israeli government announced the establishment of a new advisory committee for screening foreign investment with an unstated, yet clear, focus on Chinese investment. At the time of writing, the announcement has not been implemented, and the committee's effectiveness cannot be assessed. The shifting conversation in Israel and the establishment of an investment screening mechanism are signs that things are heading in the right direction. Still, however, the degree of Chinese interest in sensitive technologies, and the ways in which the Chinese state has acquired technological data related to the development of sensitive and dual use technologies raises possible risks. Former Shin Bet chief Yaakov Peri stated China tries "to get from Israel anything that can help their economy. As part of these efforts, Chinese officials can easily get information from Israeli officials in a long list of companies."¹ Although Peri mentioned that some protections exist to regulate the types of information transferred to China, he also noted these protections do not ensure that "critical data will not get into the wrong hands."²

Concerns over the transfer of sensitive technology to foreign entities extend beyond foreign investments to include the actual sale of technologies and academic cooperation as well (not investigated in this report). Like the United States, Israel requires special export licenses to sell dual-use technologies to foreign companies or govern-

¹ Egozi, 2018.

² Egozi, 2018.

ments. According to an article in *The Economist*, and as echoed by a current government official in Israel, there are plenty of loopholes to get around these laws.³ In an interview, one former Israeli intelligence official noted that Israel has no serious mechanism to ensure that it does not sell off its economic advantage and technological know-how.⁴ With the expansion of CFIUS guidelines under FIRRMA, the United States and its allies must determine what technologies they see as potentially damaging to national security interests not just in the present but also five to ten years down the road. As Israel asks what its relationship will be with China in the future, the United States and its allies might also find themselves asking what kinds of sensitive and potential dual-use technologies could alter the existing environment of strategic competition between the United States and China. The United States then should be able to effectively communicate to its allies which technologies are posing the most serious risks and why they do so.

Academic experts argue that Chinese investment and construction in Israel are generally beneficial, but that Israel needs to identify specific actions that China or any other foreign investor cannot take, such as providing their own telecommunications equipment or their own hardware and software components for industrial control systems; identifying restricted access areas on port or rail sites; or, documenting specific roles and responsibilities of port operators. Israel should also ensure it has the capacity to implement security measures when such are put in place.⁵

Based on conversations with over a dozen experts, Israel traditionally has not systematically evaluated the broader security concerns that arise from Chinese investment and construction in Israel. The new committee, once it becomes operational, might improve that.

³ Conversation with an Israeli official, October 22, 2018. See also “Too Open for Business? Israel’s Ties with China Are Raising Security Concerns,” 2018.

⁴ Conversation with former Israeli official, Tel Aviv, October 22, 2018.

⁵ Conversation, Israeli academic researchers, Tel Aviv, October 2018. Some of these specifications are included in parts of the classified appendix that accompanies the port contract which have received through unofficial channels. However, following the State Comptroller report that criticized the state of cybersecurity in vital infrastructure facilities, even if security measures were indeed specified, implementation could be lacking; Shapira, 2019.

However, until late 2019, Israel tended to prioritize the benefits it receives from the relationship with China—mainly start-up funding and market access. Interestingly, experts we interviewed thought the biggest issue resulting from Chinese investment was the possibility of China controlling access to Israeli ports and giving preferential treatment to Chinese ships and businesses. They argued that Israel needs to diversify against possible Chinese control of important Israeli sectors and work with other vendors and companies within other partner countries. Economic diversification is one way to limit Chinese influence over commercial activity, but it might be difficult to do so, as researchers noted that China has a substantial foothold in the Israeli market for infrastructure construction. In addition, it is important to note that concern focuses not only on whether China might monopolize certain sectors but, more importantly, that the Chinese companies involved in these sectors are state-owned, resulting in a degree of control over Israeli sectors granted to a foreign government. No other firm, let alone country, is as economically competitive, inexpensive, or efficient as Chinese infrastructure companies. Despite the fact that many in Israel recognize China's tendency to use its economic investment for political purposes and long-term geostrategic advantage, these concerns are in direct tension with the near-term benefit of low-cost, yet reliable, Chinese services, even though Israeli defense officials are aware of the risks deepening ties with China could raise for Israel and the United States. Given the limited mandate of the new committee, it might not bridge this gap. Consensus among the individuals we spoke with seemed to suggest that Israeli officials and business leaders view the relationship with China as complex but inevitable. As one former official said, "it is inconceivable that Israel would not have a relationship with China," in part because Israel simply cannot ignore China's growing presence in the region and because ties with China offer Israel important benefits.⁶ Nonetheless, Israel can and should view China's activities as nuanced and multifaceted, and develop appropriate regulations and review mechanisms to ensure that Israel still receives the benefits from its economic relations with China while also guaranteeing

⁶ Conversation with a former Israeli official, Tel Aviv, October 22, 2018.

that the risks posed by Chinese investment and construction activities are fully understood and properly mitigated. Israel's precarious position, needing to balance between its interests vis-à-vis Beijing and its strategic alliance with Washington in particular necessitates the development of such a holistic approach.

Follow-On Questions

This study has identified several outstanding sets of issues that warrant additional research. These issues range from the strategic to the tactical levels and could include both unclassified and classified research to answer important questions regarding the Israel-China relationship, and China in the Middle East more broadly:

- **The first issue relates to assessment of the risks to both Israel and the United States that are associated with Chinese penetration into Israel.** Data on Chinese investments in Israeli technology and infrastructure are not systematically collected, and further research is needed to capture the full extent of Chinese access including current bids in which Chinese companies are competing. Such data collection should extend into the classified domain to fully analyze the security risks, including intelligence and cyber risks, that deals with Chinese companies entail. For example, what type of risks are borne out of Chinese presence in the new Bayport terminal in Haifa versus Chinese agents watching the port from a nearby location or from other instances where U.S. and Chinese maritime vessels interact at sea? Could China obtain from Israel technologies that it cannot obtain from other countries, and what risks could these technologies pose to U.S. economic and security interests? More generally, once data are available, does China's investment in Israel help Beijing achieve its broader outbound investment strategic objectives?
- **A second area for further investigation relates to the effectiveness of existing regulatory bodies that monitor foreign investment and acquisition of sensitive technologies poten-**

tially with dual uses. From the U.S. perspective, how effective are existing American laws and regulatory bodies if China is able to acquire similar technologies or capabilities from other countries such as Israel with less robust or strict regulatory mechanisms? Are there alternative regulatory models or structures that might mitigate China's acquisition of sensitive technologies better than CFIUS, and if so, what are they? Several U.S. allies have their own regulatory and oversight mechanisms to monitor foreign investments in sensitive technologies, including Canada, the United Kingdom, France, and Australia.⁷ Are there lessons to be learned from these frameworks that can better protect U.S. and allied interests, including those of Israel? Further investigation is needed into the mechanism that Israel has decided to create in late October 2019—What will be its mandate? What types of deals will it examine? What foreign policy expertise will the committee utilize? Given its limited sector responsibility, how effective it could be in mitigating against the security risks of Chinese investment in technology?

- **The third set of questions relates to U.S. security and defense interests in the Middle East.** How might China exercise its increasing social and political influence in Israel, both in the short- and long-term, and what implications would this have for the United States? From a geostrategic perspective, how might China's presence in the Middle East affect other countries vying for influence throughout the region—primarily Russia and Iran? As mentioned in Chapter Five, the U.S. Navy's 6th Fleet uses the military port of Haifa as a regular port of call and the site of U.S.-Israel joint exercises. How does China's presence in and operation of a civilian port in Haifa (and Ashdod) affects U.S. risk assessments, including counterintelligence risk?
- **The fourth issue relates to the threat of the transfer of sensitive civilian, including emerging and foundational, technolo-**

⁷ Liz Alderman, "Wary of China, Europe and Others Push Back on Foreign Takeovers," *New York Times*, March 15, 2018.

gies and dual-use capabilities to China. What exactly is the nature of the threat to the United States posed by Chinese acquisition of such technologies from U.S. allies, including but not limited to Israel? Which specific technologies provide the greatest advances to China's military capabilities or otherwise pose a threat to U.S. interests and security? How can the United States effectively communicate to its partners its concerns regarding Chinese investments in such technologies? Given gaps in Chinese military technologies and associated motivations, are there certain technologies that likely will have greater application for the Chinese military than in a civilian setting, and therefore warrant greater scrutiny and oversight by U.S. regulatory bodies like CFIUS? If other U.S. allies share U.S. concerns about Chinese investments in technology and infrastructure, what existing mechanisms or oversight bodies can the United States and its partners use to create a comprehensive and partner-oriented response to these shared concerns? On the positive side, what kinds of partnerships can the United States develop with its allies to ensure its continued competitiveness in technology and innovation?

