

AUGUST 2023

COMPETING WITHOUT FIGHTING

CHINA'S STRATEGY
OF POLITICAL WARFARE

AUTHORS

Seth G. Jones
Emily Harding
Catrina Doxsee
Jake Harrington
Riley McCabe



A REPORT OF THE CSIS
TRANSNATIONAL THREATS PROJECT

CSIS

CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

AUGUST 2023

COMPETING WITHOUT FIGHTING

CHINA'S STRATEGY OF POLITICAL WARFARE

AUTHORS

Seth G. Jones

Emily Harding

Catrina Doxsee

Jake Harrington

Riley McCabe

A REPORT OF THE CSIS TRANSNATIONAL THREATS PROJECT

CSIS | CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

ROWMAN &
LITTLEFIELD

Lanham • Boulder • New York • London

ABOUT CSIS

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

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

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

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

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

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

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

ISBN: 978-1-5381-7070-0 (pb); 978-1-5381-7071-7 (eBook)

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

Rowman & Littlefield
4501 Forbes Boulevard
Lanham, MD 20706
301-459-3366 | www.rowman.com

ACKNOWLEDGMENTS

The authors owe an extraordinary debt of gratitude to numerous individuals whose help was critical during the research, writing, editing, and publication phases of this report. Thanks to Gamin Kim, Harshana Ghoorhoo, and Jared Thompson at CSIS for their outstanding research assistance and help along the way, as well as Samantha Lu who helped review Chinese language in the report for accuracy. Thanks also to a superb group of colleagues at CSIS whose work on China—including in such areas as military operations, economics, intelligence, politics, and cyber—contributed to this report. They include Kari Bingen, Jude Blanchette, Victor Cha, Gerard DiPippo, Charles Edel, Matthew Goodman, Christopher Johnstone, Scott Kennedy, James Lewis, Bonny Lin, Greg Poling, John Schaus, and Nicholas Szechenyi. In addition, thanks to CSIS's outstanding iLab team for their help in editing, formatting, and publishing the document. They include Lauren Bailey, Emma Colbran, Matthew Funaiole, Julia Huh, Alexander Kisling, Jeeah Lee, Leena Marte, Phillip Meylan, Katherine Stark, Rayna Salam, Andrew Schwartz, and William Taylor. Finally, thanks to CSIS's Congressional team, including Elizabeth Hoffman, Shivani Vakharia, and Christian Hyde, for arranging a series of briefings and discussions with Congressional staff and members.

The authors are particularly grateful to Timothy Heath and Jude Blanchette for their thorough reviews of an early draft. Their comments, critiques, and suggestions were extraordinarily helpful in improving the quality of this report.

Finally, thanks to those government officials and subject matter experts from the United States, Australia, South Korea, Japan, India, and the United Kingdom that the authors interviewed over the course of this project. Most of them did not want to be identified by name, but this report could not have been completed without their comments and practical, real-world knowledge.

This report is made possible by generous support from the Diana Davis Spencer Foundation.

CONTENTS

Executive Summary	IX
1. Introduction	2
2. The Strategic Logic of Chinese Political Warfare	8
3. Intelligence Operations	17
4. Cyber Operations	29
5. Information and Disinformation Operations	43
6. The United Front	56
7. Irregular Military Actions	65
8. Economic Coercion	81
9. Countering China	92
About the Authors	101
Appendix	103
Endnotes	105

ACRONYMS

AI/ML – Artificial intelligence/machine learning

APT – Advanced persistent threat

AVIC – Aviation Industry of China

BfV – Bundesamt für Verfassungsschutz

BRI – Belt and Road Initiative

CAC – Cyberspace Administration of China

CCG – Chinese Coast Guard

CCP – Chinese Communist Party

CCTV – China Central Television

CGTN – China Global Television Network

CIA – Central Intelligence Agency

CISA – Cybersecurity and Infrastructure Security Agency

CNTIC – China National Cyber Threat Intelligence Collaboration

CSSA – Chinese Student and Scholars Association

CUSEF – China-United States Exchange Foundation

DIA – U.S. Defense Intelligence Agency

DOD – U.S. Department of Defense

DOJ – U.S. Department of Justice

DSR – Digital Silk Road

EEZ – Exclusive economic zone

FARA – Foreign Agent Registration Act

FBI – Federal Bureau of Investigation

FIRS – Foreign Influence Registration Scheme

FITS – Foreign Influence Transparency Scheme

GNSS – Global Navigational Satellite System

GSI – Global Security Initiative

HBCU – Historically Black college and university

HUMINT – Human intelligence

ICS – Industrial control system

IP – Intellectual property

JSSD – Jiangsu State Security Department

LDA – Lobbying Disclosure Act

MICE – Money, ideology, compromise, or ego

MMFV – Maritime Militia Fishing Vessel

MPS – Ministry of Public Security (China)

MSS – Ministry of State Security (China)

NBA – National Basketball Association

NCC – National Cybersecurity Center

NUAA – Nanjing University of Aeronautics and Astronautics

ONCD – Office of the National Cyber Director

OPE – Operational preparation of the environment

OPM – U.S. Office of Personnel Management

MNR – Ministry of Natural Resources

MOU – Memorandum of understanding

NSA – National Security Agency

NSD – Network Systems Department

PAFMM – People's Armed Forces Maritime Militia

PAP – People's Armed Police

PLA – People's Liberation Army

PLAA – PLA Army

PLAF – People's Liberation Army Air Force

PLAN – People's Liberation Army Navy

PLARF – People's Liberation Army Rocket Force

PLASSF – People's Liberation Army Strategic Support Force

PMC – Private military company

PRC – People's Republic of China

PSC – Private security company

SBFVs – Spratly Backbone Fishing Vessels

SOE – State-owned enterprise

THAAD – Terminal High Altitude Area Defense

TRB – Technical Reconnaissance Bureau

UAS – Unmanned aircraft system

UFWD – United Front Work Department

2PLA – Second Department of the General Staff Department (PLA)

3PLA – Third Department, Network Systems Department

4PLA – Fourth Department, Network Systems Department

Political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives.

—George Kennan, U.S. Diplomat and Historian¹

An ambitious blueprint has been drawn for building a modern socialist country in all respects and advancing the great rejuvenation of the Chinese nation on all fronts through a Chinese path to modernization, sounding a clarion call of the times for us forging ahead on a new journey.

-Xi Jinping¹



EXECUTIVE SUMMARY

擘画了全面建设社会主义现代化国家、以中国式现代化全面推进中华民族伟大复兴的宏伟蓝图，吹响了奋进新征程的时代号角。

-习近平²

China is conducting an unprecedented campaign below the threshold of armed conflict to expand the influence of the Chinese Communist Party (CCP) and weaken the United States and its partners.

This campaign involves sophisticated Chinese espionage activities, offensive cyber operations, disinformation on social media platforms, economic coercion, and influence operations targeting companies, universities, and other organizations.

This report offers one of the most comprehensive analyses to date of Chinese political warfare activities and examines China's main actions, primary goals, and options for the United States and its partners. It sheds new light on the scope and breadth of Chinese activities and comes to several conclusions.

First, China is conducting an increasingly active and aggressive campaign to penetrate a wide range of U.S. academic institutions, companies, government agencies, and nongovernmental organizations (NGOs). The scale of China's actions in the United States is unparalleled. As one Federal Bureau of Investigation (FBI) senior official told the authors, "The system is blinking red right now. We have not seen this level of Chinese intelligence and influence activity in and around the U.S. homeland ever."³

Over the past year, for example, the FBI and Department of Justice (DOJ) have arrested or indicted

numerous individuals for espionage, cyber operations, and illegal influence campaigns. The list includes an indictment against the codirector of a U.S.-based think tank for acting as an unregistered foreign agent for China and other actions, a series of aggressive cyberattacks against senior U.S. government officials and companies such as Microsoft, and the expansion of Chinese intelligence collection sites in such countries as Cuba.

In addition, China has been involved in an expansive campaign to monitor, harass, and coerce residents of the United States and other countries as part of an extralegal repatriation effort known as Operation Fox Hunt. In 2023, for example, the FBI arrested two individuals, "Harry" Lu Jianwang and Chen Jinping, in connection with operating an illegal police station in Manhattan, New York City, for China's Ministry of Public Security (MPS). In 2023, DOJ also indicted dozens of MPS officials for conducting online intimidation against Chinese nationals residing in the United States who were critical of China.

Second, the report details that China's top target for political warfare—by far—is the United States. Chinese actions against the United States are more expansive than is generally known and include:

- **Intelligence Operations:** China's intelligence services, such as the Ministry of State Security (MSS) and MPS, are engaged in extensive human intelligence, signals intelligence, and other types of intelligence

collection as part of political warfare—including intimidating Chinese diaspora in the United States. In examining over 100 Chinese espionage cases directed at the United States and U.S. entities, this report concludes that Chinese intelligence operations are not just pervasive, but they are used to plan and execute all of China's other political warfare activities.

- **Cyber Operations:** Chinese organizations, including units within the People's Liberation Army (PLA), are involved in a cyber campaign against U.S. and other international corporations, universities, government agencies, media, think tanks, nongovernmental organizations, and other targets. These efforts are designed to help China leapfrog ahead of the West by skipping the extensive and time-consuming research and development phases for new technologies. China's cyber operations are also intended to influence foreign and domestic audiences, assist with offensive military campaigns, and improve the country's artificial intelligence and big data analytics capabilities.
- **Information and Disinformation Operations:** China is engaged in extensive information and disinformation activities overseas—including in the U.S. homeland—designed to influence decisionmaking and popular support to gain a competitive advantage. Beijing seeks to tightly control the image of China abroad, including by influencing companies, organizations, and individuals that criticize China, from the National Basketball Association to Hollywood studios.
- **United Front Work:** The CCP is involved in aggressive efforts to extend its reach overseas through united front work, which involves activity to protect and bolster the image of China and the CCP. United front work includes activities to influence individuals in such countries as the United States who are well positioned to amplify China's preferred messaging on political, economic, and other issues.
- **Irregular Military Actions:** The PLA, PLA Navy, PLA Air Force, PLA Rocket Forces, People's Armed Forces Maritime Militia, research organizations, and private security companies linked to China are involved in widespread efforts to expand Chinese influence below the threshold of armed

conflict. Chinese organizations are involved in near-seas activities (which focus on securing Chinese interests around such areas as the South and East China Seas) and far-seas activities (which are global in scope). This report constructs a dataset of Chinese private security companies that shows that there are nearly two dozen Chinese private security companies operating overseas, including in Africa, the Middle East, Asia, and Latin America.

- **Economic Coercion:** China has penetrated—or attempted to penetrate—virtually every sector of the U.S. economy, as well as many of its partners such as the United Kingdom. In addition, China is engaged in the threat or imposition of economic costs or inducements to influence decisionmaking and popular support in other countries to gain a competitive advantage. There has been considerable focus on the Belt and Road Initiative as part of a broader effort to influence foreign governments. As this report highlights, however, another concerning Chinese initiative is the Digital Silk Road, which aims to spread Chinese influence through telecommunications, e-commerce, hardware, software, big data, artificial intelligence/machine learning, and other digital infrastructure across the globe.

These tools are part of a broad strategy of *political warfare*, which U.S. diplomat George Kennan described as “the employment of all the means at a nation's command, short of war, to achieve its national objectives.”⁴ The U.S. public and other international audiences are often unaware of the full nature and scope of these Chinese activities, including those that target U.S. and other Western companies, government agencies, universities, news media, digital platforms, and other NGOs.

These tools are not mutually exclusive but are sometimes overlapping, reinforcing, and occasionally even duplicative and competitive. China presents a “whole-of-state” approach to political warfare. Multiple organizations are involved, such as the PLA, MSS, MPS, Ministry of Industry and Information Technology, United Front Work Department, and Ministry of Foreign Affairs. A wide range of non-state or quasi-state actors are also involved, from hacktivists to private security companies.

Third, China has several strategic goals in conducting political warfare. The most important is preservation of the CCP's rule. Another is expanding

Chinese influence and weakening the United States as part of balance-of-power competition. These goals are in line with China's national strategy of achieving "the great rejuvenation of the Chinese nation on all fronts."⁵ China also conducts political warfare—rather than armed conflict—to avoid conventional war and refrain from provoking other countries.

In light of these activities, the United States and its partners have been slow to identify and counter Chinese political warfare. This needs to change. Moving forward, there are several core components of an effective strategy to compete with China. These components include continuing to ground U.S. responses in democratic principles; improving the United States' understanding of China through a more systematic analysis of the country; improving defensive measures, including increasing U.S. counterintelligence resources; conducting a more effective offensive campaign; and deepening relationships with partners.

U.S. policymakers have been more comfortable with defensive measures to protect the United States from Chinese intelligence operations, cyber operations, propaganda, united front work, and other activity. But U.S. and partner offensive measures are also essential to help achieve several goals, such as reversing China's expansionism and influence by competing on a sustained basis across the globe.

At the beginning of the Cold War, Kennan authored a U.S. State Department Policy Planning Staff memorandum on political warfare that remains relevant to today's competition with China. He noted that a significant part of great power competition involves activities below the threshold of conventional and nuclear warfare.⁶ Today, China is heavily involved in many of these activities. As this report documents, China also has significant weaknesses and vulnerabilities that can be exploited. Together with its partners, the United States now needs to develop a comprehensive approach to compete in this arena that is consistent with its democratic principles and values. The clock is ticking.

Confronted with drastic changes in the international landscape, especially external attempts to blackmail, contain, blockade, and exert maximum pressure on China, we have put our national interests first, focused on internal political concerns, and maintained firm strategic resolve.

-Xi Jinping¹



INTRODUCTION

面对国际局势急剧变化,特别是面对外部讹诈、遏制、封锁、极限施压,我们坚持国家利益为重、国内政治优先,保持战略定力,发扬斗争精神,展示不畏强权的坚定意志。

-习近平²

This report examines Chinese political warfare, which includes actions below the threshold of conventional warfare designed to achieve a state's national objectives.

Examples include intelligence operations, cyber operations, information and disinformation operations, united front work, irregular military action, and economic coercion. These measures have also been referred to as gray zone actions, irregular warfare, asymmetric activities, or even unrestricted warfare.³ An analysis of political warfare is essential for two main reasons.

First, much of the U.S. focus on China has been on the growing conventional or nuclear capabilities of the People's Liberation Army (PLA) and other organizations. As one report from the U.S. Department of Defense (DOD) concludes, the PLA is “developing the capabilities to conduct joint long-range precision strikes across domains, increasingly sophisticated space, counterspace, and cyber capabilities, and accelerating the large-scale expansion of its nuclear forces.”⁴ Based on these concerns, the United States has concentrated on building conventional and nuclear capabilities to deter China with the help of its partners—and to fight China if deterrence fails. The United States' 2022 *National Defense Strategy* focuses on the conventional and nuclear threat from China and ways that the United States and its partners could sustain and strengthen conventional and

nuclear deterrence.⁵ In addition, the majority of DOD planning scenarios and operational plans (OPLANs) center on conventional war with China. The same is true with wargames over the past few years, which have focused on such scenarios as a Chinese conventional invasion of Taiwan.⁶

These actions are necessary. The United States and its partners need to continue developing military capabilities for deterrence and—if deterrence fails—warfighting. But these measures are not sufficient. As this report finds, Beijing is conducting a wide range of activities below the level of armed conflict designed to protect the CCP, weaken the United States and its allies, and expand Chinese power and influence.

Second, there is a growing body of work on Chinese political warfare and related activities.⁷ But most assessments have been relatively narrow and focused on one of the following areas: PLA gray zone activities, especially by the PLA Navy, PLA Air Force, PLA Army, People's Armed Police, China Coast Guard, and People's Armed Forces Maritime Militia; cyber and disinformation operations, including activity by the PLA Strategic Support Force; or intelligence operations, including activity by the MSS and MPS. For example, there has been a great deal of research and analysis on Chinese gray zone activity, particularly actions by the PLA. Yet most of this work has focused on military actions by the PLA—not broader political warfare by a range of Chinese organizations.⁸

Disaggregating Chinese political warfare into various parts—and not analyzing the sum of its parts—misses China’s broad and systematic attempts to expand power and influence across multiple areas. Chinese political warfare cannot be fully understood piecemeal.

RESEARCH DESIGN

This report asks several questions. What actions is China conducting against the United States and its partners as part of political warfare? What are China’s main goals in conducting political warfare? Finally, what options do the United States and its partners have to counter these Chinese activities?

To answer these questions, this report applies a mixed-methods approach. It compiles quantitative data on several issues—such as counterintelligence cases, cyber incidents, and Chinese private security companies—to better understand Chinese political warfare and assess trends over time. For example, the chapter on intelligence operations reviews more than 100 U.S. indictments of individuals accused of conducting activities on behalf of China. The chapter on Chinese irregular military activities constructs a database of Chinese private security companies that have operated outside of China, sample locations in which they are reported to operate, the types of services they have provided, and some of their known clients.

In addition, the report utilizes several types of qualitative information to better understand Chinese political warfare. Members of the research team collected and analyzed Chinese documents, including documents from CSIS’s open-source project, *Interpret: China*.⁹ The chapter on information and disinformation relies on a body of English-language primary source speeches from the Chinese Ministry of Foreign Affairs and the CSIS *Interpret: China* database. The CSIS team also scraped and analyzed the tweets of prominent Chinese Communist Party (CCP) spokespersons. Furthermore, the intelligence chapter analyzes one of the few unclassified Chinese-language documents illuminating China’s approach to intelligence: a book by two Chinese intelligence veterans, Huo Zhongwen and Wang Zongxiao. The chapter on irregular military activities relies on a variety of primary and secondary sources, including Chinese research publications, government white papers, press releases, and speeches by officials; analysis and data reported by U.S. and partner governments and research institutions; and satellite imagery.

Finally, CSIS analysts conducted interviews with U.S. government officials, academic and corporate subject matter experts, and officials from several foreign countries, such as the United Kingdom, Australia, Japan, and South Korea.