- **The final question is what types of security risks are associated with growing Israeli-Chinese academic cooperation and increase in the number of Chinese students in Israel.** Will more academics and students be used as human intelligence aiding China's efforts to identify desirable technologies and sensitive information? In what areas do Israeli and Chinese academics collaborate? What do these partnerships entail? Could deeper academic cooperation increase knowledge transfer from Israel to China, against Israeli and U.S. interests? Could enhanced Israeli-Chinese academic collaboration undermine Israeli-U.S. cooperation?

Chinese Investments in Israel

Data in this appendix were collected from several primary sources including an analysis conducted by Doron Ella in his article “Regulation of Foreign Investments and Acquisitions: China as a Case Study,” which was published in the INSS report *Israel-China Relations: Opportunities and Challenges* in Hebrew.¹ In addition, it drew on publicly available sources, primarily U.S., Israeli, Chinese, and other international news articles; and technology and financial websites, such as Tech Crunch. Data on VC investments were drawn from the VCs’ websites. This list is not necessarily exhaustive, as data on Chinese investment in Israel are scattered and not collected systematically.

¹ Ella, 2019a.

Table A.1
Chinese Investments in Israel

Israeli Entity	Chinese Entity	Investment Sum (Millions \$)	Notes	Year	Sector	Details
Tnuva	Bright Food (state-owned)	1,400	56% stake	2015	Agriculture and Natural Resources	Dairy
Makhteshim- Agan (Adama)	ChemChina (state-owned)	3,800	Bought 60% for 2400 million USD in 2011, later bought remaining 40% for 1400 million USD	2011, 2016	Agriculture and Natural Resources	Agrochemicals
Kaiima	Horizons Ventures Ltd.	65		2013	Agriculture and Natural Resources	Agro-Biotech
InnoGen	Pando Group	Undisclosed		2015–2016	Biomedical	Medi-Aesthetic
Lumenis	XIO Group	510		2015	Biomedical	Medical Laser Equipment
Alma Lasers Ltd.	Fosun International Ltd.	240	96% stake	2013	Biomedical	Medical Tech (semiconductors)

Table A.1—Continued

Israeli Entity	Chinese Entity	Investment Sum (Millions \$)	Notes	Year	Sector	Details
Rainbow Medical	ZTE, Ping-An, Yongjin	25		2015	Biomedical	Med-Tech
Cnoga Medical	GoCapital	12.5		2015	Biomedical	Med-Tech
Cnoga Medical	BOE (state-owned)	50		2017	Biomedical	Med-Tech
Brighttonix Medical	Pando Group	Undisclosed		2015–2016	Biomedical	Med-Tech
Inovytect	Vincent Medical	3		2017	Biomedical	Med-Tech
Oramed Pharmaceuticals Inc.	Hefei Tianhui Incubator of Technologies (HTIT)	50		2015	Biomedical	Pharmaceutical
Endospan	Xizang Haisco Pharmaceutical Group Co.	10		2015	Biomedical	Pharma-Tech
Technion	Li Ka Shing Foundation	130		2015	Other	Academy

Table A.1—Continued

Israeli Entity	Chinese Entity	Investment Sum (Millions \$)	Notes	Year	Sector	Details
Ahava	Fosun Ltd.	77		2016	Other	Cosmetics
Tipa	Horizons Ventures Ltd.	10		2014	Other	Industrial (biodegradable packaging)
Waze	Horizons Ventures Ltd.	30		2011	Technology	GPS Mapping
Magisto	Horizons Ventures Ltd.	21	Two rounds, (\$5.5 million in 2011, \$13 million in 2013)	2011, 2013	Technology	Video Creative
Desti	Horizons Ventures Ltd.	1		2012	Technology	Online Travel Apps
Onavo	Horizons Ventures Ltd.	10		2012	Technology	Mobile Applications
Wibbitz	Horizons Ventures Ltd.	2.3		2012	Technology	Text-to-Video
Ginger Software	Horizons Ventures Ltd.	5.4		2012	Technology	Mobile Keyboards

Table A.1—Continued

Israeli Entity	Chinese Entity	Investment Sum (Millions \$)	Notes	Year	Sector	Details
Shine	Horizons Ventures Ltd.	3.3		2012	Technology	Mobile
Preen.me	Horizons Ventures Ltd.	0.8		2012	Technology	Marketing
Invi	Horizons Ventures Ltd.	3		2012	Technology	Messaging
Stevie	Horizons Ventures Ltd.	1.5		2012	Technology	Social
Contacts+	Tencent Holdings	1		2012	Technology	Mobile Applications
EverythingMe	Horizons Ventures Ltd.	3.5		2012	Technology	Mobile Applications
Cortica	Horizons Ventures Ltd.	33.4	Three rounds (\$7 million in 2012, \$6.4 million in 2013, \$20 million in 2014)	2012–2014	Technology	Visual Search
Nipendo	Horizons Ventures Ltd.	8		2013	Technology	Cloud computing

Table A.1—Continued

Israeli Entity	Chinese Entity	Investment Sum (Millions \$)	Notes	Year	Sector	Details
Meteo-Logic	Horizons Ventures Ltd.	3		2013	Technology	Data Analytics
Pebbles Interfaces	Xiaomi	11		2013	Technology	Hardware and software
Core Photonics	Horizons Ventures Ltd.	28.3	Two rounds (\$10.5 million in 2013, \$17.8 million in 2015)	2013, 2015	Technology	Phone Cameras
FeeX	Horizons Ventures Ltd.	6.5		2014	Technology	Finance
Meekan	Horizons Ventures Ltd.	0.75		2014	Technology	Digital Calendars
eToro	Ping-An Insurance	27		2014	Technology	Forex
Pixellot	Baidu	3		2014	Technology	Video Capturing
Crosswise	Horizons Ventures Ltd.	3		2014–2015	Technology	Cross-Device Identification Mapping

Table A.1—Continued

Israeli Entity	Chinese Entity	Investment Sum (Millions \$)	Notes	Year	Sector	Details
Payoneer	Ping-An Insurance	Undisclosed	Two rounds	2014-2015	Technology	e-commerce
Tonara	Baidu	5		2015	Technology	Mobile Applications
Taboola	Baidu	Undisclosed		2015	Technology	Internet Advertising
Windward	Horizons Ventures Ltd.	10.8		2015	Technology	Maritime data and analytics
Visualead	Alibaba	5		2015	Technology	QR Codes
Thetaray	Alibaba	5		2015	Technology	Threat detection solutions
TravelFusion	Ctrip	160		2015	Technology	Online travel service
The Floor	Pando Group	2		2016	Technology	Tech Incubator
IronSource Ltd.	China Broadband Capital Partners (CBC), Ping An	85	Including other investors	2015	Technology	Adware

Table A.1—Continued

Israeli Entity	Chinese Entity	Investment Sum (Millions \$)	Notes	Year	Sector	Details
Twiggle	Alibaba	5 to 10		2016	Technology	e-commerce
Dynamic Yield	Baidu	22		2016	Technology	Personalization
Neura	Lenovo	11		2016	Technology	Internet of Things
Toga Networks	Huawei	Undisclosed		2016	Technology	IT and Telecom
HexaTier	Huawei	42	Terms undisclosed	2016	Technology	Database security
Playtika	Giant Interactive Group	4,400	Consortium of Chinese companies, led by Giant	2016	Technology	Mobile gaming
Lumus	Zhejiang Crystal-Optech Co.	15		2016	Technology	LOE wearable display
Lumus	Alibaba	6		2017	Technology	LOE wearable display
Servotronix Motion Control	MIDEA	170		2017	Technology	Motion electronics
Kaymera	GoCapital	10		2016	Technology	Threat detection solutions

Table A.1—Continued

Israeli Entity	Chinese Entity	Investment Sum (Millions \$)	Notes	Year	Sector	Details
Singulariteam	Tencent Holdings, RenRen	102		2015	VC Fund	AI and robotics
Canaan Partners Israel	Lenovo	10		2014	VC Fund	SaaS/Enterprise, Mobile Computing, and Internet Infrastructure
Carmel Ventures (now Viola Ventures)	Baidu, Ping-An, Qihoo	194	Including other investors	2014	VC Fund	Software, new enterprise infrastructure, big data, digital media, consumer applications and semiconductors
Pitango Venture Capital	Yongjin Group	20		2014	VC Fund	Technology and healthcare