POLITICAL WARFARE

As used in this report, political warfare refers to activities short of conventional and nuclear warfare that are designed to expand a country’s influence and legitimacy, as well as weaken its adversaries.¹⁰ Political warfare is not new. As historian Hal Brands concludes, “During the Peloponnesian War, Athens and Sparta sought to widen each other’s internal divisions. During the Cold War, it would have been odd had America *not* waged political warfare against the Kremlin, since the nuclear revolution made it so essential to win without violence.”¹¹ The Soviet Union and United States utilized political warfare during the Cold War to achieve several goals: weaken a population’s trust in its institutions of government (whether in the United States, the Soviet Union, or their allied countries), establish or widen cleavages between individuals and groups in society, and establish or exploit divisions between allies.¹²

More broadly, political warfare includes tools of statecraft that governments can use to shift the balance of power in their favor without fighting each other directly, such as disinformation, cyber operations, intelligence operations, and economic coercion. Political warfare is designed to strengthen a state and weaken its adversaries by sowing or exploiting internal divisions, creating schisms within and among its partners, and draining its resources and energy. Other government officials and scholars have used different terms—such as irregular warfare, hybrid warfare, gray zone activity, asymmetric conflict, and the indirect approach—to capture some or all of these activities.¹³

As U.S. State Department diplomat George Kennan observed, “Political warfare is the logical application of Clausewitz’s doctrine in times of peace”—that is, in the absence of direct armed conflict. “Such operations are both overt and covert,” Kennan explained. “They range from such overt actions as political alliances, economic measures [such as the Marshall Plan during the Cold War], and ‘white’ propaganda to such covert operations as clandestine support of ‘friendly’ foreign elements, ‘black’ psychological warfare and even encouragement of underground resis-

tance in hostile states.”¹⁴ As Kennan argued, the creation and survival of the British Empire and the Soviet Union were in part caused by their effective application of political warfare.¹⁵

Political warfare involves actions that impact the cost-benefit calculations of states and their populations without resorting to brute force, which can often have high costs in blood and treasure.¹⁶ Political warfare can include several components:

- **Intelligence Operations:** The practice of obtaining political, military, economic, and other intelligence to coerce or otherwise gain a competitive advantage over an adversary. For the purpose of political warfare, these intelligence activities are more than just routine espionage since they are designed to weaken adversaries below the level of armed conflict. In addition, intelligence collection plays a critical role in informing and supporting *all* other components of political warfare.
- **Cyber Operations:** Actions taken through unauthorized access to computer networks to coerce or otherwise gain a competitive advantage over an adversary, ranging from denial of service to disruption and confusion, to physical, real-world effects like destruction of equipment through penetration of an industrial control system.
- **Information and Disinformation Operations:** The collection and dissemination of information to influence decisionmaking or popular support. As highlighted in Chapter 6, China has also used a specific type of influence operation, termed “united front work,” to gather information on, manage relations with, and attempt to influence individuals inside and outside of China—including individuals in overseas communities that hold political, economic, or academic influence.
- **Irregular Military Actions:** Activities taken by military forces—or units directly or indirectly linked to military forces—to coerce or otherwise gain a competitive advantage over an adversary below the threshold of armed conflict.
- **Economic Coercion:** The threat or actual imposition of economic costs or inducements on a target to influence decision-making or popular support and to gain a competitive advantage.

Political warfare is distinct from conventional warfare, which has sometimes been referred to as “regular” warfare. Conventional warfare involves the direct use of army, navy, air force, and other military capabilities to defeat an adversary’s armed forces on a battlefield; control territory, populations, and forces; or annihilate an enemy’s war-making capacity.¹⁷ Political warfare is also different from nuclear warfare, which involves the use of—or threat to use—nuclear weapons against adversaries.

Some might object that the concept of political warfare can include almost anything a state does below the threshold of armed conflict. But this would be incorrect. The vast majority of state activity overseas—such as routine diplomacy, development work, humanitarian assistance, and trade—are *not* examples of political warfare. States engage in numerous other actions that have nothing to do with political warfare, such as public financial management, infrastructure construction, asset management, market engagement, rule of law, and governance.¹⁸ What pushes an activity into the arena of political warfare is when its goal is to expand a country’s power and weaken its adversaries as part of balance-of-power competition. Political warfare is *power politics short of conventional war*.

Some might also be uncomfortable with using the term “warfare” to describe nonviolent actions such as economic coercion and information operations.¹⁹ But that is not how countries such as China see it. They apply a broad view of warfare as a struggle between competing entities and not just the use of brute force. China has used terms such as the “three warfares” (三战), which includes media, psychological, and legal warfare. None of the three warfares involves the use of violence.²⁰ As the Chinese general Sun Tzu remarked, the supreme art of war is to “subdue the enemy *without fighting*.”²¹ Other countries have also conceptualized warfare as including nonviolent actions. For example, Iran has utilized terms such as *jang-e narm* (soft war), which includes such activities as propaganda and disinformation to influence others. Likewise, Russia has used terms such as *aktivnyye meropriyatiya* (active measures) as a tool of warfare against the United States and its partners.

The *political* nature of political warfare is a critical component because states can use a range of tools below the threshold of armed conflict to influence, deter, or coerce others.²² Chinese activities are particularly well suited for examining the concept of political warfare because of

the ubiquitous role of the CCP, a *political* party, in society. The party has only strengthened under President and General Secretary Xi Jinping. As China expert Jude Blanchette contends, “Xi is surrounded by advisers who think primarily in political, not military terms.”²³ The result has been that political warfare is an important component of China’s tool kit. “Chinese military planners began to focus on ‘informationalization’ of the PLA,” notes David Kilcullen, “bringing it into the modern digital era and renewing their emphasis on political warfare.”²⁴

All countries—or at least all aspiring powers—utilize political warfare. But the Chinese practice of political warfare is different from many other countries in several respects. First is its size and scope. A much larger component of the Chinese government is engaged in political warfare than is typical of historical cases, and Chinese organizations are involved in a wide range of activities. During the Cold War, for instance, U.S. special operations forces and the Central Intelligence Agency (CIA) were primarily engaged in political warfare for the United States, while the KGB was the main actor for the Soviet Union. But China has leveraged the PLA, MSS, MPS, Ministry of Industry and Information Technology, United Front Work Department, Ministry of Foreign Affairs, and other agencies. Second, China is heavily engaged in co-opting, attempting to co-opt, and coercing Chinese diaspora populations overseas. This has led to a growth in extraterritorial activity—such as the establishment of so-called police stations overseas—to monitor, co-opt, and even harass Chinese citizens. Third, China under Xi Jinping is unusually concerned about protecting its image overseas and countering criticism from a wide range of actors, such as educational institutions, corporations, research organizations, media (including social media), and governments. This paranoia may be partly a desire to preserve the CCP’s rule—and indeed Xi Jinping’s legacy—and to prevent domestic opposition and instability.²⁵

CAVEATS

There are several limitations of this research. First, there are notable challenges in understanding China’s intentions, capabilities, and actions. China—including such organizations as the PLA—is opaque. China translates a limited amount of information into English. Western governments and academics have failed to translate into English and make publicly available some of China’s most

important military documents, speeches, and reports. Most Americans have to rely on what the CCP chooses to translate into English using state-run media and propaganda outlets. In addition, the Chinese system is structured in such a way that there is tremendous secrecy about the role that senior officials play and the mechanisms of government. To deal with these challenges, this report qualifies its judgments based on analyzing the available evidence, sourcing information, and highlighting information gaps.

Second, some Chinese political warfare activities are designed to be clandestine, making it difficult to assess what the Chinese government is doing, either directly or indirectly through proxies or partners. These proxies and partners can include front organizations, hackers, private security companies, fishing vessels, media organizations, spies, non-governmental institutions, and others. Because of the clandestine nature of some aspects of political warfare, it is sometimes impossible to know with certainty whether and how the Chinese government was involved. Again, this report has tried to qualify its judgments and document its primary and secondary sources.

Third, this report relies on unclassified and open-source information. Even classified assessments that use signals intelligence, human intelligence, satellite intelligence, and other types of intelligence face information hurdles and gaps in knowledge. A reliance on open-source information presents even greater hurdles. Nevertheless, taking precautionary steps—such as qualifying judgments where appropriate and identifying gaps in information—still leads to a useful understanding of Chinese political warfare.

Despite these caveats, this report is still able to compile a useful overview and understanding of Chinese political warfare.

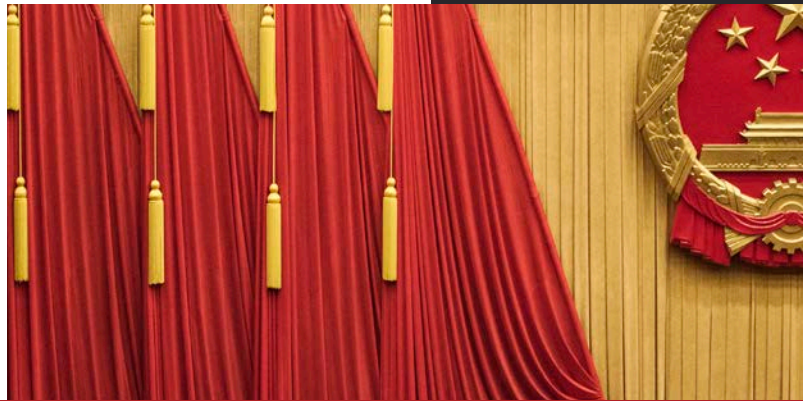
OVERVIEW OF THE REPORT

The rest of this report is divided into the following chapters to better understand Chinese political warfare. Chapter 2 provides an overview of the strategic logic of Chinese political warfare. Chapter 3 analyzes Chinese intelligence operations, which are important to all other aspects of political warfare. Chapter 4 focuses on Chinese cyber operations, including offensive cyber activities. Chapter 5 examines Chinese influence efforts, including information and disinformation operations. Chapter 6 explores united front work. Chapter 7 examines

China's irregular military actions, including using such means as fishing vessels, the People's Armed Forces Maritime Militia, and private security companies. Chapter 8 explores Beijing's global economic coercion. Finally, Chapter 9 outlines how the United States and its partners can better counter Chinese political warfare.

Sino-U.S. relations already cannot return to their former state. In response to the United States' multi-pronged attack and wide-ranging suppression, China must consider and formulate long-term and strategic response strategies.

-Ni Guihua and Zhu Feng¹



THE STRATEGIC LOGIC OF CHINESE POLITICAL WARFARE



中美关系已经回不到过去。应对美国的多头出击、多元打压，中国必须思考和制定长远和战略性应对策略。

-倪桂桦 朱锋²

2

China has a long history of political warfare.³

Between the third and fifth centuries BC, for example, Wu Qi, Sima Rangju, Sun Bin, Sun Tzu, and others were influential in the art of covert and clandestine activities.⁴ More recently, an assessment by two People's Liberation Army (PLA) officers concluded that the “use of asymmetrical measures, which create power for oneself and make the situation develop as you want it to, is often hugely effective.”⁵ This chapter provides an overview of Chinese political warfare. It asks two sets of questions: What are China's main goals in conducting political warfare, and how does China conceptualize the use of these activities? What are the primary organizations involved in political warfare? To answer these questions, the chapter examines Chinese and other primary and secondary sources.

The chapter makes two main arguments. First, China has several strategic goals in conducting political warfare. One set of goals is preserving the CCP, expanding Chinese power and influence, and weakening adversaries as part of balance-of-power competition. In addition, China aims to compete with the United States and other countries while *avoiding* conventional war and limiting security fears that might come from conventional military activities.

Second, numerous Chinese institutions are involved in political warfare, such as the PLA, Ministry of State Security, Ministry of Public Security, Ministry of Industry and Information Technology, United Front

Work Department, and Ministry of Foreign Affairs. There are also a wide range of non-state entities involved in political warfare, such as hacktivist organizations, member of the Chinese diaspora, and private security companies. While the Chinese government attempts to establish a whole-of-nation approach to domestic and international security, there is neither one clear strategic concept for political warfare nor one lead agency.

These two arguments suggest a complex bureaucratic structure of concepts, agencies, and actions involved in planning and executing political warfare. In some areas, such as intelligence operations and united front work, there is likely more centralization through the Ministry of State Security and United Front Work Department, respectively. But these activities are not always well synchronized. As the U.S. commander of the Office of Naval Intelligence assessed, “We have strong indications that Xi Jinping . . . is not aware of everything his security forces are doing. We think it's a function of the unwieldiness of China's governance model.”⁶

The rest of this chapter is divided into four sections. The first examines Chinese strategic goals in using political warfare. The second discusses major Chinese concepts for political warfare, which include a mix of military, economic, ideological, and other efforts designed to gain a competitive advantage. The third section describes the main organizations involved in Chinese political warfare. And the fourth provides a brief conclusion.

STRATEGIC GOALS

In utilizing political warfare, Chinese leaders likely have several goals that are interlinked. If implemented effectively, they can maximize benefits (such as expanding power and influence) and minimize risks (such as triggering security concerns and a balancing coalition).

First, China utilizes political warfare to preserve the CCP's rule, expand Chinese power and influence, and weaken its adversaries—especially the United States. These goals are in line with China's national strategy of achieving “the great rejuvenation of the Chinese nation on all fronts.”⁷ Chinese leaders view the international security environment as increasingly hostile and the United States as a major competitor. “The Central Committee has brought together the entire Party, the military, and the Chinese people and led them in effectively responding to grave, intricate international developments and a series of immense risks and challenges,” Xi noted in his report to the 20th National Congress of the Chinese Communist Party (CCP).⁸

The concept of “strategic advantage” (势 or *shi*) has long been an important aspect of Chinese strategic thinking and an influential component of military, diplomatic, intelligence, and other actions.⁹ Under *shi*, a state seeks a relative advantage over its opponent, no matter how slight. In this approach, *shi* is a dynamic—rather than fixed—concept and may evolve as the balance of power changes. As the Chinese scholar Zhongqi Pan argued: “What China fights for is not just national interests, but relative advantage in *shi*. . . . In terms of the strategic goal, China aims to build, accumulate and maintain a relative advantage of *shi* vis-à-vis other countries including the U.S. at regional level, and probably at global level as well.”¹⁰

Expanding Chinese power is part of Xi Jinping's desire for a “great national rejuvenation” and for the PLA to become a world-class military by 2049.¹¹ For Xi and other officials, the process of rejuvenation is in part a process of competition with its chief rival, the United States. This competition may not occur primarily on a conventional battlefield but rather in the economic, technological, informational, and diplomatic spheres. In the 20th National Congress report, Xi tasked the PLA with achieving the same three-stage military modernization plan (including a range of targets for 2027, 2035, and 2049) that has been in place since 2020. Part of China's focus is maintaining a

favorable external environment, including in the Indo-Pacific, in which countries align with and acquiesce to China's policies and preferences.¹²

Second, China likely utilizes political warfare to limit provoking other countries. The tools of political warfare are critical for expanding Chinese power and influence *without* triggering major pushback—including causing a conventional war or, at the very least, prompting an adversary to establish a balancing coalition.¹³ The desire to prevent a balancing coalition has a long tradition in balance-of-power politics. The growing strength and potential threat of a rising power have historically led one or more states to balance against the emerging power. Balancing states can increase their own economic and military power (internal balancing) or band together with a coalition of countries (external balancing).¹⁴ Military conquest by the rising power invariably causes fear among neighboring states and potential challengers.¹⁵ But it is less clear that political warfare elicits the same type of security concerns. As Bonny Lin argues in her analysis of Chinese gray zone actions, “These international tactics offer China more indirect and, in some cases, less visible and seemingly legitimate ways to pressure countries that could invite less regional or international criticism and pushback.”¹⁶

In short, China likely pursues political warfare in a competitive environment to increase its power and minimize potential opposition. These activities are part of the broader goals of China's rejuvenation by increasing military, economic, technological, political, and other forms of power.

KEY CONCEPTS

To achieve these goals, there are several concepts that China uses to capture aspects of political warfare. Table 2.1 highlights some of the key concepts, from strategic advantage (势) to military operations other than war (非战争军事行动).

One of China's most frequently used terms is military operations other than war (非战争军事行动, or MOOTW). For example, the 2020 edition of *The Science of Military Strategy*, published by the PLA's National Defense University, includes a comprehensive chapter on MOOTW, which it defines as “non-war military operations carried out by a country or political group to achieve a certain political goal.”¹⁷ The PLA's dictionary of military terms similarly defines MOOTW as “the armed forces' use of military operations to pro-

Figure 2.1

Concepts Relevant to Political Warfare

TERM	EXPLANATION
Asymmetric Means (非对称)	Use irregular means against an adversary, such as cyber warfare. ¹⁸
Civil-Military Fusion (军民融合)	Integrate security and development strategies to build an integrated national strategic system and capabilities to achieve China's goal of national rejuvenation. ¹⁹
Cognitive Domain Operations (认知域作战)	Adapt concepts such as public opinion and psychological warfare to the modern information environment by leveraging emerging technologies such as artificial intelligence. ²⁰
Discursive Power (话语权)	Conduct influence activities and make them internationally accepted. ²¹
Discourse War (话语战)	Influence civic discussions outside of China's borders. ²²
Economic Diplomacy (经济外交)	Engage in economic activities—including economic coercion—to advance national interests. ²³
Gray Zone (灰色地带)	Perform irregular military and other activity, including clandestine actions by Western countries. ²⁴
Hybrid Warfare (混合战争)	Orchestrate a mixture of conventional and irregular activity to achieve political objectives. ²⁵
Military Operations Other Than War (非战争军事行动)	Conduct non-war military operations to achieve a certain political goal. ²⁶
Overseas Strategic Strong Points (海外战略支点)	Establish Chinese-operated ports abroad, such as seaports, using diplomatic and other means to provide easier and more cost-effective means of conducting military operations than working with a foreign port authority or commercial entity. ²⁷
Peacetime Employment of Military Force (和平时军事力量运用)	Conduct military activities to deter or coerce an adversary that poses a threat—but without resorting to conventional war. ²⁸
Strategic Advantage (势)	Gain a relative advantage over the opponent, no matter how slight. ²⁹
Struggle (斗争)	Strive through violent or non-violent means to resolve what Marxist-Leninists deem to be “contradictions” in domestic and international society. ³⁰
Three Warfares (三战)	Create an information advantage through public opinion warfare (舆论战), psychological warfare (心理战), and legal warfare (法律战). ³¹
United Front (统战)	Protect and bolster the image of China and the CCP, including by monitoring and countering criticism overseas. ³²

tect national security and development interests that do not directly lead to war.”³³ MOOTW has generally included stability operations, maritime rights enforcement, and other actions designed to expand Chinese influence.

In 2003, the CCP's Central Committee and the Central Military Commission approved an important concept for the PLA called the “three warfares” (三战).³⁴ It includes three components: public opinion warfare (舆论战), psychological warfare (心理战), and legal warfare (法律战).³⁵ Building on Mao Zedong's contention that the military's goal is to carry out “the political tasks of the revolution,” the three warfares offer a way for the PLA to establish and expand Chinese political power and influence at home and abroad without resorting to armed conflict.³⁶ In this sense, the PLA is not a national military but rather the armed wing of the CCP,

which defends the *political* power of the CCP.³⁷ The components of the three warfares are intended to be reinforcing rather than mutually exclusive. Together, they are designed to help China wage information warfare against the United States and other competitors across the globe.