Table A.1—Continued

Israeli Entity	Chinese Entity	Investment Sum (Millions \$)	Notes	Year	Sector	Details
Jerusalem Venture Partners	Alibaba	10	Estimate	2015	VC Fund	Cybersecurity, Big Data/Predictive Analytics, Media/Next-Gen Tech, and Cloud & Enterprise Software
Jerusalem Venture Partners	Shengjing 360	Undisclosed		2016	VC Fund	Cybersecurity, Big Data/Predictive Analytics, Media/Next-Gen Tech, and Cloud & Enterprise Software
GeneSort	Aid Partners	23		2017	Biomedical	Medical diagnosis
Alibaba DAMO Academy	Alibaba	Unknown	\$15 billion worldwide over 3 years	Announced Technology 2017		Research lab

Table A.1—Continued

Israeli Entity	Chinese Entity	Investment Sum (Millions \$)	Notes	Year	Sector	Details
Infinity Augmented Reality	Alibaba	15	25% stake, making Alibaba the largest shareholder	2016	Technology	Augmented Reality
eyeSight	Kuang-Chi	20		2016	Technology	Computer vision, smart home
AgentVI	Kuang-Chi	7	Including another investor	2016	Technology	Data analytics
Beyond Verbal	Kuang-Chi	3		2016	Technology	Voice analytics (biomedical applications)
SQream Technologies	Alibaba	26.4	Including other investors	2018	Technology	Data analytics
ReWalk Robotics	Timwell (based in Hong Kong)	20		2018	Biomedical	Wearable robotic exoskeleton
Vectorious	GEOC	9.5	Including other investors	2018	Biomedical	Heart monitoring
Saturas	Hubei Forbon Technology Co. Ltd	4	Including other investors	2018	Agriculture	Sensors for automatic irrigation

Table A.1—Continued

Israeli Entity	Chinese Entity	Investment Sum (Millions \$)	Notes	Year	Sector	Details
NA	Comfort Group (subsidiary of Ogawa)	10	Intended	2018	Biomedical	Digital health, quality of life
Tyto Care	Ping An Global Voyager Fund	25	Including other investors	2018	Biomedical	Medical devices, home health
IOptima, subsidiary of BioLight Israeli Life Sciences Investments Ltd	Chengdu Kanghong Pharmaceutical Group	56		2017	Biomedical	Ophthalmology
BondIT	Fosun	14.25		2017	Technology	Finance
ColorChip	Unknown	300		2018	Technology	Data center components
The Floor	Fosun	5		2018	Technology	Tech Incubator, Fintech
Mantis Vision, Mantis Technologies	Luenmei Quantum	55	Including other investors	2018	Technology	3D content
Mobileye	Baidu		NA	2018	Technology	Autonomous vehicles, machine vision

Table A.1—Continued

Israeli Entity	Chinese Entity	Investment Sum (Millions \$)	Notes	Year	Sector	Details
Future Meat Technologies	BitsXBites	2.2	Including other investors	2018	Agriculture	Lab-grown meat
Airobotics	BlueRun Ventures China	32.5	Including other investors	2017	Technology	Drones
Core Photonics (cameras), Aurora Labs (AI), Anagog (AI), Coronet (cybersecurity), Epistema (data analytics), PayKey (fintech), Orca AI, Protego (cyber), Twiggle (AI, e-commerce), VayaVision (AI), Armeron (cyber)	MizMaa	80.1	\$100 million intended; \$80.1 million as of the time of writing, including other investors	2016–2018	VC Fund	Technology, mostly AI and cybersecurity
Copyleaks	Unknown	1.1	Including other investors	2018	Technology	AI, with applications in education

Table A.1—Continued

Israeli Entity	Chinese Entity	Investment Sum (Millions \$)	Notes	Year	Sector	Details
eToro	China Minsheng Financial	100	Including other investors	2018	Technology	Forex
Current and past portfolio include: Mobileye (collision avoidance), Orex CR Technologies (medical tech), Lamina Technologies (manufacturing; controlling stake), Dori Media Group, Tufin (cyber), Satixfy (satellite communications), XJET (3D printing), Cyren (cloud)	China Everbright Ltd.	200	Joint fund with Israeli VC Catalyst	2014–2018	VC Fund	Mostly technology, medical

References

Ahronheim, Anna, "Naval Experts Concerned over China's Increasing Presence in Mediterranean," *Jerusalem Post*, August 23, 2018. As of June 28, 2019: <https://www.jpost.com/Israel-News/Naval-experts-concerned-over-Chinas-increasing-presence-in-Mediterranean-565625>

"AI Plagiarism Detection Co Copyleaks Raises \$1.1m," *Globes*, March 29, 2018. As of December 21, 2018: <https://en.globes.co.il/en/article-ai-plagiarism-detection-co-copyleaks-raises-11m-1001229996>

Alderman, Liz, "Wary of China, Europe and Others Push Back on Foreign Takeovers," *New York Times*, March 15, 2018. As of June 28, 2019: <https://www.nytimes.com/2018/03/15/business/china-europe-canada-australia-deals.html>

Amit, Hagai, "In Turnaround, Israel May Form Body to Vet Foreign Investment," *Haaretz*, July 16, 2018. As of June 28, 2019: <https://www.haaretz.com/israel-news/business/in-turnaround-israel-may-form-body-to-vet-foreign-investment-1.6273677>

Arms Control Association, "The Wassenaar Arrangement at a Glance," webpage, December 2017. As of June 28, 2019: <https://www.armscontrol.org/factsheets/wassenaar>

Azulay, Yuval, "Rotsim La'avod Be'chul: 2,200 Muamadim al 12 Misrot Nispachim Mischariyim [Want to Work Abroad: 2,200 Candidates for 12 Commercial Attaché Positions]," *Globes*, December 2, 2013.

Barboza, David, "Alibaba Buying South China Morning Post, Aiming to Influence Media," *New York Times*, December 11, 2015. As of January 5, 2018: <https://www.nytimes.com/2015/12/12/business/dealbook/alibaba-scmp-south-china-morning-post.html>

Bar-Eli, Avi, "Carmelton, Chinese Firm Reach Compromise on Tunnels Project," *Haaretz*, November 3, 2008. As of December 12, 2018: <http://www.haaretz.com/print-edition/business/carmelton-chinese-firm-reach-compromise-on-tunnels-project-1.256492>

Barkat, Amiram, "Eilat Railway Hits Financing Buffer," *Globes*, May 21, 2014. As of December 12, 2018:

<http://www.globes.co.il/en/article-eilat-railway-hits-financing-buffers-1000940302>

Barzilai, Amnon, "Israel, China Agree on Compensation for Cancelled Phalcon Deal," *Haaretz*, March 13, 2002.

Ben-Gedalyahu, Dubi, "China's Baidu Teams With Mobileye on Web Car Platform," *Globes*, July 3, 2018. As of June 17, 2019:

<https://en.globes.co.il/en/article-chinas-baidu-teams-with-mobileye-on-web-car-platform-1001244316>

Biedermann, Ferry, "China Is Increasingly Becoming Key for Israel's High-Tech Industry," *CNBC*, July 18, 2017. As of December 9, 2018:

<https://www.cnbc.com/2017/07/18/china-is-increasingly-becoming-key-for-israels-high-tech-industry.html>

Blenkinsop, Philip, "EU Promises Tough Line on U.S., China While Pushing for Free Trade," *Reuters*, June 23, 2017. As of December 9, 2018:

<https://www.reuters.com/article/us-eu-summit-trade-idUSKBN19E1RS>

———, "EU Countries Back Investment Screening Plan with China in Mind," *Reuters*, December 5, 2018. As of January 9, 2020:

<https://www.reuters.com/article/us-eu-china-investments-idUSKBN1O42F3>

Blizovski, Avi, "Machon Chadash: Ha'Sinim Yilmedu Chadshanut Meha'Yisraelim [New Institute: The Chinese Will Learn Innovation from the Israelis]," *PC Anashim U'Mechasvim*, December 26, 2017.

Bob, Yonah Jeremy, "Exclusive: Historic Case Against Bank of China for Millions in Terror Financing Dismissed," *Jerusalem Post*, November 8, 2015. As of June 28, 2019:

<https://www.jpost.com/Israel-News/Politics-And-Diplomacy/Exclusive-Historic-case-against-Bank-of-China-for-millions-in-terror-financing-dismissed-432381>

Bothwell, Ellie, "Israel Looks to Asia," *Inside Higher Ed*, July 14, 2017. As of June 28, 2019:

<https://www.insidehighered.com/news/2017/07/14/israeli-universities-expand-partnerships-asia>

Cai Ye, 见证华为任正非和孙亚芳历史不得不说的故事, ["Evidence from the Histories of Huawei's Ren Zhengfei and Sun Yafang that Must Be Spoken"], *Sina Blog of Cai Ye*, April 19, 2012.

Canaan, homepage, undated. As of January 5, 2018:

<http://www.canaan.com>

Caspit, Ben, "Does China Endanger Israel's Security?" *Al-Monitor*, January 11, 2019. As of June 27, 2019:

<https://www.al-monitor.com/pulse/originals/2019/01/israel-russia-china-benjamin-netanyahu-nadav-argaman-cyber.html>

Catalyst Fund, homepage, undated. As of September 4, 2018:
<http://catalyst-fund.com/>

Cendrowski, Scott, "China's Global 500 Companies Are Bigger than Ever—and Mostly State-Owned," *Fortune*, July 22, 2015. As of June 28, 2019:
<http://fortune.com/2015/07/22/china-global-500-government-owned>

———, "China's WeChat Is a Censorship Juggernaut," *Fortune*, April 14, 2017. As of January 5, 2018:
<http://fortune.com/2017/04/14/china-wechat-tencent-censorship-709-crackdown>

Chan, Minnie, "First Djibouti . . . Now Pakistan Port Earmarked for a Chinese Overseas Naval Base, Sources Say," *South China Morning Post*, January 5, 2018. As of June 28, 2019:
<https://www.scmp.com/news/china/diplomacy-defence/article/2127040/first-djibouti-now-pakistan-port-earmarked-chinese>

"China, Israel Announce Innovative Comprehensive Partnership," *Xinhua*, March 21, 2017. As of December 7, 2018:
http://www.xinhuanet.com/english/2017-03/21/c_136146441.htm

China Railway Construction Corporation Ltd., "CCECC Signs [sic] Israel's First Light Rail Operation Maintenance Contract," November 16, 2017. As of December 12, 2018:
http://english.crcc.cn/art/2017/11/16/art_441_575027.html

"Chinese Company Connects Tel Aviv Rail, Tehran," *Times of Israel*, July 6, 2015. As of January 5, 2018:
<https://www.timesofisrael.com/chinese-company-connects-tel-aviv-rail-tehran>

"Chinese Investments in Israel Could Pose Security Threat, Shin Bet Chief Warns," *Haaretz*, January 9, 2019. As of June 28, 2019:
<https://www.haaretz.com/israel-news/business/chinese-investments-in-israel-could-pose-security-threat-shin-bet-chief-warns-1.6827146>

Coats, Daniel R., *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*, testimony before the Senate Select Committee on Intelligence, January 29, 2019. As of February 18, 2019:
<https://www.odni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>

Cohen, Hedy, "Arison, Chinese Co Win TA Light Rail Underground Tender," *Globes*, May 19, 2015. As of December 12, 2018:
<http://www.globes.co.il/en/article-arison-chinese-co-win-ta-light-rail-underground-tender-1001037996>

Cohen, Roger, "Did Israel Put Money over Justice?" *New York Times*, February 28, 2015. As of February 11, 2020:
<https://www.nytimes.com/2015/03/01/opinion/sunday/roger-cohen-did-israel-put-money-over-justice.html>

Cohen, Tova, "Tel Aviv, Tsinghua Universities Set Up \$300 Mln Research Center," *Reuters*, May 19, 2014. As of June 28, 2019:

<https://www.reuters.com/article/us-israel-china-research/tel-aviv-tsinghua-universities-set-up-300-mln-research-center-idUSKBN0DZ18N20140519>

Cohen, Tova, and Catherine Cadell, "Huawei in Talks to Buy Israeli Cyber Company HexaTier: Sources," *Reuters*, December 20, 2016. As of June 28, 2019:

<https://www.reuters.com/article/us-huawei-tech-hexatier-m-a/huawei-in-talks-to-buy-israeli-cyber-company-hexatier-sources-idUSKBN149106>

Confucius Institute Headquarters, "About Confucius Institute/Classrooms," webpage, 2014. As of June 28, 2019:

http://english.hanban.org/node_10971.htm

Coren, Ora, "Washington Obstructing Israeli High-Tech Exports to China," *Haaretz*, January 22, 2014. As of June 28, 2019:

<https://www.haaretz.com/israel-news/business/premium-u-s-barring-israeli-tech-export-to-china-1.5313832>

Corrin, Amber, "Can the Navy Protect This Ship from Hackers?" *Fifth Domain*, April 30, 2018. As of June 28, 2019:

<https://www.fifthdomain.com/it-networks/2018/04/30/fast-transport-navy-ships-struggle-with-cyber-risks/>

Dagoni, Ran, "Harpy UAV Compromise with US: No Upgrades for China," *Globes*, May 25, 2005.

Ducklin, Paul, "Lenovo 'Superfish' Controversy—What You Need to Know," *Naked Security by Sophos*, February 20, 2015. As of January 5, 2018:

<https://nakedsecurity.sophos.com/2015/02/20/the-lenovo-superfish-controversy-what-you-need-to-know>

Efron, Shira, Howard J. Shatz, Arthur Chan, Emily Haskel, Lyle J. Morris, and Andrew Scobell, *The Evolving Israel-China Relationship*, Santa Monica, Calif.: RAND Corporation, RR-2641-RC, 2019. As of June 18, 2019:

https://www.rand.org/pubs/research_reports/RR2641.html

Egozi, Arie, "Israeli Worries About Chinese Investment Spark Calls For Closer Scrutiny," *Breaking Defense*, October 16, 2018. As of June 28, 2019:

<https://breakingdefense.com/2018/10/israeli-worries-about-chinese-investment-spark-calls-for-closer-scrutiny>

Elis, Niv, "Private Ashdod Port Building Ahead of Schedule, Says Ports Company," *Jerusalem Post*, April 12, 2016. As of June 27, 2019:

<https://www.jpost.com/Business-and-Innovation/Private-Ashdod-port-building-ahead-of-schedule-says-ports-company-451039>

Ella, Doron, "Regulation of Foreign Investments and Acquisitions: China as a Case Study," in Assaf Orion and Galia Lavi, eds., *Israel-China Relations: Opportunities and Challenges*, Tel Aviv: Institute for National Security Studies, August 2019a. As of January 9, 2020:

<https://www.inss.org.il/publication/regulation-of-foreign-investments-and-acquisitions-china-as-a-case-study/?offset=1&posts=11&outher=Doron%20Ella>

———, "A Regulatory Mechanism to Oversee Foreign Investment in Israel: Security Ramifications," Institute for National Security Studies, INSS Insight No. 1229, November 19, 2019b. As of January 9, 2020:

<https://www.inss.org.il/publication/a-regulatory-mechanism-to-oversee-foreign-investment-in-israel-security-ramifications/?offset=0&posts=12&outher=Doron%20Ella>

Elliott, Dorinda, "Tencent
 The Secretive, Chinese Tech Giant That Can Rival Facebook and Amazon," *Fast Company*, April 17, 2014. As of January 5, 2018:

<https://www.fastcompany.com/3029119/tencent-the-secretive-chinese-tech-giant-that-can-rival-facebook-a>

Evron, Yoram, "Between Beijing and Washington: Israel's Technology Transfers to China," *Journal of East Asian Studies*, Vol. 13, No. 3, December 2013, pp. 503–528.

Evron, Yoram, "Israel's Response to China's Rise: A Dependent State's Dilemma," *Asian Survey*, Vol. 56, No. 2, March–April 2016, pp. 392–414.

Fan Jida, 以色列如何成为创新驱动型国家 ["How Israel Became an Innovation-Driven Nation"], *Journal of Theory Guidance*, December 2016.

Foreign Investment Review Board, "About FIRB," webpage, undated. As of June 27, 2019:

<https://firb.gov.au/about-firb>

———, *Annual Report 2016-17*, Canberra: Commonwealth of Australia, 2018. As of June 27, 2019:

<https://cdn.tspace.gov.au/uploads/sites/79/2018/05/FIRB-16-17-Annual-Report.pdf>

Forsythe, Michael, "Fosun Group's Chairman Is Said to Be Missing in China," *New York Times*, December 10, 2015. As of June 28, 2019:

<https://www.nytimes.com/2015/12/11/business/chairman-of-fosun-group-of-china-is-said-to-be-missing.html>

Gabison, Yoram, "IDB Selling Remaining 40% Stake in Adama to ChemChina for \$1.4 Billion," *Haaretz*, July 18, 2016. As of December 12, 2018:

<http://www.haaretz.com/israel-news/business/premium-1.731512>

Gao, Charlotte, "What's China's Stance on Trump's Jerusalem Decision?" *The Diplomat*, December 7, 2017. As of June 28, 2019:
<https://thediplomat.com/2017/12/whats-chinas-stance-on-trumps-jerusalem-decision>

Garver, John, "China-Iran Relations: Cautious Friendship with America's Nemesis," *China Report*, Vol. 49, No. 1, 2013, pp. 69–88.