The first component, media warfare, involves the use of broadcast, print, and online efforts to influence domestic and international public opinion in ways that support Chinese interests and undermine its competitors. China recognizes that newspapers, television, radio, social media, and even organizations such as civilian institutions are all legitimate mediums to influence populations.³⁸ Overseas, China has waged media warfare through broadcasts of the state-run China Central Television (CCTV) and China Global Television Network (CGTN), inserts paid for by the Chinese government

in newspapers such as the *Washington Post* and *New York Times*, and educational institutions.³⁹

The second component, psychological warfare, is designed to sow dissent, disaffection, and discord among soldiers and the civilian population of competitors such as the United States.⁴⁰ Psychological warfare also leverages television, radio broadcasts, leaflets, and other mediums—much like media warfare—but it is designed to achieve military purposes. As one analysis in the PLA journal *China Military Science* concluded, the goal of psychological warfare should be to “sap the enemy’s morale, disintegrate their will to fight, ignite the anti-war sentiment among citizens at home, heighten international and domestic conflict, weaken and sway the will to fight among its high-level decision makers, and in turn lessen their superiority in military strength.”⁴¹

The third component, legal warfare, involves the exploitation of international and domestic law to assert the legitimacy of Chinese claims. *The Science of Military Strategy* argued that for the PLA, “international law is a powerful weapon to expose the enemy, win over sympathy and support of the international community [for China], and to strive to gain the position of strategic initiative.” It went on to explain that China needed to publicize its “own humanitarianism and reveal a lot of the war crimes committed by the opponent in violation of law . . . to compel [the] opponent to bog down in isolation and passivity.”⁴² Influential Chinese military texts emphasize that the PLA should justify its military actions through legal means before beginning any conflict.⁴³

In addition, Chinese leaders and experts have utilized other concepts to describe elements of political warfare, which are highlighted in Figure 2.1. These include asymmetric means (非对称), civil-military fusion (军民融合), cognitive domain operations (认知域作战), discursive power (话语权), discourse war (话语战), economic diplomacy (经济外交), gray zone (灰色地带), hybrid warfare (混合战争), overseas strategic strong points (海外战略支点), peacetime employment of military force (和平时期军事力量运用), strategic advantage (势), struggle (斗争), and united front (统战). China has also utilized such notions as the “holistic security concept” (整体安全概念) to expand the definition of security at home and abroad to include nearly a dozen fields, including political, territorial, military, economic, cultural, social, scientific and technological, information, ecological, financial, and nuclear security.⁴⁴

MAIN ORGANIZATIONS

There are several organizations involved in spearheading political warfare, such as the PLA, Ministry of State Security, Ministry of Public Security, Ministry of Industry and Information Technology, United Front Work Department, and Ministry of Foreign Affairs. As this report highlights, there are also nongovernment actors—from hacktivists to private security companies and Chinese citizens—involved in political warfare. Figure 2.2 highlights some of the most important state organizations and examples of their activities. While the Chinese government—especially the CCP—attempts to establish a whole-of-nation approach, there is no single, centralized organization involved in *all* of these political warfare activities. Instead, there are multiple overlapping entities that span the military, economic, political, ideological, intelligence, law enforcement, and other realms. As this section notes, there are a range of non-state actors—from fishing vessels to hackers—that are also involved in political warfare.

PEOPLE’S LIBERATION ARMY

The PLA is involved in a range of political warfare activities in addition to preparing for conventional and nuclear war and deterrence. The PLA sits under the broader command and control of the Central Military Commission, which is China and the CCP’s main national defense organization and is chaired by Xi Jinping. The PLA Navy (PLAN), PLA Air Force (PLAAF), PLA Army (PLAA), PLA Rocket Force (PLARF), and other organizations play important roles.

The PLAN, for example, has been involved in harassing and disrupting commercial activities in disputed territories as well as sailing into contested territory in the East China Sea, Senkaku Islands, Thitu Island, and other areas. The PLAAF has conducted air operations—including with unmanned aircraft systems (UASs)—in disputed territories and harassed specific commercial activities, including around the Spratly Islands, the Taiwan Strait, and other locations. The PLAA and PLARF have also conducted political warfare activities against such countries as India, including around the disputed China-India border.⁴⁵

In addition, the People’s Armed Police (PAP) and the China Coast Guard (CCG) have been involved in political warfare activities. The PAP is a paramilitary force within China’s armed forces charged with maritime security and internal security. The CCG, which is subordinate to the PAP, is re-

Figure 2.2

Examples of Chinese Organizations Involved in Political Warfare

ORGANIZATION	EXAMPLES OF ACTIVITY
China Coast Guard	Conducts maritime operations, including around disputed territory.
People's Armed Forces Maritime Militia	Conducts maritime operations, including around disputed territory.
People's Armed Police	Conducts internal security, riot control, disaster response, and maritime rights protection.
People's Liberation Army	
— <i>PLA Air Force</i>	Conducts air operations—including with unmanned aircraft systems (UASs)—in disputed territories and harasses specific commercial activities.
— <i>PLA Army</i>	Orchestrates land-based operations to collect intelligence and conduct subversive activities.
— <i>PLA Navy</i>	Harasses and disrupts specific commercial activities in disputed territories and sails into contested territory in the East China Sea, Senkaku Islands, and other areas.
— <i>PLA Rocket Force</i>	Orchestrates land-based operations to collect intelligence and conduct subversive activities.
— <i>PLA Strategic Support Force</i>	Conducts offensive cyber operations, intelligence collection, and information operations.
Ministry of Foreign Affairs	Orchestrates information, disinformation, and misinformation activity and engages in subversive efforts to expand Chinese influence and power.
Ministry of Industry and Information Technology	Oversees China's network infrastructure and coordinates with technology companies and universities.
Ministry of Public Security	Monitors dissidents and foreigners, particularly those located within China.
Ministry of State Security	Conducts intelligence operations (including against members of the Chinese diaspora) through human intelligence, signals intelligence, and other means; oversees counterintelligence; conducts cyber operations, including offensive cyber operations; and orchestrates a range of subversive activity.
United Front Work Department	Conducts information, disinformation, and misinformation activity to protect and bolster the image of China and the CCP, including by pressuring individuals and organizations overseas.

SOURCE: CSIS RESEARCH AND ANALYSIS.

sponsible for a broad range of maritime security missions and has as many as 1,040 regional and oceangoing patrol vessels.⁴⁶ The People's Armed Forces Maritime Militia (PAFMM), which is a subset of China's national militia, is involved in protecting maritime claims, conducting surveillance and reconnaissance, protecting fisheries, and conducting search and rescue missions. It is also involved in political warfare, especially to advance China's disputed sovereignty claims in such areas as the South and East China Seas.⁴⁷ These Chinese organizations have also leveraged non-state actors, including those involved in fishing. Mao Zedong argued that the PLA needed to leverage fishermen as an important component of competition, stating "The navy must also rely on the people; it must rely on fishermen. It must plant roots among the fishermen."⁴⁸

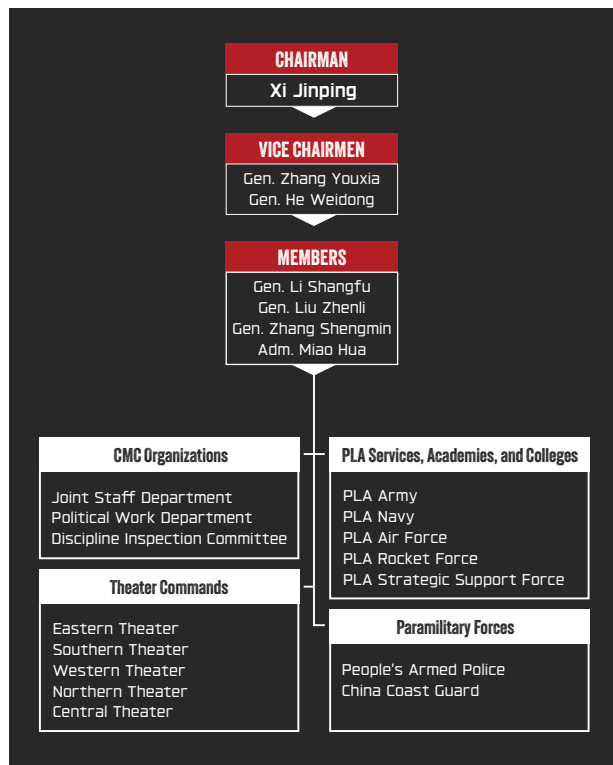
The PLA has also been involved in influence operations through the Strategic Support Force (SSF), a

theater-level organization established to centralize the PLA's space, cyber, electronic, information, communications, and psychological warfare missions.⁴⁹ The SSF combines technology and information systems into an organization that is critical for offensive cyber operations as well as intelligence gathering and technical reconnaissance.⁵⁰ As part of its modernization effort, the PLA consolidated previously decentralized cyber units into the SSF beginning in late 2015 and throughout 2016 to improve the PLA's combat capabilities. This effort was designed to create a more efficient and effective organization that could conduct cyber defense, espionage, and offensive operations.

Cyber operations are centralized under the Networks Systems Department. It includes the previous Third Department (3PLA), which housed the majority of cyber operations; Fourth Department (4PLA), which was responsible for computer network attacks; and the Informatization Department,

Figure 2.3

China's Military Leadership



SOURCE: U.S. DEPARTMENT OF DEFENSE, *MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA* (WASHINGTON, DC: OFFICE OF THE SECRETARY OF DEFENSE, 2022), 43, [HTTPS://MEDIA.DEFENSE.GOV/2022/NOV/29/2003122279/-1/-1/1/2022-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF](https://media.defense.gov/2022/NOV/29/2003122279/-1/-1/1/2022-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF); BRIAN WAIDELICH, *CHINA'S NEW MILITARY LEADERSHIP: POSSIBLE STRENGTHS AND WEAKNESSES* (ARLINGTON, VA: CENTER FOR NAVAL ANALYSES, NOVEMBER 11, 2022), [HTTPS://WWW.CNA.ORG/OUR-MEDIA/INDEPTH/2022/11/CHINAS-NEW-MILITARY-LEADERSHIP-POSSIBLE-STRENGTHS-AND-WEAKNESSES](https://www.cna.org/our-media/indepth/2022/11/chinas-new-military-leadership-possible-strengths-and-weaknesses).

which handled network defense.⁵¹ The Network Systems Department includes such elements as the 61726 Unit (Wuhan) and the 61786 Unit (Beijing). The 311 Base that oversees the three warfares is directly under the PLASSF, as are PLA Units 61486 and 61419, which have been tied to cyberattacks against European, U.S., Japanese, and South Korean officials.⁵² Figure 2.3 highlights some of China's main military organizations, which all sit under the Central Military Commission.

MINISTRY OF STATE SECURITY

The Ministry of State Security (MSS) is China's main civilian intelligence and counterintelligence authority responsible for domestic and foreign intelligence operations. The organizational structure of the MSS consists of a central ministry, provincial state security departments, and state security bureaus. The 2017 National Intelligence Act gave the MSS broad powers to compel Chinese citizens and organizations to assist with intelligence activities as

well as to monitor domestic and foreign individuals and entities.⁵³ This power allows China to leverage a range of non-state actors to assist with intelligence collection. Indeed, China has historically relied on front organizations, contractors, and private citizens to conduct state-sponsored offensive cyber operations, which allows the government to claim deniability.⁵⁴

The MSS is heavily involved in influence operations overseas, which is a critical aspect of political warfare. For example, the MSS's Tenth Bureau infiltrates overseas Chinese student and dissident groups, the Eleventh Bureau engages Western diplomats and others, and the Twelfth Bureau manages front organizations designed to influence Western targets of influence.⁵⁵ As MI5, the United Kingdom's domestic intelligence agency, warned UK citizens:

The motive behind Chinese intelligence service cultivation of Westerners is primarily to make “friends”: once a “friendship” is formed [they] will use the relationship to obtain information which is not legally or commercially available to China and to promote China's interest. Cultivation of a contact of interest is likely to develop slowly: [they] are very patient. . . . The aim of these tactics is to create a debt of obligation on the part of the target, who will eventually find it difficult to refuse inevitable requests for favours in return.⁵⁶

MINISTRY OF PUBLIC SECURITY

The Ministry of Public Security (MPS) is the lead domestic civilian police force, with responsibility for establishing public order, supervising public information networks, and conducting other law enforcement functions. It shares the counterintelligence mission with, and is directed by, the MSS. This shared mission with the MSS typically involves monitoring dissidents and foreigners located within China as well as policing the internet and social media platforms. The MPS's Eleventh Bureau, the Cybersecurity Protection Bureau, is involved in targeting cybercrime and overseeing the protection system for information security.⁵⁷ The MPS is involved in a range of political warfare activities, including influence operations, cyber activity, and monitoring members of the Chinese diaspora overseas through extraterritorial police stations.

MINISTRY OF INDUSTRY AND INFORMATION TECHNOLOGY

The Ministry of Industry and Information Technology (MIIT) oversees China's network infrastructure, including data security. The MIIT has coordinated with technology companies, including Huawei and

Tencent, as well as elite universities to develop an open-source hosting platform in China, relying on Gitee, the Chinese alternative to GitHub.⁵⁸

UNITED FRONT WORK DEPARTMENT

Overseen by the Central Committee of the CCP, the United Front Work Department (UFWD) attempts to protect and bolster the image of the party by monitoring and countering criticism overseas—often by recruiting or pressuring the Chinese diaspora. The Chinese government considers members of the diaspora to be “overseas compatriots” (侨同胞们), who owe a measure of loyalty to the Chinese homeland.⁵⁹ There is purposefully some confusion about UFWD activity, as MSS personnel have operated under the cover of the UFWD.⁶⁰

More broadly, the CCP has long emphasized the importance of united front work to conduct influence operations, with Xi Jinping calling it a “magic weapon” (法宝).⁶¹ Since 2015, Xi has advocated for the “Great United Front” and endeavored to reinvigorate united front work across the globe. Rather than leaving united front work only up to the UFWD, the Great United Front initiative supports united front work as a critical aspect of the CCP. United front work focuses on several targets: members of minority political parties (parties other than the CCP which are legally allowed to exist); general individuals who are not members of the CCP; intellectuals who are not members of the CCP; ethnic minorities; important religious figures; key corporate officials; members of the new social strata; students that are overseas or who have recently returned, including their relatives in the mainland; compatriots in Hong Kong, Macao, and Taiwan, including their relatives in the mainland; and overseas Chinese, returned overseas Chinese, and relatives of overseas Chinese.⁶²

MINISTRY OF FOREIGN AFFAIRS

The Ministry of Foreign Affairs (MFA) is responsible for the foreign relations of China, including formulating foreign policy, administering the nation’s diplomatic missions, representing Chinese interests at the United Nations, negotiating foreign treaties, and advising the State Council on foreign affairs. Foreign affairs officials have also been involved in political warfare actions.

Following the outbreak of Covid-19, for example, senior officials from the MFA were heavily involved in disinformation and misinformation—including efforts directed at the United States. Zhao Lijian, an MFA spokesman, wrote on Twitter in March 2020 that the U.S. military might have spread

Covid-19 in the Chinese city of Wuhan. “It might be US army who brought the epidemic to Wuhan,” he wrote. “Be transparent! Make public your data! US owe us an explanation!”⁶³ The claim that the U.S. Army had infected individuals in Wuhan was utterly false. Undeterred, the Chinese government amplified the claim on the official Twitter accounts of Chinese embassies and consulates.

The MFA was also involved in an influence campaign directed at the National Basketball Association, which is discussed in more detail in Chapter 5. In 2019, the Chinese government reacted angrily when Daryl Morey, the general manager of the Houston Rockets basketball team, supported protesters in Hong Kong. He tweeted: “Fight for Freedom. Stand with Hong Kong.”⁶⁴ In response, the Chinese consulate in Houston released a statement expressing its “strong dissatisfaction” with Morey’s tweet, noting that “anybody with conscience would support the efforts made by the Hong Kong Special Administrative Region to safeguard Hong Kong’s social stability.”⁶⁵ In 2020, the U.S. government retaliated by ordering China to close its consulate in Houston.⁶⁶

Overall, a range of state organizations—such as the PLA, MSS, MPS, MIIT, UFWD, and MFA—are integral to the planning and execution of political warfare. These organizations have frequently leveraged private citizens (including overseas Chinese), companies, and non-governmental organizations to assist in irregular activities.

CONCLUSION

As this chapter shows, political warfare is an important aspect of China’s strategy of national rejuvenation. China conducts political warfare to expand its power and influence below the level of armed conflict and to minimize security concerns that might be triggered by conventional warfare. Chinese leaders are sensitive about being perceived as revanchist. During the 20th National Congress, Xi Jinping adamantly noted that China was only interested in “peaceful development,” including a desire to “further consolidate national security; fulfill the goals for the centenary of the People’s Liberation Army in 2027; make solid progress in building a *Peaceful China*.”⁶⁷

Chinese state and non-state actors have conducted several types of activities as part of political warfare: intelligence operations, cyber operations, information and disinformation operations, united front activity, irregular military actions, and eco-

conomic coercion. For example, the CCP has used its economic clout to suppress international criticism of its own violations of democratic principles and human rights. It has also pressured governments, international institutions, and the private sector to echo its preferred narrative.⁶⁸

The stakes are high. For the United States and the West at large, China is the chief ideological opponent, largest economic and technological competitor (including in such battlegrounds as microelectronics, 5G wireless technology, and artificial intelligence), most capable military challenger, and greatest geopolitical rival.⁶⁹

To help understand the nuances of China's political warfare, the next chapter focuses on intelligence operations.

The ability of foreign affairs, news, military, security, and other departments to collect information and intelligence has been significantly improved, and the ability of relevant leading departments to comprehensively evaluate information and intelligence has continuously strengthened.

-Zhang Tuosheng¹



INTELLIGENCE OPERATIONS

安全等部门搜集信息情报的能力明显提高,有关领导部门综合评判信息情报的能力不断加强。

-张沱生²

3

This chapter examines Chinese intelligence operations as part of political warfare, particularly Chinese actions against the United States.

While espionage is a normal part of statecraft, this report focuses on the political warfare aspects of intelligence operations. Intelligence operations play a critical role in political warfare by helping states—in this case China—obtain political, military, economic, and other information to coerce or otherwise gain a competitive advantage over an adversary. Intelligence operations also play an important role in informing and supporting other components of political warfare, such as information and disinformation campaigns, united front activity, and economic coercion. As Linda Robinson concludes in her study of political warfare, “Political warfare places a high demand on intelligence.”³ As another assessment concludes, “Conducting political warfare by trying to build up foreign groups requires reliable intelligence about those groups’ motivations as well as about their capacities.”⁴

Few characterizations better describe the modern Chinese intelligence apparatus than a passage from the 2,400-year-old military treatise *The Methods of the Sima*: “In general, to wage war: employ spies against the distant, observe the near.”⁵ Along these lines, this chapter analyzes how China’s military and civilian intelligence services employ spies as part of political warfare, with the primary in-

tent of illuminating Chinese human intelligence (HUMINT) tradecraft and collection priorities. Overall, Chinese overseas intelligence activities are more centrally directed and driven by specific intelligence priorities than is typically acknowledged. Many—including the chief of the United Kingdom’s Security Service (MI5)—describe China pursuing a “thousand grains of sand” intelligence strategy, describing how China uses citizens in key positions to collect small pieces of information that together form a more complete intelligence picture.⁶ Such a strategy is much harder to disrupt. As this chapter shows, the empirical, open-source record indicates that Chinese HUMINT operations are methodical, resource intensive, and driven by well-defined intelligence priorities.

This chapter diverges from most existing literature on Chinese intelligence activities by analyzing Beijing’s HUMINT services through the lens of the HUMINT agent acquisition cycle, the five-phase process used by intelligence officers to spot, assess, develop, recruit, and handle human sources.⁷ This process is important in understanding Chinese political warfare. The analysis relies on a review of cases of known or suspected Chinese intelligence activities, with a particular focus on cases dating from 2015 to present. It includes an evaluation of court records from more than 100 U.S. indictments of individuals accused of conducting activities on behalf of China as well as analysis of similar cases overseas where that data is available.

Although Chinese primary source documents describing the structure and operations of the country's civilian and military intelligence services are scarce, recent Chinese counterintelligence investigations and disclosures by intelligence and law enforcement agencies worldwide are generating an increasing volume of data that illuminates the operational tradecraft of China's intelligence services. These disclosures expose key patterns and commonalities across cases during each phase of China's efforts to recruit sources and to shape these sources' collection. While the majority of data analyzed in support of this chapter were derived from U.S. federal court documents, there is ample evidence that the Chinese intelligence tradecraft and collection priorities apply equally to U.S. partners. As such, these findings—although largely focused on U.S. examples—can contribute to global efforts to detect and disrupt Chinese intelligence operations.

The remainder of this chapter begins with a brief overview of China's intelligence services. It then proceeds into further analysis of how the Chinese intelligence services execute overseas operations across the spotting, assessing, developing, recruiting, and handling phases, which are critical for political warfare. Finally, this chapter examines Chinese intelligence and law enforcement efforts to intimidate and harass members of the Chinese diaspora living overseas—including in the United States—by such organizations as the Ministry of Public Security.

CHINA'S INTELLIGENCE SERVICES

Contemporary Chinese intelligence activities are primarily conducted under the 2017 National Intelligence Law. The law does not explicitly define the roles and responsibilities of the civilian and military agencies that comprise China's intelligence community, but it describes many of the intelligence services' broader authorities. For example, Article 7 requires that “all organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with the law, and shall protect national intelligence work secrets they are aware of.” Article 12 authorizes China's intelligence services to “establish cooperative relationships with relevant individuals and organizations and retain them to carry out related work.”⁸ Both of these provisions establish the legal basis for some of the Chinese intelligence services' key patterns of behavior, specifically their heavy reliance on various cut-outs and proxies.

Intelligence serves a central role in broader Chinese Communist Party (CCP) history and lore. In 1931, three CCP spies who had penetrated the Kuomintang security apparatus provided early warning that a high-level CCP intelligence official had defected to the Kuomintang. Mao Zedong later claimed that this operation—known as the Three Heroes of the Dragon's Lair—changed the course of the revolution by warning key underground cadre that they would soon be exposed. Among those who were saved was China's future premier Zhou Enlai, who served a key role in Chinese intelligence and security affairs until his death in 1976.⁹

The Chinese intelligence apparatus has been reorganized repeatedly since the founding of the CCP and the establishment of the People's Republic of China (PRC). While roles, missions, and organizational structure have changed, the one constant is that the CCP and China have maintained formalized, professional intelligence services since the party's founding in 1927.¹⁰ This structure has evolved today into a broader Chinese intelligence community that includes both civilian and military elements, as outlined in Figure 3.1.

On the civilian side, the Ministry of State Security (MSS) has been Beijing's premier foreign intelligence service since it was established in 1983. The MSS is often described as combining the foreign intelligence collection responsibilities of the Central Intelligence Agency (CIA) with the domestic counterintelligence and counterespionage authorities of the Federal Bureau of Investigation (FBI). This analogy is useful—up to a point—in describing the overarching mission of the MSS. However, the MSS combines these foreign and domestic authorities in unique ways when conducting its operations. This results in several hallmark characteristics of Chinese intelligence operations. Perhaps most notable is Beijing's continued reliance on mainland China not just as a hub for operational oversight and coordination but for the actual business of recruiting and handling foreign sources.

The MSS is composed of a headquarters component and approximately 18 component bureaus. Each of these subordinate bureaus is assigned a number and charged with a specific functional or regional portfolio. For example, as of 2018, the Sixth Bureau was responsible for overseas collection on science and technology issues.¹¹ The MSS also maintains provincial and city divisions and bureaus, such as the Shanghai State Security Bureau, the Beijing State Security Bureau, and the Jiangsu State Security Department (JSSD). Each of these regional MSS offices mirrors the num-

bered component structure of MSS headquarters so that the JSSD, for example, has its own Sixth Bureau that likely coordinates with the Sixth Bureau at MSS headquarters in Beijing. Several scholars over the years have scoured Chinese primary sources in an effort to map the specific structure, roles, and responsibilities of the MSS. However, the accuracy of this work is variable and often becomes quickly dated. One attribute that the Chinese intelligence services share with their Western counterparts is a tendency to reorganize, including the MSS's rearrangement of bureau numbers. For example, MSS files disclosed in a U.S. court case revealed that the overseas science and technology bureau in the JSSD was renumbered from the Fourth Bureau to the Sixth Bureau in December 2013.¹²

The Ministry of Public Security (MPS) is China's primary domestic security service. The MPS is mainly responsible for police work within China, but it also has extensive internal security authorities. Since the initiation of Xi Jinping's anti-corruption campaign at the 18th Party Congress in 2012, the MPS has been increasingly tied to overseas operations. These activities are less focused on collecting political, economic, or military intelligence information. Instead, they are an extension of a decades-long role for the MPS in "political security," which includes efforts to exert pressure on overseas dissidents and perceived enemies. The MPS traditionally has undertaken domestic activities to send messages to its targets overseas, such as by arresting family members in China.¹³ The MPS continues this specific technique but is now augmenting this domestic pressure with deployments overseas to harass, intimidate, and repatriate overseas Chinese citizens who Beijing accuses of political or financial corruption.¹⁴ These activities are likely spearheaded by the MPS's First Bureau, which is reportedly responsible for monitoring Chinese political dissidents who live outside of China.¹⁵

For the United States and its partners, the MPS's overseas operations are arguably the most concerning of any of China's overseas intelligence activities. This is because the MPS is engaged in operations that extend far beyond the boundaries of traditional espionage. Espionage—that is, spying on other nations to glean insights about their capabilities and intentions—is an accepted, acknowledged, and normal practice by intelligence agencies in the arena of geopolitics. MPS operations, however, are often something entirely different. In many circumstances, they manifest in egregious violations of another na-

tion's sovereignty or reflect a blatant refusal to accept international law. These operations involve attempts by Beijing to extend the arm of its increasingly authoritarian governance to any of its perceived enemies, anywhere in the world—even if it means violating the constitutions and laws of the democratic nations where the MPS conducts these activities. Examples include uncoordinated law enforcement activities on a global scale, with recent reports indicating that Chinese law enforcement elements have quietly established more than 50 "overseas police service centers" in 21 countries across five continents.¹⁶

Within the People's Liberation Army (PLA), two branches are primarily charged with intelligence duties. The Intelligence Bureau of the Joint Staff Department of the Central Military Commission is the PLA's primary HUMINT arm, roughly equivalent to the U.S. Defense Intelligence Agency (DIA).¹⁷ Prior to the large-scale reorganization and modernization of the PLA in late 2015, the Intelligence Bureau was known as the Second Department of the General Staff Department of the PLA, more commonly known as 2PLA. The bureau was traditionally complemented by signals intelligence, electronic warfare, information operations, and offensive cyber capabilities within the Third Department (3PLA) and Fourth Department (4PLA).¹⁸ Of these groups, 3PLA maintains the highest public profile outside of China. The U.S. Department of Justice (DOJ) indicted five 3PLA computer network operators in 2014, and the economic espionage activities of one of the organization's components (Unit 61398) were exposed by a U.S. cybersecurity firm in 2013.¹⁹ Both 3PLA and 4PLA were renamed and reorganized during a series of PLA reforms in late 2015, with both components likely integrated into the Network Systems Department of the PLA's Strategic Support Force (SSF), which is also subordinate to the Central Military Commission.²⁰

CHINA'S INTELLIGENCE DOCTRINE AND THE AGENT ACQUISITION CYCLE

This chapter's focus on examining Chinese intelligence operations through the lens of the agent acquisition cycle serves two purposes. The first purpose is to illuminate how China's national-level intelligence collection priorities are operationalized by the intelligence services. This includes describing how the MSS and its counterparts

identify and approach potential sources, task and handle these sources, and how the services work with specific customers to refine information needs and requirements. The second purpose is to examine how the various elements of the Chinese state—including the CCP, state research institutions, private companies, and the technical, cyber, and HUMINT elements of the intelligence services—contribute to Chinese intelligence operations. The goal is to provide a more coherent alternative to the common characterization of the Chinese intelligence threat as “one thousand grains of sand.” This term can lend the inaccurate impression that China’s activities are decentralized and opportunistic, while also opening the United States and its allies to criticism that they are indiscriminately targeting Chinese academics, students, businesspeople, and journalists by labeling them all as suspected agents of the CCP. The intent is to use fact-based, empirical evidence to illuminate Chinese intelligence tradecraft, which includes the activities of the state organs, affiliated research and development institutions, and various cut-outs, co-optees, and nontraditional collectors.²¹

Chinese primary sources describing Beijing’s modern approach to intelligence theory, doctrine, and operations are less abundant compared to writings on other security topics, particularly Beijing’s views on military modernization and strategy. Nevertheless, Chinese documents across the spectrum of national security strategy and doctrine reflect the abiding importance of intelligence in statecraft and warfare. Information is at the heart of Beijing’s military modernization efforts, which emphasize the pursuit of “information dominance.” While these documents reflect the enduring importance of intelligence to modern China, much of what Western scholars know about the specifics of how China’s clandestine services advance Beijing’s interests come from the U.S. prosecution of Chinese officers and agents, public warnings from Western leaders, and non-government analysts.

One of the few Chinese-language documents available in the West illuminating China’s approach to intelligence work is a book published in 1991 by two Chinese intelligence veterans—Huo Zhongwen and Wang Zongxiao—titled *Sources and Techniques of Obtaining National Defense Science and Technology Intelligence*. It describes a broader Chinese intelligence apparatus that is built to advance both national security and commercial interests. The book examines how science and technology collection is a shared

responsibility across the intelligence services, research and academic institutions, and state-owned enterprises. It is a system that maintains no clear lines between military modernization and economic growth, a distinction that—at least in the United States—is a line established in intelligence policy and doctrine.²² As Huo and Wang conclude: “Intelligence work will become the heart of the new industrial revolution.”²³ This perspective on intelligence can be observed in cases where China’s professional intelligence officers collaborate with science and technology institutions to identify collection requirements that advance China’s commercial interests.

Huo and Wang’s work also describes China’s historical reliance on open-source information, which in their estimation accounted for 80 percent of China’s science and technology intelligence collection. Like the Soviets during the Cold War, China recognized the intelligence value of various Western periodicals and government reports, and Huo and Wang’s work methodically details the specific governmental and nongovernmental sources of technical insights that were of particular benefit to China’s commercial and military modernization. Nevertheless, they acknowledge that the remaining 20 percent of China’s intelligence needs “must come through the collection of information using special means, such as reconnaissance satellites, electronic eavesdropping, and the activities of special agents (purchasing or stealing), etc.”²⁴

Despite the blurring of national security and commercial interests in China’s approach to intelligence collection, Huo and Wang argue that China shares with the West similar perspectives on the broader intelligence collection process, specifically the intelligence cycle. They emphasize the importance of developing collection requirements, identifying the most effective means of collecting against certain requirements, and “immediately [analyzing and studying] the feedback that has been received from the information consumer and adjust the collection process in a timely manner, thus improving the work of collection.”²⁵ Although there is no definitive open-source Chinese intelligence doctrine available, the cases reviewed in support of this chapter strongly suggest that the MSS and its counterparts adhere to many of the same fundamentals of the traditional intelligence cycle and, as an extension of that cycle, the recruitment of human agents using techniques that are shared historically with China’s foreign counterparts, including the CIA, MI6, and Russian intelligence agencies.

SPOTTING AND ASSESSING

The overall agent recruiting process can be thought of as a filter, as illustrated in Figure 3.1. At the top are the two broadest phases: spotting and assessing. Activities within these two phases are highly interconnected, as they are both largely analytic and, in most circumstances, passive. It is also in these two phases where there is ample evidence demonstrating how the Chinese intelligence services integrate all-source capabilities into their efforts to identify and evaluate potential human sources. Specifically, China's intelligence services employ and often blend three primary techniques during the spotting and assessing phase: open-source intelligence analysis; domestic and overseas cut-outs, co-optees, and proxies; and technical operations, including computer network intrusions.

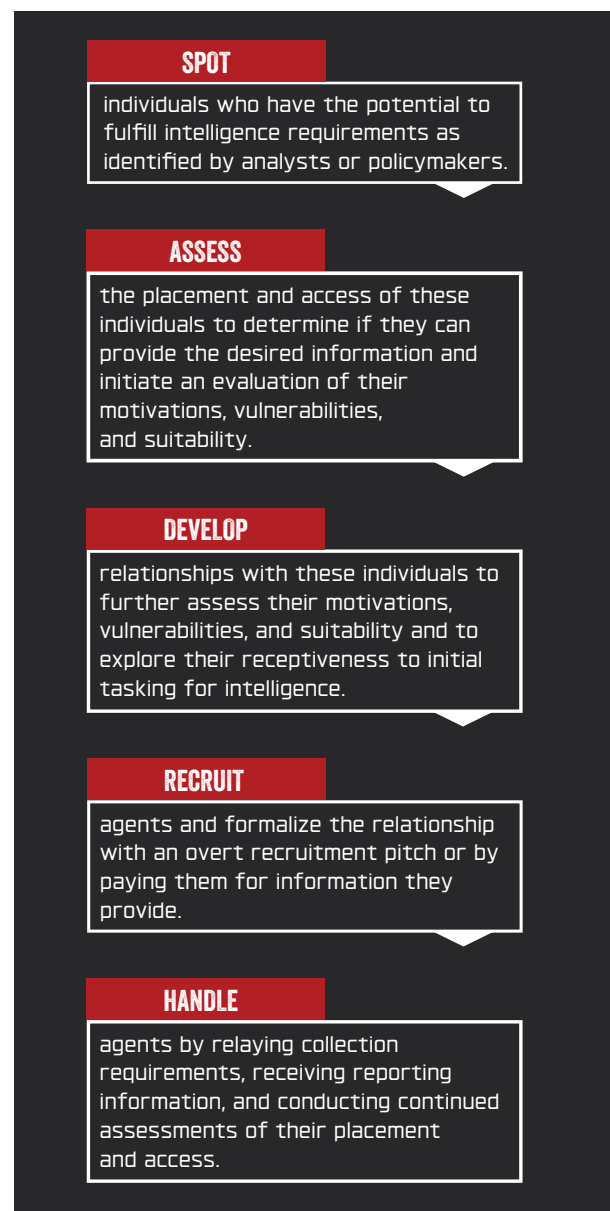
It is during the spot and assess phases that HUMINT collectors begin the process of transforming customer intelligence requirements into actual collection. Depending on the specificity of the information need, the potential pool of sources that are initially spotted and assessed can range from exceptionally large to exceptionally small. For example, one U.S.-based spotter for the MSS simply sought contact with individuals with current or prior military or intelligence experience. Initial contacts would be routed back to MSS officers in China for further assessment of the individual's potential access to classified or other non-public information that would be responsive to China's information needs. In other circumstances, the spotting and assessing pool will be narrowly tailored, such as focusing on individuals who may have access to highly specialized technologies that would contribute to China's economic or military modernization.

CUT-OUTS, CO-OPTees, AND PROXIES

One important trademark of Chinese intelligence operations is the use of various cut-outs, co-optees, and proxies. The use of such individuals—who often present themselves as businesspeople, students, or academics—creates a buffer of plausible deniability between China's intelligence apparatus and its potential human sources. China's clandestine services have not traditionally adopted the same operating models as their U.S., UK, Russian, or other counterparts. In these countries, intelligence officers are often celebrated for their ability to navigate hostile or denied environments. Leveraging various types of official or nonofficial cover, CIA, MI6, and KGB officers during the Cold War developed innovative and sophisticated tradecraft

Figure 3.1

The Agent Acquisition Cycle²⁶



SOURCE: CSIS RESEARCH AND ANALYSIS; AND BURKETT, "AN ALTERNATIVE FRAMEWORK FOR AGENT RECRUITMENT."

that they used to recruit and handle high-level sources within an adversary's government.

China's isolation during most of the Cold War fostered a very different HUMINT culture, one that involved a much less prominent overseas role for the intelligence cadre. Compounding this isolation was the paranoia of the Cultural Revolution, where the relentless focus on ideological purity and widespread suspicions of foreign influence resulted in purges within the intelligence and security apparatus.²⁷ The MSS did deploy some personnel abroad—for example, under journalistic

cover—during the Cold War, but their primary mission was unclear. They likely assisted broader efforts to spot and assess potential sources while also collecting insights and non-public information from individuals who believed they were speaking with Chinese state media.²⁸ However, none were definitively tied to sensitive recruitments within the U.S. government.

In addition, Chinese intelligence services have traditionally preferred that recruitments and subsequent source meetings occur inside of China or a third country.²⁹ The comparatively limited overseas footprint of China's HUMINT officers likely nurtured the culture of using proxies and cut-outs as key components in the spotting and assessing phase. In the current era, social media and the internet are increasingly used for the spotting and assessing phases, though recent cases reinforce that overseas proxies continue to be key contributors to early-stage recruiting efforts.

This includes the case of Jun Wei Yeo, a Singaporean national who was convicted in the United States on charges that he was serving as a spotter and assessor for the MSS.³⁰ Yeo received intelligence requirements from China-based MSS officers, who relied on Yeo to spot and assess potential U.S.-based sources. Yeo's MSS handlers had a wide range of intelligence interests, with a particular focus on non-public U.S. government information. These taskings included requests for Yeo to identify sources who could report on Southeast Asia, the U.S. Department of Commerce, artificial intelligence, and the trade war between the United States and China. On multiple occasions, Yeo met separately with different MSS officers in China, all of whom issued identical tasking.³¹ These incidents further reinforce this chapter's broader contention that Chinese intelligence collection is more centrally directed and organized than is often appreciated.³²

THE ROLE OF OPEN-SOURCE INTELLIGENCE AND SOCIAL MEDIA

Within the spotting and assessing phases, recent investigations and global intelligence service statements reflect that open-source intelligence analysis—particularly the exploitation of social media—has become a preferred technique for China's intelligence services. According to U.S., UK, and German intelligence officials, Chinese intelligence officers and proxies have conducted thousands of soft approaches on LinkedIn in recent years.³³ More than 10,000 such incidents have occurred in the United Kingdom alone, according to MI5 chief Ken McCallum.³⁴ A 2017 study conducted

by Germany's domestic intelligence service, the Bundesamt für Verfassungsschutz (BfV), found China's intelligence approaches on LinkedIn to match the scale observed by MI5. In its report, the BfV disclosed several inauthentic profiles and front organizations, posting as headhunters, consultants, think tanks, and scholars, who the service assessed were working for Chinese intelligence.³⁵ This shift toward social media in the early phases of the recruitment process offers the Chinese intelligence services a platform to conduct low-cost, low-risk activities in the early phases of the recruitment cycle.