Gertz, Bill, "Chinese Telecom Firm Tied to Spy Ministry," *Washington Times*, October 11, 2011. As of January 5, 2018:
<https://www.washingtontimes.com/news/2011/oct/11/chinese-telecom-firm-tied-to-spy-ministry>

"Gesture Tech Firm Eyesight Nabs \$20 Million Chinese Investment," *Times of Israel*, May 15, 2016. As of December 18, 2018:
<https://www.timesofisrael.com/gesture-tech-firm-eyesight-nabs-20-million-chinese-investment>

Gold, Michael, "Taiwan Government Investigates Xiaomi on Potential Cyber Security Concerns," *Reuters*, September 24, 2014. As of January 5, 2018:
<http://in.reuters.com/article/taiwan-xiaomi-cybersecurity/taiwan-government-investigates-xiaomi-on-potential-cyber-security-concerns-idINKCN0HJ18T20140924>

Goldenberg, Suzanne, "Israel and US Clash over Spy Plane Sale to China," *The Guardian*, April 9, 2000. As of June 27, 2019:
<https://www.theguardian.com/world/2000/apr/10/israel>

Goodman, Peter S., and Jane Perlez, "Money and Muscle Pave China's Way to Global Power," *New York Times*, November 25, 2018. As of June 28, 2019:
<https://www.nytimes.com/interactive/2018/11/25/world/asia/china-world-power.html>

Gorodisky, Sonia, "Hachrizu al Chevrot Ha'Bniya Ha'Siniyot Be'Yisrael Kegorem Rikuzi [Declare Chinese Construction Companies in Israel as Concentration Element]," *Globes*, July 26, 2017. As of June 28, 2019:
<https://www.globes.co.il/news/article.aspx?did=1001247570>

Government of Canada, "Investment Canada Act," webpage, April 6, 2018. As of June 27, 2019:
<https://laws-lois.justice.gc.ca/eng/acts/i-21.8/fulltext.html>

Government of Israel, "Horaot Le'Giluy Be'Hitkashrut Le'Rechishat Nechasim [Instructions for Disclosing Communication Regarding the Purchase of Assets]," section 36A of the Securities Law, 1968.

———, *Hok Ha'Havarot Ha'Memshaltiyot* [Law of Governmental Companies], 1975.

———, *Hok Haganat Ha'Pratiyut* [Privacy Protection Law], 1981.

- Groll, Elias, "U.S. Navy Investigating if Destroyer Crash Was Caused by Cyberattack," *Foreign Policy*, September 14, 2017. As of June 28, 2019: <https://foreignpolicy.com/2017/09/14/u-s-navy-investigating-if-destroyer-crash-was-caused-by-cyberattack/>
- Gutman, Lior, "China's PMEC Looking to Buy Israeli Electricity Power Station," *Calcalist*, January 20, 2019. As of June 28, 2019: <https://www.calcalistech.com/ctech/articles/0,7340,L-3754593,00.html>
- "Gwadar Port About China's Interests, Not Pakistan's: US Think-Tank," *Economic Times*, February 9, 2018. As of June 28, 2019: <https://economictimes.indiatimes.com/news/defence/china-has-commercial-military-interests-in-gwadar-us-think-tank/articleshow/62840212.cms>
- Haber, Eldar, and Tal Zarsky, "Protecting Critical Infrastructure from Cyberattacks [Hebrew]," *Mishpat U'Mimshal*, 2017. As of January 9, 2020: <http://law.haifa.ac.il/images/documents/cyberspaceProtec.pdf>
- Hanemann, Thilo, and Daniel H. Rosen, "Chinese Investment in the United States: Recent Trends and the Policy Agenda," *Rhodium Group*, December 9, 2016. As of December 10, 2018: <https://rhg.com/research/chinese-investment-in-the-united-states-recent-trends-and-the-policy-agenda>
- Harel, Amos, "Israel Is Giving China the Keys to Its Largest Port—and the U.S. Navy May Abandon Israel," *Haaretz*, September 17, 2018. As of June 18, 2019: <https://www.haaretz.com/us-news/.premium-israel-is-giving-china-the-keys-to-its-largest-port-and-the-u-s-navy-may-abandon-israel-1.6470527>
- , "With Its National Security at Stake, Israel Takes Sides in U.S.-China Trade War," *Haaretz*, May 26, 2019. As of June 28, 2019: <https://www.haaretz.com/israel-news/.premium-u-s-china-trade-war-israel-takes-sides-national-security-1.7280881>
- Heruti-Sever, Tali, "Yair Shamir Metsig: Ha'Malatim Ha'Tsarfatiyim, Hakronot Hasiniyim, Hayoets Hamefukpak, Ve'Nigudei Hainyanim [Yair Shamir Presents: The French UAVs, the Chinese Cars, the Shady Consultant, and the Conflicts of Interests]," *The Marker*, January 30, 2017. As of January 5, 2018: <https://www.themarker.com/career/1.3462828>
- Hirschauge, Orr, "China's Huawei Coy About Its Ties to Israeli Firm," *Wall Street Journal*, June 2, 2016.
- Huang Wenbin and Andreas Wilkes, *Analysis of China's Overseas Investment Policies*, Bogor, Indonesia: Center for International Forestry Research, Working Paper 79, 2011. As of December 10, 2018: http://www.cifor.org/publications/pdf_files/WPapers/WP-79CIFOR.pdf

Innovation, Science, and Economic Development Canada, *Annual Report: Investment Canada Act 2016-17*, Ottawa, 2017. As of June 27, 2019: [https://www.ic.gc.ca/eic/site/ica-lic.nsf/vwapj/2016-17AnnualReport.pdf/\\$file/2016-17AnnualReport.pdf](https://www.ic.gc.ca/eic/site/ica-lic.nsf/vwapj/2016-17AnnualReport.pdf/$file/2016-17AnnualReport.pdf)

“Iran Finalizes €2.2b Rail Deal with China’s CMC—Exclusive,” *Financial Tribune*, May 20, 2017. As of January 5, 2018: <https://financialtribune.com/articles/domestic-economy/64854/iran-finalizes-22b-rail-deal-with-china-s-cmc-exclusive>

“Iran Launches \$2.7bn High-Speed Rail Project,” *Trade Arabia*, February 26, 2015. As of January 5, 2018: http://www.tradearabia.com/news/cons_276351.html

“Israel Received Bids to Build World’s Biggest Desalination Plant,” *Reuters*, October 7, 2018. As of June 28, 2019: <https://www.reuters.com/article/us-israel-desalination/israel-received-bids-to-build-worlds-biggest-desalination-plant-idUSKCN1MH0OI>

“Israel Said to Bar China, Turkey from Bidding for \$40 Million Airport Tender,” *Times of Israel*, January 25, 2019. As of June 28, 2019: <https://www.timesofisrael.com/israel-said-to-bar-china-turkey-from-bidding-for-airport-tender/>

Israeli Council for Higher Education, “Academic Cooperation with China and India—General Information,” webpage, undated. As of February 13, 2020: <https://che.org.il/en/academic-cooperation-with-china-and-india-general-information/>

“Israeli Minister Reassures U.S. over Chinese Telecoms Investment,” *Reuters*, January 18, 2019. As of June 19, 2019: <https://www.reuters.com/article/us-israel-china-usa/israeli-minister-reassures-u-s-over-chinese-telecoms-investment-idUSKCN1PC0ZX>

Israeli Ministry of Foreign Affairs, “Israel-China Task Force to be Launched,” March 30, 2015.

Jerusalem Venture Partners, “Companies,” webpage, undated. As of December 18, 2018: <https://www.jvpvc.com/companies/#filter=.vertical>

Kanner, Israel, and Doron Ella, “China’s New Cybersecurity Law and the Implications for Israel,” *Israel Defense*, April 4, 2017. As of June 28, 2019: <https://www.israeldefense.co.il/en/node/29135>

Katz, Yaakov, and Amir Bohbot, “How Israel Used Weapons and Technology to Become an Ally of China,” *Newsweek*, May 11, 2017.