Several notable investigations in the United States since 2017 reflect how China's intelligence services use LinkedIn to identify and evaluate potential sources of classified information, trade secrets, and other non-public information. In many instances, Chinese intelligence uses LinkedIn to identify and contact current and former cleared government employees or to advertise various business, consulting, and employment opportunities that may interest former members of the intelligence community or U.S. Department of Defense.³⁶ Jun Wei Yeo used social media, particularly LinkedIn, extensively in his activities on behalf of the MSS. Yeo created a fake consulting company and posted job opportunities on LinkedIn. He later claimed he received over 400 resumes, 90 percent of which were submitted by current and former U.S. government and military personnel with security clearances. Yeo then forwarded the resumes to MSS officers in China for further evaluation and guidance on potential recruitment options.³⁷ Yeo augmented his efforts on LinkedIn by attending public events to contact individuals from lobbying firms or defense contracting companies who could be possible targets.³⁸

COMPUTER NETWORK OPERATIONS

China's bulk data theft campaigns—including operations targeting the U.S. Office of Personnel Management (OPM), Equifax, Anthem, Marriott, and others—are examined in this report's chapter on Chinese cyber operations (Chapter 4).³⁹ Nevertheless, it is important to acknowledge the extent to which Beijing's acquisition of this data can contribute to HUMINT operations. While these operations have been attributed to various elements of the Chinese intelligence services—primarily regional components of the MSS and the 3PLA—there is little definitive evidence available detailing how China may be weaponizing this data.⁴⁰

However, the information from these operations could help HUMINT officers assess potential ave-

nues to recruit a source. Examples might include verifying an individual's current or prior relationship with the U.S. government, identifying whether that individual is in financial distress or poor health, scrutinizing their travel history, or shaping ways to develop an initial approach and a source development plan. Four factors typically influence an individual's decision to spy for a foreign government: money, ideology, compromise, or ego, often referred to as "MICE."⁴¹ What is known about the personal data that China has exfiltrated suggests that the information could be highly valuable for Chinese HUMINT recruiters weighing whether an individual may be vulnerable to certain recruitment approaches. The U.S.-based MSS spotter Jun Wei Yeo attested that these types of vulnerabilities, including financial troubles, job dissatisfaction, or familial issues, were what he was trained by the MSS to evaluate when assessing source candidates.⁴²

DEVELOPING AND RECRUITING

Spotting and assessing are intended to narrow a pool of potential source candidates. It is against this smaller group that intelligence officers initiate the process of building a relationship with prospective sources. Key markers of this phase for Chinese intelligence operations include increased face-to-face contact, often in China during the source development phase. Overall, the majority of development approaches analyzed in support of this research involved offers of employment, business, consulting, or other financial opportunities, with a smaller set of individuals driven by ideological support for China and the CCP. Ultimately, postmortems of historic American espionage cases find that most spies are motivated by a combination of the MICE factors rather than by one factor alone.⁴³

The developing and recruiting phases of the agent acquisition cycle substantially increase the volume of risk that a recruiting organization incurs. The spotting and assessing phases are largely passive, while the developing and recruiting phases are active and increasingly expose recruiters to potential discovery. China partially compensates for this risk during the development and recruitment phases by continuing its reliance on cut-outs, proxies, and other forms of cover. Chinese intelligence officers and their proxies primarily approach developmental sources under commercial or academic cover. There is a dual logic in this approach, providing plausible deniability to both recruiter and target.

Recruiters present themselves as representing private or academic interests rather than China and the CCP. This approach may appeal to prospective recruits interested in rationalizing their openness to providing information to a foreign entity. In the case of Kevin Mallory, his responsiveness to initial contact via LinkedIn translated into an introduction to an individual who represented himself as working for a Chinese think tank, the Shanghai Academy of Social Sciences. Despite these efforts to operate under the nominal cover of the academy, which is known to have close ties to the MSS, Mallory—as a former CIA and DIA officer—appears to have been aware that the individuals he met with were representatives of Chinese intelligence.⁴⁴

These types of approaches and initial taskings epitomize the developmental phases of HUMINT operations. Developmental recruits are often asked to share information that may be somewhat sensitive—though not classified—as a means to gauge the source's responsiveness to tasking, as well as to lay the groundwork for gradually expanding the information-sharing relationship into more sensitive areas.⁴⁵ The added exchange of money at this phase—even before any formal recruitment pitch—also establishes the terms of what will ultimately become a transactional relationship. In cases where the source is a U.S. government employee or cleared defense contractor, this information exposes the recruit to legal jeopardy.

China's development and recruitment of Shapour Moinian followed a similar pattern. After an initial approach on LinkedIn, Moinian traveled to Hong Kong to meet with an individual who claimed to represent a technical recruiting company seeking out aviation industry consultants. The Chinese recruiter claimed she was seeking Moinian's "rich experiences and skills" for a client who was working on aircraft design. Moinian agreed to provide information and materials regarding various aircraft designed or manufactured in the United States, for which he was financially compensated. An unnamed UK aviation expert mentioned by MI5 in July 2022 also traveled repeatedly to China to be "wined and dined." The Chinese interlocutors then asked and paid him for detailed technical information on military aircraft, at which point the UK government intervened.⁴⁶

Commercial cover was also a key feature of China's recruitment of former FBI electronics technician Kun Shan "Joey" Chun. However, unlike the Mallory and Moinian cases, where the developmental phase required only of a handful of meetings, Chun's

relationship with Chinese intelligence took several years to reach the stage where he began meeting directly with Chinese government officials and providing them with sensitive FBI information. Chun's relationship originated in 2005, when a China-based printer company solicited an investment from one of Chun's relatives. Over the next five years, the Chinese company paid for Chun to travel on an annual basis, travel that he actively concealed from the FBI. In 2011, the company paid for a trip to Europe, where Chun met directly with a Chinese government official who told Chun he knew he worked for the FBI. At this stage, Chun began reporting information about FBI personnel, structure, technological capabilities, surveillance practices, and surveillance targets.⁴⁷

One variation of China's efforts to appeal to commercial and economic interests of potential sources is the manner in which the intelligence services work through research institutes and universities. This includes recruitment into China's so-called "talent plans," such as the Thousand Talents Plan and the Hundred Talents Plan. Disaggregating the numerous licit and illicit mechanisms that China relies upon to acquire advanced technology from the United States is beyond the scope of this chapter. Nevertheless, several recent cases reveal how China's state-affiliated research institutions and the talent plans have served as critical platforms for China to extract trade secrets and intellectual property (IP) from U.S.-based sources. Although many cases do not involve a direct connection between China's research institutions and the intelligence services, there are some striking exceptions.

Most notable is the trial of Yanjun Xu, an MSS officer who was the deputy division director of the Sixth Bureau in the JSSD. In that case, the United States disclosed how the Sixth Bureau, which is responsible for overseas collection of science and technology information, worked directly with organizations such as the Jiangsu Science and Technology Promotion Association, the Aviation Industry of China (AVIC), and the Nanjing University of Aeronautics and Astronautics (NUAA) to arrange presentations and exchanges with overseas experts known to be working on technologies that were Chinese collection priorities.⁴⁸ This included Xu in his capacity as an MSS officer directly arranging a set of discussions in China with experts from across the global aviation industry, including representatives of at least six of the world's leading aerospace companies.⁴⁹ As reflected in Xu's communications with his intelligence customers within the Chinese science and technology apparatus, the purpose of these exchanges was to elicit

sensitive IP and trade secrets, including items such as design manuals, design and simulation software, composites, power systems, and other information about civilian and military aircraft.⁵⁰ The MSS often augments its human source development efforts during "exchanges" in China by conducting technical operations against their visitors' devices.⁵¹

Beyond the primary methods that China uses to spot, assess, develop, and recruit sources, the final element involves the specific tradecraft that China uses to handle its human sources.

HANDLING SOURCES: OPERATIONALIZING INTELLIGENCE REQUIREMENTS

China's global intelligence activities are merely one element of broader political warfare. Nevertheless, they are a critical element of Beijing's approach to security competition. China's pursuit of various forms of classified U.S. defense and intelligence information contributes to broader efforts to secure an information advantage over the United States, particularly if Beijing were to learn information about the United States that Washington believes to be protected. This logic extends into the science and technology sphere, where Chinese intelligence operations are designed to fulfill key knowledge gaps for China's commercial and military technology research and development efforts. China's intelligence services play a crucial role in recruiting human sources to fulfill specific customer science and technology requirements for China's economic and military advantage. It is in this area that the case of MSS officer Yanjun Xu is so striking.

As previously noted, Xu was a senior MSS officer assigned to the JSSD Sixth Bureau, where he was responsible for collecting overseas science and technology information. In his activities, Xu worked closely with officials in various state entities, including AVIC and the NUAA, to refine aviation-related collection requirements. For example, in 2013, Xu exchanged messages with an official at AVIC who relayed specific information that the AVIC official was seeking from Boeing, including analytical tools for Boeing's proprietary airframe and specific portions of the *Boeing Design Manual*.⁵² These types of exchanges are critical in understanding the specificity of Chinese science and technology collection requirements that were

directly passed from state-owned enterprises and research institutions to China's foreign intelligence service. Separate communications revealed how Xu and the MSS would report back information that had been collected. In one instance, Xu sent detailed technical information about various aspects of the KC-135 aerial refueling aircraft, requesting that the recipient review the information and provide feedback on the MSS's report.

These types of insights into the inner workings of the MSS and its customers manifest in the ways that China handles its human sources. In Xu's case, the MSS and the NUAA directly collaborated to shape the specific topics that visitors would brief during their presentations in China. In one case, Xu and the NUAA official worked in tandem to encourage a U.S.-based aerospace engineer to provide a presentation on highly technical topics related to GE Aviation's trade secrets and IP. As the relationship between Xu and the engineer progressed, Xu was clear about how information requirements were being developed, writing to the engineer: "I will touch base with the scientific research department here to see what technology is desired and I will let you know what to prepare." Xu later refined the specific areas of interest for the engineer, expressing that there was particular interest in software, system specifications, and design processes. Later, when the engineer expressed concern about sending certain information from his GE Aviation e-mail address, Xu responded: "It might be inappropriate to send directly from the company, right?"⁵³

OVERSEAS HARASSMENT AND REPRESSION

Chinese intelligence agencies have also been increasingly active in intimidating members of the Chinese diaspora overseas and in conducting influence operations. Many of these instances are part of Operation Fox Hunt, a global and extralegal PRC effort to monitor, harass, and in some cases repatriate Chinese diaspora living abroad. In June 2023, for example, a federal jury in New York convicted three individuals of stalking and coercing several residents of the United States.⁵⁴ In April 2023, the FBI arrested two individuals, "Harry" Lu Jianwang and Chen Jinping, in connection with opening and operating an illegal police station in Manhattan, New York City. According to the FBI and DOJ, the two individuals were working for the Fuzhou branch of the MPS to locate and conduct coercive activities against Chinese dissi-

dents living in the United States.⁵⁵ Lu Jianwang's official role was president of the America Changle Association NY, a nonprofit organization whose offices housed the police outpost.⁵⁶ In its response to the arrests, the Chinese embassy in Washington described the organization as being "provided by local overseas Chinese communities who would like to be helpful" and that "they are not police personnel from China."⁵⁷

In a separate case, the DOJ charged 40 MPS officers in April 2023 with conducting an intimidation campaign against Chinese nationals residing in the United States whose political views and actions were critical of China.⁵⁸ The DOJ has referred to this type of activity as "repression schemes."⁵⁹ Also in April 2023, a federal jury convicted Pras Michel, a Grammy-winning artist and former member of the hip-hop group Fugees, of working with the MPS to conduct a clandestine campaign to influence senior U.S. officials.⁶⁰ More broadly, the Chinese government has conducted widespread harassment of Chinese critics of China abroad, though it is not always clear if—and to what degree—Chinese intelligence and law enforcement organizations are involved. Beginning in October 2022, for example, China was allegedly involved in making more than a dozen false bomb threats at luxury hotels and embassies in Europe, the United States, the Middle East, and Asia using the names of Chinese dissidents.⁶¹

In addition to Operation Fox Hunt, China has also engaged in Operation Skynet, a parallel program to target the finances of Chinese citizens, including dissidents, residing overseas. According to the FBI, Operation Skynet includes PRC efforts to repatriate money by some Chinese living abroad "by both restricting and seizing assets still located in the PRC."⁶² In 2022, for example, DOJ charged Sun Hoi Ying with conducting illegal activities as part of Operation Skynet.⁶³

Chinese diplomatic officials argued that these organizations—including the so-called police stations—were not actually engaged in police and intelligence work and that they were staffed by "volunteers" who were responsible for assisting Chinese nationals with routine tasks, such as renewing drivers' licenses.⁶⁴ In some cases, researchers identified connections between various overseas police outposts and specific regional components of the MPS, tying such stations directly back to Chinese intelligence and law enforcement. One study of these MPS stations assessed that there are at least 104 of these outposts across 53 countries.⁶⁵ As an FBI investigation into a Chi-

nese police station in New York City found, the MPS was unambiguously involved in harassing members of the Chinese diaspora in the United States. According to the lead FBI agent involved in the investigation:

Although the MPS is generally identified as the PRC's primary domestic law enforcement agency—responsible for public safety, general criminal investigation, national security and internet security—its mission extends beyond law enforcement and into functions more associated with an intelligence service. The MPS routinely monitors, among others, Chinese political dissidents who live in the United States and in other locations outside the PRC. The MPS has used cooperative contacts both inside the PRC and around the world to influence, threaten and coerce political dissidents abroad. Indeed, I am aware that the PRC government has threatened and coerced Chinese political dissidents living in the United States in an effort to silence them.⁶⁶

CONCLUSION

Measuring the impact of Chinese intelligence operations as part of political warfare is challenging on several levels. The first challenge is defining what counts as intelligence operations in the modern era. China employs a wide range of licit and quasi-licit means to acquire sensitive and critical information. This includes investing in foreign firms that possess valuable IP that can support China's military or commercial interests. It includes the use of "talent programs" and other joint research initiatives to facilitate the transfer of valuable technical knowledge back to Chinese institutions. As the U.S. Senate Select Committee on Intelligence acknowledged in a comprehensive study of the U.S. counterintelligence enterprise, competitors need not break U.S. laws to fulfill key intelligence collection needs. In one noteworthy recent study, a U.S. private intelligence firm identified 167 individuals connected to Los Alamos National Laboratory who had returned to China to work in areas critical to the PLA's military modernization, including hypersonic weapons, deep-penetrating munitions, and undersea systems.⁶⁷ A separate investigation by the *Washington Post* found that Chinese hypersonic researchers are simply purchasing from U.S. suppliers software that aids in designing and modeling hypersonic systems.⁶⁸

In addition, there are concerns about cyber-enabled economic intelligence efforts, which are analyzed in this report's chapter on Chinese cyber operations (Chapter 4). The economic and strategic benefits of these activities are vast, particularly in terms of trade secrets, military technology, and sensitive U.S. government information stolen. In 2012, then head of the National Security Agency (NSA) General Keith Alexander described cyber-enabled economic espionage as "the greatest transfer of wealth in history."⁶⁹ The economic loss to the United States alone is often estimated at \$30–600 billion annually.⁷⁰

U.S. economic losses also translate directly into Chinese military advances. Su Bin, a Chinese-Canadian businessman, assisted Chinese PLA cyber officers in their efforts to steal trade secrets regarding the C-17, F-22, and F-35 aircraft. This included more than 630,000 files—totaling more than 65 gigabytes—on the C-17 aircraft. Such theft allows China to evade the costs, both in time and money, to modernize its systems. For a sense of the scale of the investments that went into the three aircraft targeted during the Su Bin case, the U.S. government spent more than \$100 billion over a period of more than three decades to modernize these airlift and fighter systems.⁷¹

The overall economic damage caused by Chinese licit, quasi-licit, and cyber collection likely far outpaces that which can be attributed to the country's HUMINT services. However, this is not to undersell the economic damage caused by HUMINT collection operations. Although not explicitly connected to the MSS, one recent U.S. conviction involved a scientist stealing trade secrets valued at \$1 billion from a U.S. petroleum company.⁷² MSS officer Xu Yanjun worked to target GE Aviation's processes for manufacturing composite jet engine fan blades, a technology that no other global company has duplicated in the more than 25 years since it was first certified by the Federal Aviation Administration.⁷³

It is also difficult to measure the impact of Chinese efforts to acquire private information about U.S. and allied decisionmaking and policy, though it is critical to assess the totality of Chinese cases rather than isolated incidents. The reason is that Chinese intelligence officers have long recognized the value of what is often referred to as the "mosaic theory" of secrecy, in which individual facts can illuminate an otherwise opaque picture when integrated into a broader body of knowledge.⁷⁴ As Huo and Wang wrote, "By picking here and there among the vast amount of public materials and

accumulating information a drop at a time, often it is possible to basically reveal the outlines of some secret intelligence, and this is particularly true in the case of the Western countries.”⁷⁵ Correspondingly, cases such as China’s successful recruitment of Candace Claiborne, a comparatively low-ranking U.S. State Department official, should be viewed merely as one piece within a broader mosaic. While Claiborne may not have operated within the inner circles of U.S. decisionmaking, her reporting on the periphery of these circles undoubtedly contributed to Beijing’s broader efforts to penetrate U.S. policy deliberations with respect to China.

There is also a subset of cases that have undermined U.S. and allied national security in ways that are difficult to measure—but are likely significant. Consider the damage associated with the 2015 OPM breach, during which Chinese cyber actors stole detailed background investigation information for nearly 20 million U.S. citizens. This data included “Social Security Numbers; residency and educational history; employment history; information about immediate family and other personal and business acquaintances; health, criminal and financial history; and other details,” as well as “findings from interviews conducted by background investigators and fingerprints” for some individuals.⁷⁶ From a HUMINT targeting perspective, the Chinese government—at a minimum—is in possession of detailed dossiers on nearly 20 million Americans who have applied for access to classified information.

Finally, there are the instances where Chinese agents have successfully penetrated U.S. intelligence agencies and gained access to government secrets, details of overseas intelligence operations, and the identities of U.S. sources in China. The first American intelligence officer charged with spying for China was Larry Wu-Tai Chin, a retired career linguist for the CIA’s Foreign Broadcast Information Service who passed classified information to Beijing for decades before his conviction in 1986. Prosecutors said of Chin at his trial, “For 30 years, he was a direct funnel from the American intelligence community to the People’s Republic of China.”⁷⁷ Two more recent cases are those of Jerry Chun Shing Lee and Alexander Yuk Ching Ma, both former CIA case officers. Ma’s case, which is still pending, includes the submission into evidence of a 2001 video recording of Ma and a colleague meeting with MSS officers and revealing CIA officer identities, human asset identities, operational tradecraft, and security communication practices.⁷⁸ Lee was convicted in a 2019 case where he was

discovered traveling with a notebook that included “CIA-related operational notes from asset meetings, operational meeting locations, operational phone numbers, true names of assets, and information about covert facilities.”⁷⁹ More broadly, China has expanded its signals intelligence collection capabilities against the United States by establishing intelligence collection facilities in Cuba, roughly 100 miles from Florida, and other locations.⁸⁰

As China’s U.S. counterparts can attest, the public often only hears about intelligence failures, not successes. Nevertheless, the cases analyzed in connection to this chapter all included notable tradecraft failures on the part of the Chinese intelligence services. One of the more amusing is that, in the closing arguments at Yanjun Xu’s trial, his defense attorneys pointed to his poor tradecraft skills as a reason to doubt the U.S. government’s contention that he was a senior MSS officer.

Some historians of Chinese intelligence have cited the country’s lack of a strong external HUMINT tradition as one of the reasons why Beijing has compensated by building a massive cyber operations capability. However, there are some types of information critical to China’s broader strategic interests that can only be pursued with human sources. Many of the cases cited in this chapter involved tradecraft that is likely unworkable in an era of heightened technical surveillance. This observation is doubly ironic given that China itself has built the world’s most advanced surveillance state. But China’s surveillance state only resolves half of the guidance from the 2,400-year-old *Methods of the Sima* noted at the beginning of this chapter. While Beijing has nearly perfected its ability to “observe the near,” the current era of HUMINT will require China’s spies to modernize how they “employ spies against the distant.” And the success of Chinese political warfare will hinge, to some degree, on how well China can improve its HUMINT capabilities.

Cyberspace has become a new pillar of economic and social development, and a new domain of national security.

- China's Military Strategy (2015)¹

CYBER OPERATIONS

网络空间是经济社会发展新支柱
和国家安全新领域。

-中国的军事战略²



In January 2021, Microsoft's John Lambert was on the edge of his seat.

It felt like “the moment before a firecracker goes off. You know something’s going to happen and you want to know: How loud is this going to be?”³ The firecracker was a massive hack of Microsoft Exchange, a product used by an estimated 1 million businesses worldwide.

The initial hack was concerning but not historic. An attacker used a curiously specific piece of data—targeted email addresses—to break into servers and steal address books, calendars, and email. Then, as Microsoft prepared to issue a patch, a second wave hit. Tom Burt, Microsoft’s corporate vice president for security and trust, said “All of a sudden we saw hundreds a day and then that continued to escalate until we were seeing north of several thousand a day. It was a very significant and noisy escalation.”⁴ Victims included local governments, police, hospitals, Covid-19 facilities, entities in the energy and transportation sector, airports, and prisons.⁵ Security researchers estimated that China breached more than 30,000 servers in the United States and hundreds of thousands worldwide. One former national security official called the attack “massive” and said, “We’re talking thousands of servers compromised per hour, globally.”⁶ A security researcher told *Wired* magazine: “China just owned the world—or at least everyone with Outlook Web Access,” the researcher said. “When was the last time someone was so bold as to just hit *everyone*?”⁷

Microsoft publicly attributed the attack to China relatively quickly. Researchers at the Microsoft Threat Intelligence Center indicated that the culprits were both known and unknown. Several known Chinese actors had been involved, along with a wide range of unknown groups apparently operating from inside China. All were using the same exploit. The attack was stunning in its scope and brazenness but was also the latest in a long line of increasingly aggressive Chinese attacks in the cyber domain.

This chapter examines China’s cyber operations, which play an important role in political warfare. As Benjamin Jensen argues, “Cyber coercive campaigns are online political warfare. They work in an indirect and additive manner to coerce rivals and signal resolve.”⁸ Since 2014, China has hacked and stolen the data of about 80 percent of Americans. In early 2014, Beijing hacked the health insurance company Anthem and then over the next year exfiltrated an estimated 78 million names, birth dates, and social security numbers.⁹ Beijing also hacked the Office of Personnel Management (OPM) in late 2014, an attack that became public in 2015, and stole 22.1 million records, including security clearance background checks. Then in 2017, Beijing hacked credit reporting agency Equifax and stole credit information for 147.9 million Americans. Between 2014 and 2018 Beijing hacked Starwood Hotels (later purchased by Marriott) and stole reservation, credit card, passport, and other travel information from an estimated 500 million people.¹⁰

This repeated collection of vast amounts of data means that Beijing knows more about Americans than Americans likely know about themselves.

Since 2014, China has hacked and stolen the data of about 80 percent of Americans.

As this chapter shows, China has developed a robust set of capabilities in the cyber domain, complete with a revamped bureaucratic structure designed to transition seamlessly between political warfare and conflict. Attacks have intensified, mirroring the “wolf warrior diplomacy” and other increasingly assertive elements of Chinese state power. Beijing’s data theft is perhaps the best known of its endeavors, but it is only one part of China’s cyber operations. The Chinese Communist Party (CCP) also uses cyber tools for intelligence collection, military operations, corporate advantage, and even personal financial gain for the operators. China almost certainly is turning a massive databank into a training field for advanced artificial intelligence/machine learning (AI/ML) systems. In addition, the Chinese government is using cyber tools to create sophisticated influence campaigns and appears poised to use cyber operations for real-world effects, including attacks that could endanger lives. China’s growing sophistication and increasing aggressiveness in its campaigns mean it can compete effectively with the United States and Russia, from penetrating defense contractors to holding critical infrastructure in the United States at risk.

However, the CCP and its cyber tools are not 10 feet tall. As Chinese offensive capabilities have improved, defenses in the United States have become more focused and have been given increased resources. Government entities such as the Cybersecurity and Infrastructure Security Agency (CISA) and the Office of the National Cyber Director (ONCD) have bolstered the security of U.S. government weak spots and raised awareness in the private sector about both the threat and the responsibility to secure one’s own systems. And China’s approach is hardly foolproof. Smoothing out the seams of the massive reorganizations within the bureaucracy from 2015 and 2018 will be challenging, just as adaptation is hard for every bureaucracy. Further, in contrast to Russia, which has hidden behind ambiguity over whether actors are criminals or state-supported or both, Beijing has been public about its attempts to

bring a sprawling group of hackers under the close control of the state. The rest of the world would be justified in putting Beijing on notice that attacks emanating from Chinese territory are at the very least presumed acceptable to Beijing.

Along these lines, this chapter seeks to explore a set of tools that function in the cyber domain to further the CCP’s larger foreign policy goals in the area of political warfare. There is crossover with other chapters—particularly those covering intelligence operations (Chapter 3), information and disinformation operations (Chapter 5), and economic coercion (Chapter 8)—because they are partially achieved using tools in the cyber domain. Examining cyber tools in its own chapter allows a thorough understanding of how China organizes itself to make the most out of use of these tools, from the bureaucratic structures in place to the decisions about how to focus efforts and deploy resources.

Offensive cyber tools are programs designed to identify and exploit a vulnerability in an adversary’s networks, leading to the ability to map a network, find and extract data, damage computer systems, or potentially cause a system managed by a vulnerable network to function inappropriately, causing death or damage. Offensive cyber tools can establish a persistent presence for a wide range of uses, from information gathering to potential kinetic operations. Along that spectrum lie acts of cyber sabotage and eventually cyber warfare, which could include destruction of property or deaths of personnel. This chapter draws on Chinese strategy documents and military academic work to explore how Beijing approaches offensive cyber operations, nesting that activity under China’s larger strategy of “information warfare.”

The rest of this chapter is divided into the following sections. It reviews the creation and development of China’s cyber capability, maps the agencies and main actors responsible for China’s cyber program, and establishes China’s goals for its cyber program. Finally, it discusses the implications of China’s increasing skill set in cyber operations.

CYBER OPERATIONS: A KEY ELEMENT OF INFORMATION WARFARE

Chinese doctrine views cyber operations as a core element of information warfare. The father of Chinese information warfare, Major General Wang Pufeng, summarized how information

has become central to all aspects of warfighting in his seminal 1995 work *Information Warfare and the Revolution in Military Affairs*. He wrote: “Information war is a crucial stage of high-tech war. . . . At its heart are information technologies, fusing intelligence war, strategic war, electronic war, guided missile war, a war of ‘motorization’ [jidong zhan], a war of firepower [huoli]—a total war. It is a new type of warfare.”¹¹ Twenty years later, China’s 2015 Military Strategy spelled out the role of computer network operations, calling it a “new pillar of economic and social development” and a “new domain of national security.”

网络空间是经济社会发展新支柱和国家安全新领域。网络空间国际战略竞争日趋激烈，不少国家都在发展网络空间军事力量。中国是黑客攻击最大的受害国之一，网络基础设施安全面临严峻威胁，网络空间对军事安全影响逐步上升。加快网络空间力量建设，提高网络空间态势感知、网络防御、支援国家网络空间斗争和参与国际合作的能力，遏控网络空间重大危机，保障国家网络与信息安全，维护国家安全和社会稳定。¹²

[Cyberspace has become a new pillar of economic and social development, and a new domain of national security. As international strategic competition in cyberspace has been turning increasingly fierce, quite a few countries are developing their cyber military forces. Being one of the major victims of hacker attacks, China is confronted with grave security threats to its cyber infrastructure. As cyberspace weighs more in military security, China will expedite the development of a cyber force, and enhance its capabilities of cyberspace situation awareness, cyber defense, support for the country’s endeavors in cyberspace and participation in international cyber cooperation, so as to stem major cyber crises, ensure national network and information security, and maintain national security and social stability.]¹³

China’s strategy for information warfare developed over decades, and to implement this vision, China has established a robust cyber capability, both in-house in the security services and on a contract or volunteer basis.

THE EVOLUTION OF CHINA’S CYBER CAPABILITIES

China’s cyber program started as most others, with a group of cutting-edge hackers in a small community testing out new talents and capabilities

as a side job or a hobby. In May 1999, the United States became a major target. In retaliation for the United States’ accidental bombing of the Chinese embassy in Belgrade, “patriotic hackers” defaced U.S. government websites with messages denouncing the North American Treaty Organization.¹⁴ Then in August 1999, Chinese private hackers targeted 10 Taiwanese government pages and left statements saying, “There is only one China in the world and the world only needs one China.”¹⁵

Military and civilian organizations grew over time, and by the early 2010s, China was a robust and increasingly sophisticated cyber power. U.S. cybersecurity firms began to uncover the scope of Chinese activity. Between 2013 and early 2016, leading cybersecurity firm Mandiant tracked at least 72 civilian, military, and ostensibly private Chinese cyber organizations operating on the world stage.¹⁶ Another firm, CrowdStrike, evaluated China’s cyber posture in its 2015 Global Threat Report. It found 28 Chinese cyber groups pursuing defense and law enforcement targets and many other groups attacking targets in energy, transportation, government, technology, healthcare, finance, telecommunications, media, manufacturing, and agriculture.¹⁷ One such unit was People’s Liberation Army (PLA) operated Unit 61398, which has reportedly stolen terabytes of data from organizations worldwide since 2006.¹⁸ Mandiant identified 141 companies targeted by Unit 61398, of which 115 were in the United States.

By 2014, Chinese cyber activity had become widespread, aggressive, and noisy, likely in part because of the sheer number of actors engaging in cyber activity with unclear deconfliction and organization. China had three departments overseeing cyber activities: the PLA, which operated 12 specialized operation bureaus; Technical Reconnaissance Bureaus (TRB) for each military region; and the Ministry of State Security (MSS).

While the exact reasons for the timing are unclear, 2015 became a watershed moment for China’s cyber capabilities. Beijing appears to have decided that its cyber efforts needed better coordination and centralized control, and it embarked on a massive reorganization of its military cyber units. These efforts were likely built from Xi Jinping’s reforms launched in 2012, when he became general secretary of the CCP. At the 18th Central Committee meeting that same year, Xi told the Third Plenary that “in the face of the rapid development of Internet technology and applications, the current management system has obvious drawbacks, such as multi-management, overlapping functions,

inconsistent powers and responsibilities, and efficiency.”¹⁹ A Xinhua article at the time compared the organization of China’s cyber operations to “water control at Kowloon,” suggesting uncontrolled growth and lack of organization, with a degree of improvisation.²⁰

Some commentators have suggested that a summit between President Obama and President Xi in 2015 was a turning point. The United States had been increasingly vocal about its impatience with Chinese intellectual property (IP) and other data theft and had been increasing diplomatic pressure. That diplomacy culminated in a summit in Washington, D.C., in September 2015. At the summit, both powers agreed not to conduct economically motivated cyber espionage—a subset of China’s collection, but a large one. At the press conference announcing the agreement, Xi said, “China strongly opposes and combats the theft of commercial secrets and other kinds of hacking attacks.”²¹

Little evidence exists that the summit was causal. Given the timing of the rollout of a complicated reorganization in December, just a few months later, it was more likely the CCP had already planned the policy shift and used the summit as a way to win diplomatic points for a decision that was already made. Within a year of the summit, serious doubts had emerged about whether China had slowed down its cyber espionage activity, or whether it had in fact refocused its efforts. As a Council on Foreign Relations analysis concluded in 2016, Chinese entities “may be becoming more stealthy and sophisticated in their attacks,” noting that Assistant Attorney General John Carlin said China had reduced the volume of attacks but had become more focused and calculated.²² Leading cybersecurity researchers published papers reporting that the volume of Chinese cyberattacks on the United States had lessened, but espionage continued in particular strategically significant sectors.

THE GREAT REFOCUSING: THE CREATION OF THE PLA STRATEGIC SUPPORT FORCE

China’s 2015 Military Strategy laid out a clear goal: “China will expedite the development of a cyber force and enhance its capabilities of cyberspace situation awareness, cyber defense, [and] support for the country’s endeavors in cyberspace.”²³ In 2015, to further that goal, the PLA moved cyber capabilities from widely scattered and loosely coordinated forces into a largely coherent, centralized group within a new organization: the Strategic Support Force (SSF). SSF was created to prepare China for twenty-first century warfare, uniting most of the PLA’s cyber,

space, electromagnetic, and psychological warfare capabilities under one chain of command.²⁴ The SSF seeks to disrupt an adversary’s capabilities to conduct warfare, in particular by sabotaging command systems—or systems of systems—in the early stages of a conflict. Further, it seeks to create a nearly seamless transition to a war footing by creating permanent operational groups.²⁵

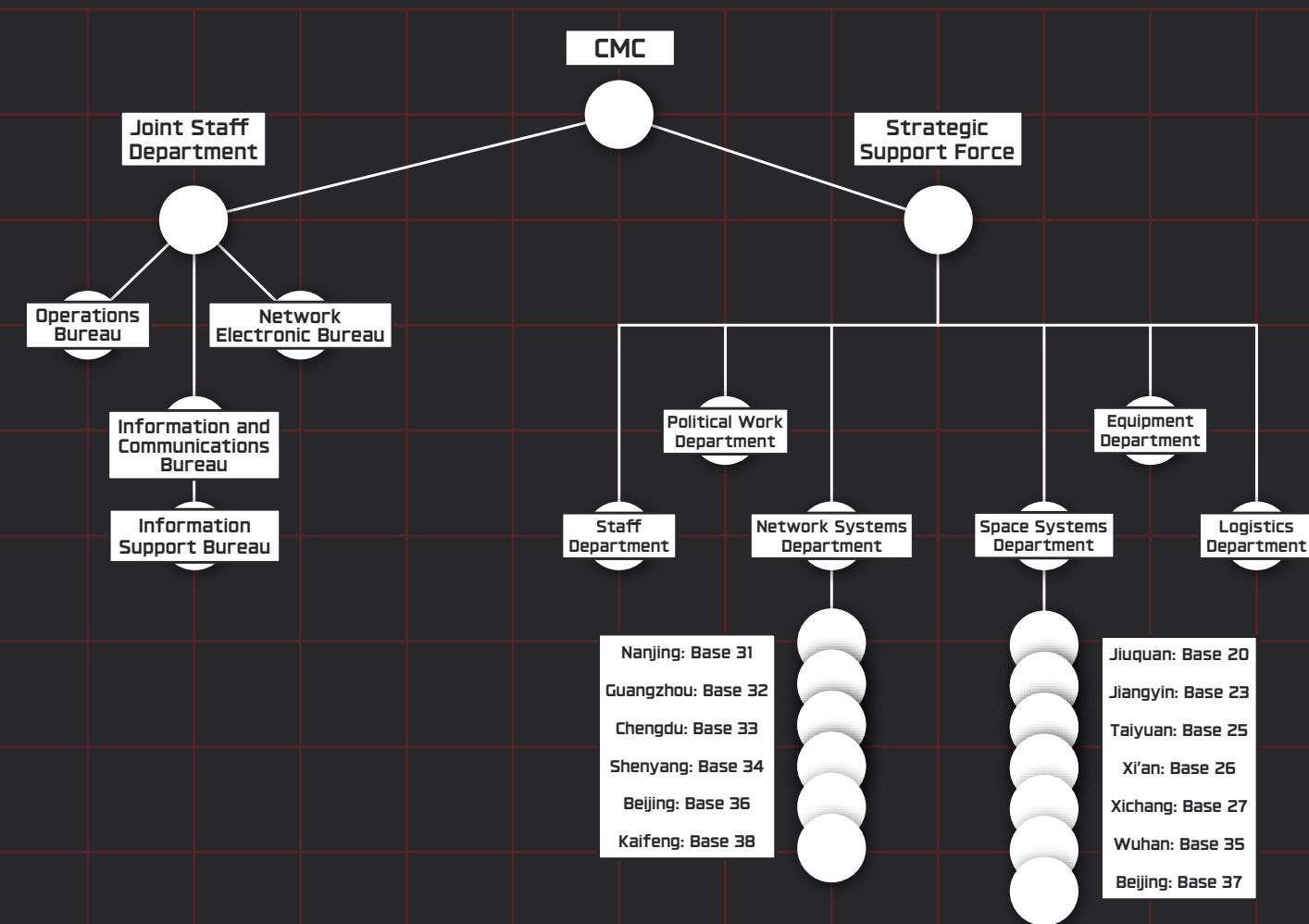
Within the SSF, the Network Systems Department (NSD) oversees cyber and information warfare.²⁶ The reorganization pursued a “bricks, not clay” approach, which means that units were generally kept whole as the bigger structures were deconstructed and rearranged.²⁷ For example, PLA Unit 69010 pre-2015 was the Lanzhou Military Region’s second TRB. In the reorganization, it was reassigned largely intact to the SSF NSD.²⁸

After 2015, Mandiant described a much more targeted effort by Chinese cyber entities associated with the PLA. They assessed that the focus for many Chinese actors shifted from IP theft to strategic intelligence collection and the establishment of persistent accesses for potential future use.²⁹ The number of actors decreased precipitously as well. Mandiant reported in 2016 that they had seen a dramatic drop in cyber espionage from 72 suspected China-based groups. Mandiant researchers cited several factors, “including President Xi’s military and political initiatives, the widespread exposure of Chinese cyberoperations, and mounting pressure from the U.S. Government.”³⁰ Similarly, the Institute for Critical Infrastructure Technology hypothesized that China was attempting to control its operatives and better focus its efforts.³¹

A U.S. Department of Justice (DOJ) indictment five years later laid out what the Federal Bureau of Investigation (FBI) saw as the main targets of MSS-affiliated actors, which reflect this narrower focus on strategic topics: high-tech manufacturing; medical device, civil, and industrial engineering; business, educational, and gaming software; solar energy; pharmaceuticals; and defense. One DOJ indictment charges the defendants with conspiring to steal trade secrets, including “technology designs, manufacturing processes, test mechanisms and results, source code, and pharmaceutical chemical structures.”³³ There is a clear selection bias in this kind of data collection. The U.S. government only knows about the activity it has found, or that victims have reported, and such reporting is highly inconsistent. Further, the publicly available data are from only those cases the DOJ felt it had the evidence to pursue.

Figure 4.1

Organization of PLA Joint Staff Department Cyber Warfare Capabilities and PLA Strategic Support Force



SOURCE: CSIS RESEARCH AND ANALYSIS.

However, the conjunction of a reorganization of China's cyber activity and a seemingly narrower scope of targets can logically be seen as more than a coincidence.