Keck, Zachary, “Chinese Hackers Target Israel’s Iron Dome,” *The Diplomat*, August 2, 2014. As of December 12, 2018: <https://thediplomat.com/2014/08/chinese-hackers-target-israels-iron-dome>

Knockel, Jeffrey, Sarah McKune, and Adam Senft, "Baidu's and Don'ts: Privacy and Security Issues in Baidu Browser," *The Citizen Lab*, February 23, 2016. As of January 5, 2018:

<https://citizenlab.ca/2016/02/privacy-security-issues-baidu-browser/>

Knockel, Jeffrey, Adam Senft, and Ron Deibert, "WUP! There It Is: Privacy and Security Issues in QQ Browser," *The Citizen Lab*, March 28, 2016. As of January 5, 2018:

<https://citizenlab.ca/2016/03/privacy-security-issues-qq-browser>

Krebs, Brian, "Hackers Plundered Israeli Defense Firms that Built 'Iron Dome' Missile Defense System," *KrebsOnSecurity*, July 28, 2014. As of June 28, 2019: <https://krebsonsecurity.com/2014/07/hackers-plundered-israeli-defense-firms-that-built-iron-dome-missile-defense-system>

Krekel, Bryan, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, Falls Church, Va.: Northrop Grumman, March 7, 2012. As of January 5, 2018:

<https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-066.pdf>

Kumaraswamy, P.R., "Israel-China Relations and the Phalcon Controversy," *Middle East Policy*, Vol. 12, No. 2, pp. 93–103. As of April 14, 2019: <https://www.mepc.org/journal/israel-china-relations-and-phalcon-controversy>

Kynge, James, Chris Campbell, Amy Kazmin, and Farhan Bokhari, "Beijing's Global Power Play: How China Rules the Waves," *Financial Times*, January 12, 2017. As of June 28, 2019:

<https://ig.ft.com/sites/china-ports/>

Lappin, Yaakov, "Security Concerns Prompts Israel to Review China's Huawei 5G Network," *Breaking Israel News*, March 15, 2019.

Lee, Victor Robert, "China Builds Space-Monitoring Base in the Americas," *The Diplomat*, May 24, 2016. As of January 5, 2018:

<http://thediplomat.com/2016/05/china-builds-space-monitoring-base-in-the-americas>

Levi, Sarah, "Chinese Enrollment at Israeli Universities Skyrockets," *Jerusalem Post*, August 14, 2017.

Liu Hua, "Xi Jinping Meets with Israeli Prime Minister Netanyahu," *Xinhua*, March 21, 2017.

Liu Zhen, "Free Trade and Top Tech: What China Wants from Israel," *South China Morning Post*, March 21, 2017. As of June 28, 2019:

<https://www.scmp.com/news/china/diplomacy-defence/article/2080922/free-trade-and-top-tech-what-china-wants-israel>

Lunden, Ingrid, "Israel VC Singulariteam Raises 2nd Fund, \$102M Backed by Tencent, Renren Founders," *Techcrunch*, January 28, 2015. As of January 5, 2018: <https://techcrunch.com/2015/01/28/singulariteam-vc-fund>

"Made in China 2025' Plan Revealed," *Xinhua*, May 19, 2018.

McBride, James, and Andrew Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?" *Council on Foreign Relations*, August 2, 2018. As of June 28, 2019: <https://www.cfr.org/background/made-china-2025-threat-global-trade>

Melman, Yossi, "Cause for Concern? Chinese Investment and Israel's National Security," *Jerusalem Post*, April 7, 2018. As of June 27, 2019: <https://www.jpost.com/Jerusalem-Report/Chinese-TAKEAWAY-546692>

Milhaupt, Curtis J. and Wentong Zheng, "Beyond Ownership: State Capitalism and the Chinese Firm," *Georgetown Law Journal*, Vol. 103, No. 3, March 2015.

Miller, Joe, "Israeli Iron Dome Firms 'Infiltrated By Chinese Hackers,'" *BBC News*, July 31, 2014. As of June 28, 2019: <https://www.bbc.com/news/technology-28583283>

MizMaa, homepage, 2018. As of June 18, 2019: <http://www.mizmaa.com>

Mozur, Paul, "China Presses Its Internet Censorship Efforts Across the Globe," *New York Times*, March 2, 2018. As of June 28, 2019: <https://www.nytimes.com/2018/03/02/technology/china-technology-censorship-borders-expansion.html>

Mozur, Paul, and Jane Perlez, "China Tech Investment Flying Under the Radar, Pentagon Warns," *New York Times*, April 7, 2017. As of June 28, 2019: <https://www.nytimes.com/2017/04/07/business/china-defense-start-ups-pentagon-technology.html>

Murphy, Jack, "Here's What Sets China's International Espionage Apart from Everyone Else," *Business Insider*, July 11, 2015. As of June 28, 2019: <https://www.businessinsider.com/how-china-spies-2015-7>

National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace*, Washington, D.C., 2018. As of April 11, 2019: <https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf>

NCSC—See National Counterintelligence and Security Center.

No Man's Land, "Ha'Kiboosh Ha'Sini: Haim Hadirat Ha'Maatzama Ha'Sinit Le'Yisrael Sakana Bitchonit? [Chinese Occupation: Is the Penetration of the Chinese Superpower to Israel a Security Risk?]" *Kan 11*, March 11, 2019. As of January 9, 2020: <https://www.youtube.com/watch?v=7QC9Lmc-sg0>

Novet, Jordan, "China's WeChat Captures Almost 30% of the Country's Mobile App Usage: Meeker Report," *CNBC*, May 31, 2017. As of January 5, 2018: <https://www.cnbc.com/2017/05/31/wechat-captures-about-30-percent-of-chinas-mobile-app-usage-meeker-report.html>

NTA, "Red Line Map," undated. As of January 22, 2020: <https://www.nta.co.il/red-line-map>

O'Keeffe, Kate, "Trump Blocks China-Backed Fund from Buying Lattice Semiconductor," *Wall Street Journal*, September 13, 2017. As of January 9, 2018: <https://www.wsj.com/articles/trump-blocks-china-backed-fund-from-buying-u-s-chip-maker-lattice-1505335670>

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*, Washington, D.C., March 2018. As of December 10, 2018: <https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF>

Orbach, Meir, "Western Digital, Huawei, Invest in Cloud Storage Company," *Calcalist*, September 6, 2017. As of June 28, 2019: <https://www.calcalistech.com/ctech/articles/0,7340,L-3720660,00.html>

Orion, Assaf, "Challenges to Israel's Policy on China," in Assaf Orion and Galia Lavi, eds., *Israel-China Relations: Opportunities and Challenges*, Tel Aviv: Institute for National Security Studies, August 2019. As of January 10, 2020: <https://www.inss.org.il/publication/challenges-to-israels-policy-on-china>

OurCrowd, "Funded Portfolio," webpage, undated. As of December 18, 2018: <https://www.ourcrowd.com/funded-portfolio>

Penn, David, "ThetaRay Lands \$5 Million Investment from Alibaba, Partners with PwC," *Finovate Blog*, December 4, 2015. As of January 5, 2018: <http://finovate.com/thetaray-lands-5-million-investment-from-alibaba-partners-with-pwc>

Perez, Bien, "China Taps Nation's Who's Who of Technology to Anchor Ownership Shakeup at Unicom's Parent," *South China Morning Post*, August 16, 2017. As of September 27, 2018: <https://www.scmp.com/tech/article/2106982/unicom-shares-halted-speculation-mounts-new-investors-its-parent-company>

Pham, Sherisse, "Why China's Tech Giants Are Cozying Up to the Communist Party," *CNN Business*, November 4, 2018. As of June 28, 2019: <https://www.cnn.com/2018/11/02/tech/china-tech-communist-party/index.html>

Phillips, Tom, "Mysterious Confession Fuels Fears of Beijing's Influence on Hong Kong's Top Newspaper," *The Guardian*, July 25, 2016. As of January 5, 2018: <https://www.theguardian.com/world/2016/jul/25/south-china-morning-post-china-influence-hong-kong-newspaper-confession>

Pitango Venture Capital, "About," webpage, undated. As of September 3, 2018: <https://www.pitango.com/about/about-pitango/>

———, "Our Portfolio Companies," webpage, undated. As of September 3, 2018: <https://www.pitango.com/portfolio>

Plan, Fred, Nalani Fraser, Jacqueline O'Leary, Vincent Cannon and Ben Read, "ATP40: Examining a China-Nexus Espionage Actor," *FireEye Threat Research*, March 4, 2019.

Pomfret, John, "Lines Crossed in China; State-Owned Firms Bully Customers, One Another in Fight for Telecom Turf," *Washington Post*, August 17, 2002.

"Pompeo Warns U.S. Could Curb Security Ties with Israel over China Relations," *Times of Israel*, March 21, 2019. As of June 27, 2019: <https://www.timesofisrael.com/pompeo-warns-us-could-curb-security-ties-with-israel-over-china-relations>

Poulin, Gregory Noddin, "Sino-Israeli Economic Ties Blossoming," *The Diplomat*, December 1, 2014. As of June 28, 2019: <https://thediplomat.com/2014/12/sino-israeli-economic-ties-blossoming/>

Premoli, Aldo, "The Evolving Role of Maritime Straits," *Global Risk Insights*, December 13, 2016. As of June 28, 2019: <https://globalriskinsights.com/2016/12/the-evolving-role-of-maritime-straits>

Prime Minister's Office, "PM Netanyahu's Remarks at Israeli Presidential Conference," press release, June 20, 2013.

Prime Minister's Office, "Tochnit Le'kidum Ve'harchavat Ha'ksharim Ha'kalkaliyim Bein Israel V'Sin [A Plan to Promote and Expand the Economic Relations Between Israel and China]," press release, June 5, 2014.

———, Government Decision #251, "Strengthening Economic Cooperation with China [Hebrew]," May 19, 2013. As of May 3, 2019: https://www.gov.il/he/departments/policies/2013_dec251

———, "Security Cabinet Statement," press release, October 30, 2019. As of November 1, 2019: https://www.gov.il/en/departments/news/spoke_national_security301019

Public Law 115-232, Foreign Investment Risk Review Modernization Act, August 13, 2018.

Rabi, Idan, "Chinese Fund Mizmaa to Invest \$100m in Israeli Startups," *Globes*, June 13, 2017. As of June 18, 2019: <https://en.globes.co.il/en/article-chinese-fund-mizmaa-to-invest-100m-in-israel-1001192440>

Ramzy, Austin, "Q. and A.: How China's National People's Congress Works," *New York Times*, March 4, 2016. As of January 5, 2018:
<https://www.nytimes.com/2016/03/05/world/asia/china-national-peoples-congress-npc.html?mcubz=0>

Ravid, Barak, "Scoop: Netanyahu's Economic Adviser Backs Trump's Trade War with China," *Axios*, July 12, 2018. As of June 28, 2019:
<https://www.axios.com/natanyahu-adviser-trump-trade-war-china-71a5c4d4-2abc-4209-a2fa-5f68cdc73145.html>

———, "Trump Le'Netanyahu: Tsanen Ha'Keshet Im Sin O She'Hayachasim Imanu Aloolim Lehipaga [Trump to Netanyahu: Cool Down Connection With China Otherwise Our Ties Could Cool Down]," *Channel 13*, April 4, 2019. As of June 27, 2019:
<https://13news.co.il/item/news/politics/state-policy/trump-netanyahu-china-219348>

Reback, Gedalyah, "Kaymera Nabs \$10 Million for its Super Secure Mobile OS," *Geektime*, February 1, 2016. As of January 5, 2018:
<http://www.geektime.com/2016/02/01/kaymera-nabs-10-million-for-its-super-secure-mobile-os>

Robertson, Jordan, and Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," *Bloomberg*, October 4 2018. As of June 28, 2019:
<https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>

Robinson, Jana, "Deterring Chinese and Russian Space Hybrid Warfare by Economic And Financial Means," *Space Review*, September 18, 2017. As of March 9, 2020:
<https://www.thespacereview.com/article/3331/1>

Rogers, Mike, and C.A. Dutch Ruppersberger, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, Permanent Select Committee on Intelligence, U.S. House of Representatives, October 8, 2012.

Rosen, Gil, "Israel: Israeli Defense Export Control Regulations Amended," *Advoc*, May 8, 2015. As of June 28, 2019:
<https://www.advoc.com/news/israel-israeli-defense-export-control-regulations-amended>

Sasson, Assa, "Reports in China: Chairman of Fosun—Purchaser of Phoenix—Disappeared [Hebrew]," *The Marker*, December 10, 2015. As of June 28, 2019:
<https://www.themarket.com/markets/1.2796108>

Sauvant, Karl P., and Victor Z. Chen, "China's Regulatory Framework for Outward Foreign Direct Investment," *China Economic Journal*, Vol. 7, No. 1, 2014, pp. 141–163.

Scheer, Steven, "Israel Holds 5G Mobile Network Tender, Aims for 2020 Launch," Reuters, July 14, 2019. As of February 11, 2020:

<https://www.reuters.com/article/us-israel-telecoms-5g/israel-holds-5g-mobile-network-tender-aims-for-2020-launch-idUSKCN1U90C4>

Scissors, Derek, "Private Data, Not Private Firms: The Real Issues in Chinese Investment," *American Enterprise Institute*, January 10, 2018. As of December 12, 2018:

<http://www.aei.org/publication/private-data-not-private-firms-the-real-issues-in-chinese-investment>

Scobell, Andrew, and Alireza Nader, *China in the Middle East: The Wary Dragon*, Santa Monica, Calif.: RAND Corporation, RR-1229-A, 2016. As of June 18, 2019:

https://www.rand.org/pubs/research_reports/RR1229.html

Shamah, David, "China Firm to Build New Ashdod 'Union Buster' Port," *Times of Israel*, September 23, 2014. As of December 9, 2018:

<https://www.timesofisrael.com/china-firm-to-build-new-ashdod-union-buster-port/>

Shang Yong, "An Introduction to China's Science and Technology Policy," briefing delivered at the Kennedy School of Government, Cambridge, Mass., December 15, 2005. As of December 10, 2018:

https://www.belfercenter.org/sites/default/files/legacy/files/ministershangyong_dec_15_05_lecture.pdf

Shapira, Joseph, "Mevaker Ha'Medina, HeArchut Gufim Hiyuniyim Le'Haganat Ha'Syber [Cyber Security Preparation of Essential Bodies]," May 6, 2019. As of January 10, 2020:

<https://www.mevaker.gov.il/sites/DigitalLibrary/Pages/Reports/1427-35.aspx>

Shichor, Yitzhak, "Hide and Seek: Sino-Israeli Relations in Perspective," *Israel Affairs*, Vol. 1, No. 2, 1994, pp. 188–208.

———, "The U.S. Factor in Israel's Military Relations with China," *China Brief*, Vol. 5, No. 12, May 24, 2005.

Shiffer, Shimon, "U.S. Outraged After Israel Backs Out of Terror Suit," *Ynet News*, May 15, 2013. As of June 28, 2019:

<https://www.ynetnews.com/articles/0,7340,L-4405213,00.html>

Siboni, Gabi, and Ido Sivan Sevilla, "Regulation in Cyberspace," Tel Aviv: Institute for National Security Studies, Memorandum No. 190, April 2019. As of June 28, 2019:

<https://www.inss.org.il/publication/regulation-in-cyberspace/?offset=0&posts=87&author=Gabi%20Siboni>

Sina Finance, 政协委员张宏伟: 建议海外能源投资方式多元化 ["Zhang Hongwei (CPPCC) Suggests Diversifying The Method of Overseas Investment on Energy"], March 8, 2010. As of December 18, 2018:

<http://news.sina.com.cn/c/2010-03-08/120919815889.shtml>

Slaughter and May, “Foreign Investment in the EU: A Tale of Competing Tensions”, July 26, 2017. As of December 9, 2018:

<http://www.slaughterandmay.com/what-we-do/publications-and-seminars/publications/newsletters-and-briefings/2017/competition-regulatory-newsletter-12-25-july-2017/>

Solomon, Shoshanna, “China’s Kuang-Chi to Set Up Tel Aviv Base, Eyes Larger Firms,” *Times of Israel*, January 12, 2017. As of December 18, 2018:

<http://www.timesofisrael.com/chinas-kuang-chi-to-set-up-tel-aviv-base-eyes-larger-firms>