THE MINISTRY OF STATE SECURITY'S EVOLUTION

While the SSF looms large in China's cyber posture, the MSS has a robust set of activities at least partially focused on the United States. Civil-military cyber integration is a core tenet of the Central Commission for Integrated Military and Civilian Development, which was created in January 2017.³⁴

The MSS undertook its own reorganization in 2018 to better focus its activities.³⁵ As of 2022, the U.S.-China Economic and Security Review Commission reported that the MSS "conducts most

[of China's] global cyberespionage operations and targets political, economic, and personally identifiable information to achieve China's strategic objectives."³⁶ Indeed, the MSS was almost certainly responsible for the Microsoft Exchange hack detailed at the beginning of this chapter. Microsoft dubbed that threat group "HAFNIUM."³⁷ Recorded Future named MSS as the actor behind APT3/GOTHIC PANDA in 2017, and CrowdStrike pointed to the MSS as the actor behind APT10/STONE PANDA in 2018.³⁸ GOthic PANDA pursued a variety of technology and other targets in the United States until 2015, then shifted its focus to Hong Kong in 2016, likely in advance of Hong Kong's elections.³⁹ GOthic PANDA was also likely involved in the 2018 attack on the Winter Games in South Korea.⁴⁰ STONE PANDA has been responsible for

attacks on managed service providers and their customers to secure IP and confidential business data, including in Brazil, Canada, Sweden, India, Switzerland, Finland, Japan, Germany, France, the United Arab Emirates, the United Kingdom, and the United States.⁴¹

The MSS also oversees two civilian agencies: the China Institutes of Contemporary International Relations and the China Information Technology Security Evaluation Center. The former ostensibly acts as a think tank, carrying out track 1.5 dialogues and engaging in discussions about cyber norms with European and U.S. think tanks. The latter collects information about vulnerabilities in software and hardware products, which it likely passes along to the MSS.⁴²

Another civilian agency, the Cyberspace Administration of China (CAC), is the central internet regulator and primary control, oversight, and censor agency of the country. While the relationship between the MSS and CAC is not clear from publicly available documents, they likely at least share information.⁴³ In October 2017, the CAC released a key policy document highlighting the CCP's perspectives on cyberspace ahead of the National Congress. The document included a directive to "promote the deepened development of military-civilian integration for cybersecurity and informatization," which prompted the PLA to strengthen its partnerships with the civilian sector, notably giants such as Huawei and ZTE.⁴⁴ Following the 2018 round of governmental reform, the CAC was elevated to the Office of the Central Cyberspace Affairs Commission.⁴⁵

THE IMPORTANT ROLE OF PRIVATE AND SEMI-PRIVATE ORGANIZATIONS

China has a further, expansive set of ostensibly private or semi-private organizations working on the cybersecurity mission. For example, the National Cybersecurity Center (NCC), formerly the National Cybersecurity Talent and Innovation Base, lies at the heart of realizing China's ambition to become a cyber powerhouse. The new center has been under construction since 2017 in Wuhan and houses multiple research and talent centers, laboratories, and an operational national cybersecurity school.⁴⁶ The NCC's two non-private laboratories, the Combined Cybersecurity Research Institute and the Offense-Defense Lab, both perform cybersecurity research for the Chinese government. Under civil-military fusion, the NCC has established links to the PLA so that the military can harness the new research and tools being developed in their asymmetric operations.

Another example is the Central Commission for Integrated Military and Civilian Development, which was established in December 2017. The center, which currently operates within one of China's premier cybersecurity companies, 360 Enterprise Security Group, is charged with enhancing private sector cooperation to help ensure the military wins future cyber wars.⁴⁷ Other examples of national agencies include the China National Cyber Threat Intelligence Collaboration (CNTIC), established in 2017 by government agencies and leading cybersecurity companies, and the National Computer Network Emergency Response Technical Team, which supports the CNTIC. Both are defensively oriented, with a mission to collect cyber threat data, analyze it, and share it among national elements.⁴⁸

Both the CCP's military and civilian agencies are likely to employ a large hacking community to conduct offensive cyber operations. Before the 2015 reorganization, one theory of China's cyber activity suggested intelligence officers loosely oversaw an unstructured cluster of patriotic hackers.⁴⁹ Since these groups could undermine the more political objectives of regular PLA cyber units if allowed to operate unrestrained, they were likely tasked with surveillance and espionage only rather than offensive cyber operations that would target critical infrastructure or cause physical damage.⁵⁰

In addition to state-affiliated hackers, a group of cyber volunteers called "hacktivists" operates independently. These web-based communities are layered by several interest groups, such as malware tool developers, legitimate security researchers, and novices seeking training.⁵¹ These groups have engaged in large-scale politically motivated denial-of-service attacks, web defacement of foreign networks, and data destruction—activities that fall under "hacktivism."

The MSS continues to empower its hacker community by hiring them as contractors to launch offensive cyber activities against foreign actors—including the United States—to steal trade secrets and exfiltrate data.⁵² DOJ indictments link the MSS to private contractors for cyber espionage activity.⁵³ For example, one such indictment alleges that Ding Xiaoyang, Chen Qingmin, and Zhu Yunmin were Hainan State Security Department officers "responsible for coordinating, facilitating, and managing hackers at MSS front companies."⁵⁴ In 2007 and 2008, the First Research Institute of the Ministry of Public Security (MPS), which supports the operational elements of the MPS, posted infor-

mation security and programming job vacancies on EvilOctal.com and XFOfocus.net, two of the largest and most established hacker communities in China.⁵⁵ This action demonstrates the government's efforts to recruit from the hacker community and likely build consulting relationships. The founding member of Chinese hacker group Javaphile, who led attacks on the White House in 2001, maintains a formal consulting relationship with the Shanghai Public Security Bureau and also possesses researcher credentials at the information security engineering institute of a leading Chinese university.⁵⁶ As the U.S.-China Commission reported:

China's cybersecurity legislation weaponizes the country's cybersecurity industry and research by requiring companies and researchers to submit all discovered software and hardware vulnerabilities to the government before providing them to the vendors that can patch them. This policy, leveraged in combination with domestic hacking competitions and cooperative agreements with Chinese universities, provides China's security services with a steady stream of vulnerabilities to exploit for state-sponsored operations.⁵⁷

In addition to the same evolution that most nation-state cyber efforts experienced from the 1990s through today, China's cyber structures have undergone rapid and comprehensive reform in two bouts, in 2015 and 2018. As of 2023, the rapid reform efforts seem to have concluded, leaving the hard work of creating new internal norms, sharing practices, and developing bureaucratic fixes to new processes. While any new bureaucracy takes time to form and smooth out practices across new silos, it is likely that these reforms will largely accomplish the intended goal of centralizing decisionmaking and gaining stronger command and control over cyber efforts, given the new decisionmaking structures.⁵⁸

THE GOALS OF OFFENSIVE CYBER OPERATIONS

Chinese actors pursue activity in the cyber domain for three main reasons. The first is to steal secrets about adversary intent or capability. The second reason is to establish access points for disruption or pre-positioned destructive tools for conflict contingencies. The third reason is to help Chinese businesses leapfrog their Western competition or to enable personal financial gain. To identify these three main goals and assess the weight of each line of effort, CSIS researchers created a dataset

of Chinese cyber operations from 2010 to 2022, examining 49 major incidents that were publicly reported and credibly attributed to the Chinese government. While the data is imperfect—some incidents reported as one campaign had several sub-components, and other incidents have imprecise details—there are some preliminary trends:

- Twelve of the major attacks were directed at a government entity, including several U.S. state governments in 2022;
- An estimated 12 of these incidents involved an attack on a defense entity, including the U.S. Navy and aerospace contractors in 2018;
- Eight were upstream attacks where hackers breached a service provider that would in turn provide access to other potential targets. For example, one attack encompassed hacks of 13 telecom networks beginning in 2016;
- In more than half of the incidents, Chinese actors sought to steal industrial secrets, IP, or sensitive government data; and
- At least three of the attacks could be characterized as operational preparation of the environment, where the Chinese hackers sought vulnerabilities in U.S. and Australian government systems and in oil and gas infrastructure.

The limited dataset makes drawing conclusions about trend lines in types of attacks risky, but the variety of targets is noteworthy, as is the focus on stealing information. One cluster is worth highlighting: a series of attacks on defense contractors in 2018 and 2019, corresponding with MSS reorganization. This cluster of attacks suggests that a concerted effort to go after defense secrets corresponded with a refocusing of MSS activities in the reorganization.

Each of these reasons could encompass potentially dangerous and escalatory activity, but they are well in line with what other nations attempt. Under the goal of espionage, the hallmark of Chinese activity is the quantity of data stolen and the diversity of the target set. This practice reveals a secondary strategic goal: a likely attempt to create and train a world-class AI/ML capability. The most worrisome of the three goals is China's ability to create kinetic effects, including potential destruction of critical infrastructure, a problem set discussed below in more detail. The next section explores each of the three goals in more depth: espionage, operations, and financial motivations.

CYBER TOOLS FOR ESPIONAGE

Like most nation-states, China has worked to create a cyber operations capability to collect information on its adversaries. Those activities include normal nation-state goals, such as attempting to discern intentions. For example, in 2008 entities linked to the Chinese government broke into the campaigns of both Senator John McCain and Senator Barack Obama to gain insight into each potential administration's China policy.⁵⁹ One item apparently stolen was a draft letter from McCain to the newly elected president of Taiwan, in which McCain pledged his support for the U.S.-Taiwan relationship. But before the McCain staff finalized the letter, the Chinese embassy called to complain. Randall Scriver, then serving as a McCain campaign aide, was thoroughly surprised by the call. He said, "It certainly struck me as odd that they would be so well-informed."⁶⁰

Beijing's efforts have spanned political and military targets, with a focus on defense contractors. China attempted to break into TRANSCOM systems about 50 times between 2012 and 2013, with 20 of those attacks successful. A Senate Armed Services Committee investigation found that TRANSCOM was only aware of two of those intrusions.⁶¹ From 2007 to 2009, Chinese hackers broke into defense contractors responsible for building the F-35 fighter and stole information about the design and electronics systems. At the same time, attackers accessed the U.S. Air Force's air traffic control system, which showed the locations of U.S. military aircraft in flight.⁶² In early 2018, a Naval Undersea Warfare Centre contractor lost signals and sensor data, cryptographic information related to communications, and the submarine development unit's electronic warfare library.⁶³ Two China-linked advanced persistent threats (APTs) even targeted universities engaged in naval research with military applications.⁶⁴

Beijing has also worked to develop a robust offensive counterintelligence capability for both tactical and strategic purposes, some of which is discussed in Chapter 3. In advance of a Chinese official's visit to an unnamed country, an APT stole local call records and the guest list at his hotel, suggesting a security sweep.⁶⁵ On a strategic level, the massive data breaches of OPM in 2015, in which the data of an estimated 22.1 million people was stolen, and Starwood/Marriott hotels, in which the data of an estimated 500 million

guests was stolen, might show which Americans with security clearances travelled where and when, potentially exposing sensitive military or intelligence operations.⁶⁶

OPERATIONAL PREPARATION OF THE ENVIRONMENT

An eye-popping headline about a massive breach makes the operation seem sudden, but computer network operations usually require months of preparation. Operators must research vulnerabilities, create a tool, find a way into the target, and map the target's network, all before data extraction or kinetic effects. As a result, China has put significant effort into operational preparation of the environment (OPE): identifying vulnerabilities and establishing access points for future exploitation.

In a prominent Chinese defense journal, *Guofang Keji*, scholars highlighted the importance of this kind of reconnaissance:

Cyberspace reconnaissance operations are mission behaviors to obtain information about opponents or potential opponents' cyberspace operations and network resources. The network information of reconnaissance is the prerequisite basis for all cyber combat operations and can also be used to verify current intelligence or predictions.⁶⁷

The authors describe two types of attacks. The first is "information utilization," or "soft kill" attacks; the second is "high-precision physical destruction of hardware," such as information technology infrastructure. These forms of attack have the benefits of "remote control, flexible maneuverability, strong destructive power, and small collateral damage. It is also a basic means of network warfare."⁶⁸ OPE is necessary for precision and effectiveness in both types of attack.⁶⁹

The danger of OPE, however, is that the tactics, tools, and procedures look similar—if not identical—to activity designed to destroy or disable an adversary's capabilities. As a result, the target may not be able to tell whether the activity is designed to steal information or cause destruction. The escalatory implications of this dynamic have yet to be tested in a real-world, high-tension situation. However, Chinese scholars have identified the potential for problems: "Active cyber reconnaissance can mislead opponents into believing that cyber combat operations have begun, prompting them to be exposed as soon as possible, so as to achieve better reconnaissance results. Therefore, the cyber reconnaissance capability is the primary

core capability of the cyberspace support force construction.”⁷⁰ They seem to suggest this activity is not to be taken lightly, which may help Western nations to persuade Beijing to adopt international norms about state behavior. China’s OPE includes recruiting routers and networks for potential future operations. In October, the National Security Agency (NSA), CISA, and the FBI issued a cybersecurity advisory warning:

Chinese hacking groups have exploited publicly known vulnerabilities to breach anything from unpatched small office/home office (SOHO) routers to medium and even large enterprise networks. Once compromised, the threat actors used the devices as part of their own attack infrastructure as command-and-control servers and proxy systems they could use to breach more networks.⁷¹

Similarly, considerable amounts of Chinese cyber activities have been devoted to penetrating telecoms. These access points are force multipliers for intelligence services because an upstream attack on a telecommunications company can provide access to a host of additional targets—including all the customers of that telecommunications company. A researcher at Michigan State University found that penetrating the telecommunication sector had become the number one Chinese cyber espionage focus as of 2021, above even government targets. He wrote: “The versatility offered by telecommunications targeting combined with the more efficient and stealthier methods used is believed to indicate a higher level of maturity among active Chinese APTs.”⁷² In 2022, Chinese hackers went after Middle Eastern telecoms, using keylogger and PowerShell scripts designed to gather email content.⁷³ The threat group, known as BackDoorDiplomacy, had been targeting diplomatic entities and telecommunications companies in Africa and the Middle East since at least 2017—an apparent shift from its early government-focused efforts starting in 2010.⁷⁴ A joint cybersecurity advisory in June 2022 from NSA, CISA, and the FBI outlined how Chinese actors compromise major telecommunications companies and network service providers, noting “they establish a broad network of compromised infrastructure [and] use the network to exploit a wide variety of targets worldwide.”⁷⁵ As another assessment concludes, “Telecommunication firms are extremely high-value targets for intelligence agencies. . . . Successfully hacking them can mean opening doors to an even bigger world of prized spying opportunities.”⁷⁶

AI TRAINING

After China’s first big data breaches, some commentators wondered how it might make so much data usable. William Evanina, former director of the U.S. National Counterintelligence and Security Center, described China as “shop-vac oriented,” referring to the vast quantities of apparently non-differentiated information pulled into Beijing’s control between 2015 and 2018. The leading theory among security researchers on the purpose of that data collection effort is based on China’s stated intent to create a world-leading AI/ML capability. Data holdings from these entities were probably already structured, making it easier to use them to train AI algorithms. Further, U.S. data sets are likely more diverse than Chinese data sets, making them much better training data for AI/ML systems. The Anthem hack, which gave Beijing 78 million customer records, likely provided useful information on medical conditions and treatment plans that could further China’s biotech and pharmacological efforts.⁷⁷ These data sets have the added benefit of providing insight potentially useful for future influence operations. In another example, TikTok’s data-gathering capability reveals what media Americans find most engaging and what kinds of messages are most effective, which enables China to develop compelling messages that serve China’s larger interests.⁷⁸ TikTok, which is also discussed in Chapter 5, could be both an effective research tool and an efficient delivery mechanism for messages promoting China’s view of state surveillance and Taiwan as part of China.⁷⁹

CYBER TOOLS FOR OPERATIONS: INFORMATION OPERATIONS, DISRUPTION, AND KINETIC EFFECTS

The cyber domain has proven fruitful for collecting information and for conducting a range of other operations, from creating access for information operations to disrupting adversary plans and causing physical damage. China has become a premier player in information operations, in line with their stated strategies, and cyber tools have facilitated some of those propaganda campaigns. Cyber operations can also harass or disrupt an adversary—increasing friction of decisionmaking in a crisis, making communication challenging, or blocking access to important data. Finally, cyber operations can cause physical harm, for example, if a cyber tool is used to break equipment, cause a fire, or take a hospital offline.

This section explores this set of operations and what is known about Chinese capabilities. The broader goals and capabilities in the information operations space are discussed in Chapter 5, but this section deals with cyber operations that create accesses or collect information that can later be used to shape ideas.

CYBER OPERATIONS TO ENABLE INFORMATION OPERATIONS: ACCESS TO MEDIA AND ELECTION SYSTEMS

Information operations contain a broad bucket of activity, including efforts to shape an adversary's view of a conflict or potential conflict or efforts to weaken an adversary from within. Information operations take place in multiple ways with many tools, but increasingly they are executed in the cyber domain through social media or using tools such as deepfakes. This section briefly touches on using the cyber domain not just for spreading information payloads but for accessing force multipliers for information operations.

Cyber actors seek unauthorized access to websites, media outlets, or election systems in order to spread information payloads seemingly from inside the system or to disrupt operations. For example, China's first recorded cyber operation against the United States was an information operation: the 1999 defacement of U.S. government websites with messages denouncing NATO in retaliation for the United States' accidental bombing of the Chinese embassy in Belgrade.⁸⁰

Beijing is increasing its attacks on the media and entertainment sector, with an estimated 75 percent of China's media targets based in the Asia-Pacific.⁸¹ In 2013, Beijing-linked hackers retaliated against the *New York Times* and *Wall Street Journal* after both newspapers published articles alleging that the Chinese prime minister's family had accumulated tremendous wealth.⁸² Nearly a decade later, Mandiant uncovered that hackers linked to the Chinese government had compromised email accounts at the *Wall Street Journal* and maintained a presence on their systems for at least two years, from 2020 to 2022.⁸³

While election influence is attempting to influence voters' minds to vote a certain way, or not to vote at all, interference is an attempt to disrupt the election systems themselves. This disruption can occur by deleting voter information so that voters cannot check in at a polling station or spreading misinformation about where, when, or how to vote in order to prevent people from

voting. In 2022, China conducted operations that may have been aimed at election interference. China exploited the "log4j" vulnerability—a critical flaw in a widely used logging tool—and zero-day vulnerabilities to gain access to at least six state governments, and probably more.⁸⁴ One ingress route was through an application called USAHerds, which U.S. states use to detect and track livestock disease outbreaks.⁸⁵ China has previously also shown interest in stealing IP related to U.S. agriculture, suggesting cyber operators may have used an older access point to pivot to a new use—election interference.⁸⁶ Separately, NSA issued a warning in 2022 that Chinese hackers scanned more than 100 state-level political party domains "likely so the PRC cyber actor could build a target network for possible future operations."⁸⁷

DISRUPTION AND KINETIC EFFECTS

While it does not appear that China has attempted kinetic operations in the cyber domain, Chinese military theory acknowledges the possibility. The Chinese military has also endeavored to find gaps in the defenses of critical infrastructure. Writing in *Guofang Keji*, several Chinese military scholars noted:

The physical level requires the realization of the vertical and horizontal connection and integration of various combat units and combat elements, unified command, unified control and unified coordination. The information level requires the controllability, sharing, and robustness of command information. The above-mentioned command and control capabilities play a decisive role in the control of cyberspace and the success or failure of operations, so they have become one of the core capabilities of cyberspace combat power construction.⁸⁸

FBI and CISA have warned of long-standing Chinese efforts to identify gaps in the security of critical infrastructure such as oil and gas systems. CISA recently revealed details about Chinese attacks on oil and gas companies from 2011 to 2013. China has targeted at least 23 natural gas pipelines with spearphishing emails. Of these, 13 were confirmed compromises, 3 were "near misses," and 8 intrusions were successful but of unknown severity. FBI and CISA assessed that Chinese government actors were seeking the ability to hold pipeline infrastructure at risk in order to potentially physically damage pipelines or disrupt operations.⁸⁹ Mandiant confirmed that this line of effort is a persistent one for Beijing. Multiple threat actors tied to China have targeted industrial control systems (ICSs), including "an energy company, multiple natural gas pipeline

companies, an ICS equipment manufacturer, and an ICS security firm.”⁹⁰ Mandiant also identified the “Pulse Attacks,” which exploited a weakness in a software system called Pulse Secure, which allows people to work remotely. Chinese entities used the vulnerability to target the U.S. government and critical infrastructure, including the country’s largest water agency, the New York City subway system, and Verizon. A security researcher called it a targeted attack against a few dozen networks that all have national significance in one way or another.⁹¹

Access to critical infrastructure systems is one thing; use of that access is another. China’s intentions are still unclear. China may be exploring vulnerabilities to identify what kind of disruptive effects are possible, or it could hope for a deterrent effect, betting that the U.S. government will identify the activity. It could also be collecting accesses as OPE or contingency plans in case of conflict. The ODNI in its 2021 annual threat assessment warned that China can, “at a minimum” bring “temporary and localized” disruptions to U.S. critical infrastructure through cyberattacks.⁹² In 2022, the annual threat assessment went even further, saying “China almost certainly is capable of launching cyberattacks that would disrupt critical infrastructure services within the United States, including against oil and gas pipelines and rail systems.”⁹³ Both were silent on intentions.