State Council, 中国制造2025 [Made in China 2025], May 8, 2015a. As of December 10, 2018:

http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm

———, 关于积极推进“互联网+”行动的指导意见 [Guiding Opinions on Actively Advancing “Internet Plus” Actions], July 4, 2015b. As of December 10, 2018:

http://www.gov.cn/zhengce/content/2015-07/04/content_10002.htm

———, 关于进一步引导和规范境外投资方向的指导意见 [Guiding Opinions on Further Guiding and Regulating the Direction of Outbound Investment], August 4, 2017. As of December 7, 2018:

http://www.gov.cn/zhengce/content/2017-08/18/content_5218665.htm

Stecklow, Steve, “Special Report: Chinese Firm Helps Iran Spy on Citizens,” *Reuters*, March 22, 2012. As of January 5, 2018:

<https://www.reuters.com/article/us-iran-telecoms/special-report-chinese-firm-helps-iran-spy-on-citizens-idUSBRE82L0B820120322>

“Strait of Malacca Key Chokepoint for Oil Trade,” *Maritime Executive*, August 27, 2018. As of June 28, 2019:

<https://www.maritime-executive.com/article/strait-of-malacca-key-chokepoint-for-oil-trade>

Tanner, Murray Scot, “Beijing’s New National Intelligence Law: From Defense to Offense,” *Lawfare*, July 20, 2017. As of June 28, 2019:

<https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense>

Technion Israel Institute of Technology, “Launch of First Israeli University in China,” press release, December 19, 2017. As of June 28, 2019:

<https://www.technion.ac.il/en/2017/12/first-israeli-university-inaugurated-in-china/>

“Too Open for Business? Israel’s Ties with China Are Raising Security Concerns,” *The Economist*, October 11, 2018. As of June 28, 2019:

<https://www.economist.com/middle-east-and-africa/2018/10/13/israels-ties-with-china-are-raising-security-concerns?fsrc=scn/tw/te/bl/ed/israelstieswithchinaareraisingsecurityconcernstooopenforbusiness>

U.S. Chamber of Commerce, *Made in China 2025: Global Ambitions Built on Local Protections*, Washington, D.C., 2017. As of December 10, 2018:
https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf

U.S. Department of Justice, “ZTE Corporation Agrees to Plead Guilty and Pay over \$430.4 Million for Violating U.S. Sanctions by Sending U.S.-Origin Items to Iran,” press release, March 7, 2017. As of January 5, 2018:
<https://www.justice.gov/opa/pr/zte-corporation-agrees-plead-guilty-and-pay-over-4304-million-violating-us-sanctions-sending>

U.S. Department of State, “2015 Investment Climate Statement—China,” May 2015. As of June 18, 2019:
<https://2009-2017.state.gov/e/eb/rls/othr/ics/2015/241518.htm>

U.S. Department of the Treasury, Office of Public Affairs, “Fact Sheet: Proposed CFIUS Regulations to Implement FIRRMA,” September 17, 2019. As of November 1, 2019:
<https://home.treasury.gov/system/files/206/Proposed-FIRRMA-Regulations-FACT-SHEET.pdf>

U.S. Navy, “NMCB 11 Prepares for Juniper Cobra 18 in Israel,” press release, March 12, 2018. As of June 27, 2019:
https://www.navy.mil/submit/display.asp?story_id=104678

Viola Ventures, “Empowering Early-Stage Technology Companies to Become Global Category Leaders,” webpage, 2017. As of November 14, 2017:
<http://www.viola-group.com/fund/violaventures/#4945>

Wang, Bijun, 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.

Wee, Sui-Lee, “Mercedes-Benz Quotes the Dalai Lama. China Notices. Apology Follows,” *New York Times*, February 6, 2018. As of June 28, 2019:
<https://www.nytimes.com/2018/02/06/business/mercedes-daimler-dalai-lama-china.html>

“What’s in a Picture? The Unspoken Messages in Xi Jinping’s Group Portrait with CEOs and Senior Executives During His First State Visit to the US,” *South China Morning Post*, September 24, 2015. As of January 5, 2018:
<http://www.scmp.com/tech/leaders-founders/article/1861033/whats-picture-unspoken-messages-xi-jinpings-group-portrait?comment-sort=recommended>

White and Case, “CFIUS Reform Becomes Law: What FIRRMA Means for Industry,” August 13, 2018a. As of November 1, 2019:
<https://www.whitecase.com/publications/alert/cfius-reform-becomes-law-what-firrma-means-industry>

———, “Department of Commerce Review of Export Controls on Emerging Technologies,” November 28, 2018b. As of November 1, 2019:

<https://www.whitecase.com/publications/alert/departement-commerce-review-export-controls-emerging-technologies>

Wübbeke, Jost, Mirjam Meissner, Max J. Zenglein, Jaqueline Ives, and Björn Conrad, *Made in China 2025: The Making of a High-Tech Superpower and Consequences For Industrial Countries*, Berlin: Mercator Institute for China Studies, December 2016. As of December 12, 2018:

https://www.merics.org/sites/default/files/2017-09/MPOC_No.2_MadeinChina2025.pdf

Xiao Xian, 一带一路视角下的中国与以色列关系 [“The Role of “One Belt One Road” within Sino-Israeli Relations”], *Journal of Southwest Asia and Africa*, Vol. 2, 2016.

Yablonko, Yasmin, “Chinese Take Growing Slice of Israeli Tech Investment,” *Globes*, October 30, 2018. As of December 18, 2018:

<https://en.globes.co.il/en/article-chinese-take-growing-slice-of-israeli-tech-investment-1001258499>

Yang Jingru, 习近平考察深圳光启研究院: 国家应择天下英才而用 [“Xi Jinping Observes Shenzhen Kuang Chi Research Center: The Nation Should Select And Use The Most Outstanding Talent”], *China News*, December 14, 2012. As of September 27, 2018:

<http://www.chinanews.com/gn/2012/12-14/4407793.shtml>

Yu, Angela, “Chinese Port Operator Signs Deal to Run Israel’s Haifa Port,” *JOC.com*, June 2, 2015. As of December 12, 2018:

https://www.joc.com/port-news/international-ports/haifa-port/chinese-port-operator-signs-deal-run-israel%E2%80%99s-haifa-port_-0

Zengerle, Patricia, “Senate Panel Wants Chinese-Funded Institutes to Change or Leave U.S.,” *Reuters*, February 27, 2019. As of June 28, 2019:

<https://www.reuters.com/article/us-china-education-usa/senate-panel-wants-chinese-funded-institutes-to-change-or-leave-u-s-idUSKCN1QG33G?il=0>

Zhang Feifei, 以色列热的冷思考 [“Cool Reflections on ‘Israel Fever,’”] *Economic Observer Online*, October 22, 2016. As of September 27, 2018:

<http://www.eeo.com.cn/2016/1022/292911.shtml>

Zhou, Laura, “Chinese Island-Building Firm Wins Contract with South China Sea Rival Claimant, the Philippines,” *South China Morning Post*, October 26, 2016, updated October 27, 2016. As of January 5, 2018:

<http://www.scmp.com/news/china/diplomacy-defence/article/2040256/chinese-firm-helped-build-islands-disputed-area-south>

Ziv, Amitai, “‘Ha’Shabac Lo Yeasher:’ Ha’Sod al Hevrot Ha’Tikshoret M’eSin Ve’Rusia She’Rotsot Lipfol Be’Yisrael, [‘The Shin Bet Will Not Approve:’ The Secret About Companies from China and Russia that Want to Operate in Israel],” *The Marker*, September 26, 2019.



NATIONAL DEFENSE RESEARCH INSTITUTE

Relations between China and Israel have expanded rapidly since the early 2000s in numerous areas, including diplomacy, trade, investment, construction, educational partnerships, scientific cooperation, and tourism. Israel seeks to expand its diplomatic, economic, and strategic ties with the world's fastest-growing major economy and diversify its export markets and investments. China seeks Israel's advanced technology and values Israel's location as part of the Belt and Road Initiative. Chinese investments in Israel have grown substantially and include investments in high-tech companies that produce sensitive technologies as well as the construction and operation of key infrastructure projects. Chinese investment in sensitive technologies and construction of major Israeli infrastructure present distinct concerns for Israel and the United States. The authors examine the extent and nature of Chinese investments into Israeli technology and infrastructure and discuss the security implications these pose for Israel and the United States. The primary concern regarding investment relates to Chinese ownership of companies that might possess sensitive technology or data; concerns over construction are focused on the use of infrastructure projects to further Chinese foreign policy goals. The operation of infrastructure projects affords China unique surveillance opportunities and possibly economic and political levers of influence. The report concludes with a set of open-ended questions that merit further investigation to better understand the magnitude of risks associated with Chinese investment in the Israeli market.

\$30.00

ISBN-10 1-9774-0435-9
ISBN-13 978-1-9774-0435-0



www.rand.org