CYBER TOOLS FOR FINANCIAL GAIN

The Chinese government approaches public-private partnerships in a far different way than most Western governments. Beijing can and does compel businesses to cooperate with state priorities whether or not the outcome is helpful to the company’s bottom line. Beijing has also used state resources to advance the business interests of purportedly private entities. Cyber operations have long played a role in China’s larger strategy of IP theft to leap ahead of competitors. According to at least one assessment, China has stolen more secrets from businesses and governments than any other country.⁹⁴ In 2011, China breached the U.S. Chamber of Commerce to such an extent that even the thermostats were communicating with a computer in China and a printer began printing in Chinese.⁹⁵ In 2012, General Keith Alexander, then head of NSA, described cyber-enabled economic espionage as “the greatest transfer of wealth in history.”⁹⁶ The economic loss to the United States alone is often estimated at \$30–600 billion annu-

ally.⁹⁷ Industrial and economic espionage tends to track with China’s five-year economic development plans.⁹⁸ The Institute for Critical Infrastructure Technology assessed that “most of the technology needed to realize the 13th five-year plan will likely be acquired by stealing trade secrets from companies in other countries.”⁹⁹

The FBI has been working to raise public awareness about this threat and to encourage businesses to better secure their systems. In 2018, then deputy attorney general Rod Rosenstein said, “More than 90 percent of the department’s cases alleging economic espionage over the past seven years involve China [and] more than two-thirds of the department’s cases involving thefts of trade secrets are connected to China.”¹⁰⁰ Rosenstein explicitly tied several of these crimes back to the MSS.¹⁰¹

Large-scale industrial hacking for research and development helps Chinese industry, but individual or small groups of hackers also moonlight for their own personal financial gain. China’s cadres of contractor hackers have been known to pursue both goals. For example, APT41, also known as BARIUM or WICKED PANDA, has used the same malware for espionage and also for financially motivated activity, largely directed at the video game industry. Mandiant wrote in their groundbreaking paper on APT41 that while purely financial goals are unusual among Chinese state-sponsored groups, “evidence suggests APT41 has conducted simultaneous cyber crime and cyber espionage operations from 2014 onward.”¹⁰² The DOJ indicted seven alleged members of APT41 in 2020 and tied them to a contractor known as Chengdu 404, who has worked for the MSS. The DOJ cited espionage on behalf of the MSS and cybercrime in the indictment.¹⁰³ While little information exists on the extent to which government authorities condone or support such activity, condemnation by the government would almost certainly result in cessation of the activity.

ATTRIBUTION

Establishing clear standards for attribution, along with confidence levels for those standards, will be important for reacting to Chinese cyber activity quickly. Standards for attribution are different in the private sector than in the intelligence community, resulting in an occasional mismatch where a private researcher attempting to make headlines is willing to be forward leaning in an assessment, but the intelligence community disagrees or expresses uncertainty. That mismatch

can make the U.S. government look indecisive and vulnerable. Policymakers should fully understand the intelligence community's attribution standards and be ready to publicly explain their posture regarding investigating an attack. They should also be prepared to act in the face of some uncertainty. Perfect knowledge is an unrealistic standard in war and intelligence work, and the cyber domain is no different.

Mandiant's 2013 report *APT1: Exposing One of China's Cyber Espionage Units* was one of the first and still most high-profile cases of public attribution of a cyberattack to the Chinese government. The report traced APT1's activity back to Shanghai and identified the group as the Second Bureau of the PLA General Staff Department's Third Department, also known as Unit 61398.¹⁰⁴ A year later, the DOJ indicted five Chinese army officials for engaging in the economic espionage exposed in the Mandiant report.¹⁰⁵

Indictments are rare in comparison to the scope of Chinese hacking activity, but DOJ has pursued charges several times in the last five years. In 2021, the United States charged four Chinese nationals in a global hacking campaign that targeted dozens of U.S. companies, universities, and government agencies in the United States and abroad. In December 2018, the DOJ indicted two Chinese hackers from the MSS-affiliated group APT10, who infiltrated U.S. Navy contractors' systems to steal ship maintenance data and missile plans.¹⁰⁶ Earlier the same year, the DOJ indicted MSS officers and hackers who had conspired over several years to steal commercial aviation and technological data from the United States.¹⁰⁷

In cases where the CCP has responded to public attribution of cyberattacks, there has always been strict denial and often condemnation of what the CCP describes as efforts to intentionally tarnish China's reputation. In 2013, the Obama administration publicly and directly accused China's military of conducting cyber operations against U.S. defense contractors and network systems. The Pentagon's annual report to Congress stated, "computer systems . . . owned by the U.S. government continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military."¹⁰⁸ In response, the CCP condemned the report, instead claiming that China is against all forms of cyberattacks and is open to conversing with the United States on internet security. After a Chinese threat actor was suspected of infiltrating the networks of Afghan telecommunications providers in 2020 and 2021,

a Chinese embassy spokesperson said, "Linking cyber attacks directly to one certain government is a highly sensitive political issue. China hopes that relevant parties will adopt a professional and responsible attitude."¹⁰⁹ Xinhua News Agency, China's official state news agency, described the West's attributions as slander and instead argued that "the United States, posing a grave threat to global cybersecurity, is commanding the allies it spies on to slander China."¹¹⁰

CONCLUSION

In 2018, CrowdStrike declared that China surpassed Russia as the most prolific nation-state mounting attacks on Western entities.¹¹¹ At the time, China was shifting its targets from largely commercial secrets to strategically targeted collection.¹¹² Since 2018, Beijing has cemented its cyber strategy, developed its capabilities, and cultivated a certain boldness in its operations that reflects its larger posture toward the world and increased use of political warfare. As highlighted in Chapter 8, projects such as the Digital Silk Road have embedded Chinese communications equipment in systems around the globe, potentially making access for the purposes of both surveillance and control quite easy.¹¹³ U.S. businesses have increasingly become aware of the threat from China to their IP and realized they are a target, but Chinese offensive capabilities are expanding just as defense is improving. The future will need to include layered defense and a mindset of unity of effort, whereby businesses see the incentive for sharing information about attacks.

Despite these tremendous advances, China still suffers from several weaknesses, and its vulnerabilities are exploitable. Beijing's cyber cadre is generally composed of fast followers, meaning they copy other approaches. For example, China seemed to copycat some of Russia's influence tactics after 2016, but slowly. U.S. policymakers were already on the lookout for similar tactics, making China's activity more easily identifiable. Likewise, businesses are aware of the threat and are shoring up defenses.

China's centralized approach could be an additional weakness. Xi's attempt to exert more centralized control over cyber operations will lead to more unity of effort and less rogue or vigilante activity. However, approvals for actions likely would need to run through official processes, dramatically reducing agility and limiting opportunistic action. Decisions made by committee also tend to

squelch more innovative approaches. Further, the CCP has hardly demonstrated an appetite for risk, and the reorganization was likely in part to limit the chances that an unapproved operation went forward. U.S. policymakers could build on this concern and make clear that Beijing will be held responsible for operations emanating from its territory.

As for exploitable vulnerabilities, China has several. The financial motivation of some of their top hacking talent could be used against them, in particular if their freelancing has attracted the ire of Chinese leadership. Hackers in trouble could be encouraged to defect, bringing valuable knowledge of Chinese cyber operations and adding to the United States' pool of talent. Chinese scholars have also admitted in journal articles that the CCP does not truly understand its own defensive posture or its own gaps. Beijing remains concerned about the West's capabilities. Their new structure and goal of jointness have not been tested, so the capability of running joint operations with a cyber overlay is still theoretical. Finally, the more China seeks to protect its hacking cadre from the outside world, the more stovepiped they will become as well as less knowledgeable about tactics, techniques, and procedures.

We will accelerate the development of China's discourse and narrative systems, better tell China's stories, make China's voice heard, and present a China that is credible, appealing, and respectable.

-Xi Jinping¹



加快构建中国话语和中国叙事体系，讲好中国故事、传播好中国声音，展现可信、可爱、可敬的中国形象。

-习近平²

This chapter examines Chinese information and disinformation operations, an important component of political warfare. As Thomas Rid argues in his study of political warfare during the Cold War:

At-scale disinformation campaigns are attacks against a liberal epistemic order, or a political system that places its trust in essential custodians of factual authority. These institutions—law enforcement and the criminal justice system, public administration, empirical science, investigative journalism democratically control intelligence agencies—prize facts over feelings, evidence over emotion, observations over opinion. . . . Disinformation operations, in essence, erode the very foundation of open societies.³

China views the information environment as central to its internal stability, as a key domain through which to compete with the United States, and as a core element of its military strategy across the entire spectrum of warfare and competition. While several other chapters touch on influence in various ways—including those that deal with intelligence operations, cyber operations, the united front, and economic coercion—this chapter provides the most in-depth analysis of Chinese information and disinformation efforts. As used here, disinformation includes false information that is deliberately intended to mislead an audience.

This chapter finds that Xi Jinping has prioritized the central role of information and disinformation operations in China's global strategy. Speaking at the 20th Party Congress in October 2022, for example, Xi said: "We will accelerate the development of China's discourse and narrative systems, better tell China's stories, make China's voice heard, and present a China that is credible, appealing, and respectable."⁴ Xi used his platform at the 20th National Congress to promote the narrative that Beijing must bolster its "international discourse power" (国际话语权) to exert the influence that a nation of its political, economic, and military strength is entitled to on the global stage.⁵ Accordingly, China makes extensive use of information and disinformation that promote bias and misleading information to publicize and advance its international political agenda.

The rest of this chapter is divided into four sections. First, it examines Chinese public diplomacy. Second, it analyzes Chinese media—including social media—overseas. Third, it assesses lawful political influence and information activities. Fourth, it concludes by highlighting some of the main trends in Chinese information and disinformation operations.

CHINESE PUBLIC DIPLOMACY

Beijing's official representatives amplify key messaging themes that China employs to promote its

interests abroad by leveraging various public diplomacy mechanisms, including speeches, articles, social media, and foreign broadcast engagements. These activities exist at the lowest end of the spectrum of aggression of Chinese information and disinformation operations. Their connection to the state, the Chinese Communist Party (CCP), and increasingly Xi Jinping's vision of China's role in global affairs is almost entirely overt. In many respects, Beijing's public diplomacy practices are consistent with routine state behavior.

China uses two mechanisms to execute its public diplomacy strategy. The first is a wide body of highly positive messaging designed to promote and advance China's narrative about building alternative models for global governance untethered from the post-war Anglocentric "rules-based order." These activities directly reflect Xi's guidance to "tell China's story well" (讲好中国故事) and to bolster the country's "international discourse power" (国际话语权).⁶ This positivist messaging is complemented by the more confrontational, antagonistic approach of China's "wolf warrior" diplomats. If Beijing's positivist messaging is intended to promote China's efforts to "guide reforms of the global governance system with the principle of fairness and justice," then the purpose of the more confrontational approach is to point out the hypocrisies and contradictions in the existing world order that justify a power shift away from the United States and its allies.⁷

To explore the dynamics of both the positivist and negativist elements of Chinese public diplomacy, CSIS compiled and analyzed two datasets. First, the team analyzed Chinese speeches and articles, including those by Xi Jinping, from such sources as CSIS's *Interpret: China* library. Second, the team scraped and analyzed the tweets of prominent CCP spokespersons. Together, these sources enable the research team to identify and analyze key themes in China's messaging and consider China's two contrasting but complimentary approaches to public diplomacy.

THE POSITIVIST APPROACH

Beijing's positivist messaging is designed to promote positive narratives about China's strategy, policy, and intentions. Xi Jinping and other CCP leaders frequently tout China's accomplishments and describe China, and more specifically the CCP, as a benevolent force for good in the world. For example, in his keynote address at the CCP and

World Political Parties Summit, Xi described the achievements and ambitions of the CCP:

Working for the people's wellbeing has been the original aspiration the Chinese Communist Party cherishes all the way. With the goal of moderate prosperity in all respects achieved, China has embarked on a new journey towards building a modern socialist country. The Chinese people are brimming with a greater sense of fulfillment, happiness, and security with each passing day. It is the unswerving goal of the CCP to run our own house well, ensure a happy life for the 1.4 billion plus Chinese people, and advance the lofty cause of promoting peace and development of all mankind.⁸

THE WOLF WARRIOR APPROACH

Under Xi Jinping, China's public diplomacy is increasingly designed not only to elevate China but to discredit and ultimately displace the United States and its allies. This "wolf warrior" style of diplomacy consists of an assertiveness by Chinese government officials that embraces confrontation, denounces criticism, and emphasizes perceived hypocrisy. In the body of foreign policy speeches compiled by CSIS, one of the most common phrases identified is the term "true multilateralism" (真正的多边主义).⁹ The phrase was used frequently—appearing 52 times in the 80 speeches analyzed—and also appeared in an extraordinarily diverse range of contexts.¹⁰ In 2022 alone, this included high-level Chinese government remarks to the UN Convention on the Law of the Sea, the Forum on China-Africa Cooperation, the G20, the Munich Security Conference, and the UN Climate Change Conference.¹¹ Despite serving as a cornerstone of Chinese public messaging about China's views on the nature of the international system, the phrase is rarely contextualized or further defined. Instead, it has become a shorthand in Chinese public remarks and writings to criticize U.S. initiatives that China classifies as exclusionary and pursued to sustain Washington's interests. The use of oblique and euphemistic terminology in high-profile multilateral settings is not uncommon in the speeches analyzed by CSIS. Often wrapped in messages about China's positivist and inclusive vision of global leadership are phrases accusing Washington of maintaining a "Cold War mentality" or pursuing a "new Cold War." These accusations are particularly common in the area of technology policy, where Xi Jinping and others have alleged that the United States is

pursuing “parallel systems” or building “exclusive yards with high walls” (小院高墙).

China also applies its wolf warrior approach to shape international narratives on various items that Beijing classifies as “domestic affairs,” including the matters of Taiwan, Xinjiang, Hong Kong, maritime issues, and other human rights topics.¹² These efforts portray international condemnation of China’s human rights record as hypocritical and driven by actors with “ulterior motives” while putting forth alternative perspectives on issues such as Xinjiang and Hong Kong. Chinese leaders repeatedly argue that “Xinjiang’s door is open, and we welcome people from all over the world who harbor no bias to come to Xinjiang for visits and exchanges,” and that “Hong Kong residents enjoy far more rights and freedoms according to law than under British colonial rule.”¹³

The amplification of messages issued by China’s senior leaders serves as a crucial step in the country’s broader approach to propaganda. The key themes that party leadership repeatedly emphasize in their remarks are embraced and repackaged by a wide range of official and quasi-official state and party actors and media outlets, often in increasingly negative and aggressive forms. This is perhaps most evident in the ways that China’s diplomats exploit social media and other platforms to seed confrontational rhetoric about the United States and its allies.

One of the most prominent practitioners of this type of rhetorical escalation is Zhao Lijian, a former deputy director general and official spokesperson of the Ministry of Foreign Affairs (MFA)’ Information Department. Zhao maintains an active presence on Twitter, with nearly two million followers, where he frequently uses his account to amplify anti-Western rhetoric and to propagate various conspiracy theories.¹⁴ For example, in tweets since April 2022, he has

suggested that Covid-19 originated in a U.S. biological laboratory, that a biological accident caused the 2022 monkey pox outbreak in the United States, and that the United States was developing biological weapons at laboratories in Ukraine.¹⁵ Zhao often uses Twitter as an English-language venue to question the legitimacy of U.S. democracy and to challenge the authority of the United States to serve as—in his words—a “self-claimed ‘human rights lecturer.’”¹⁶ Zhao contrasts confrontational posts about topics such as school shootings in the United States, the murder of George Floyd, U.S. wars in the developing world, and U.S. “democracy” with highly positive tweets about China’s relationship with the Global South.

Zhao’s two most viral tweets of 2022 were posts of memes depicting the destruction associated with various post-World War II U.S. military operations.¹⁷ In 2021, Xinhua—the official state news agency of the CCP—released a short video titled “Ameri-crazy.” The video purports to be a children’s song, but it levels a barrage of accusations against the United States, claiming that the United States seeks to subjugate the world with its own version of destructive democracy. Set to the tune of “the Wellerman,” a New Zealand sea ballad that gained notoriety on

Figure 5.1

“Ameri-crazy” Video

 **Ambassade de Chine en France**  @AmbassadeChine
 Organisation du gouvernement - Chine
 It is Ameri-crazy!



SOURCE: SCREENSHOT OF TWEET BY AMBASSADE DE CHINE EN FRANCE, TWITTER POST, DECEMBER 10, 2021, 9:36 A.M., [HTTPS://TWITTER.COM/AMBASSADECHINE/STATUS/1469314982424846343](https://twitter.com/AMBASSADECHINE/STATUS/1469314982424846343).

TikTok last year, the song alleges bad behavior by the United States, from military adventurism to election fraud, with lines such as the following:

Inside of the country, money talks. All policies submit to the corp[oration.] Disinformation, Gerrymandering skew election results. Trillions of dollars burned on wars yet lack money for the sick and poor; Play human rights cop across the world yet backyard you ignore.¹⁸

In the video, the main singer is surrounded by four animals, which represent nations that the United States has imposed so-called “Ameri-cracy” on: Afghanistan, Iraq, Vietnam, and the nations that saw “chaos” during the Arab Spring protests. The host interviews each of the animals at the beginning of the video about how the United States imposed this false system of democracy, thereby harming each nation.¹⁹ The main message is that everyone should be able to choose their own system of governance, as illustrated by the refrain: “Democracy of our own, reflects our culture, will and soul. If your system can cure all, why did it cause so many woes?”²⁰

Another short video geared toward a younger audience also highlights Chinese propaganda. “Once upon a virus,” released by Xinhua, features a Lego terracotta warrior warning the United States early and often about the seriousness of the pandemic. A Lego Statue of Liberty replies with nonsensical statements and denial, then blames China, in a clear satire on the Trump administration’s response to the pandemic.

In this way, Beijing’s wolf warrior diplomacy is designed to characterize China’s competitors as rank hypocrites in their approach to human rights and support for the developing world. The intensely negative messaging creates more space for efforts to tell China’s story and promote Beijing’s claim to building an alternative model for global governance.

Although public diplomacy is the most overt manifestation of Chinese propaganda, it is also enabled by semi-transparent elements. Chinese public diplomacy frequently relies on amplifying articles in Chinese state media to lend further legitimacy to its claims. During the last 100 days of 2022, nearly 20 percent of all of Zhao’s tweets were links to articles written by a single commentator on international affairs. This “commentator” reliably posts opinion articles on Chinese state media to comment on U.S. domestic issues, including alleged partisanship in the U.S. Supreme Court,

the “Twitter Files,” and the origins of Covid-19. The author’s name is “Xin Ping.” Although he has a Gmail address, there is little evidence beyond the dozens of English-language articles and the favor of Zhao Lijian to suggest Xin Ping is a real person rather than a pen name used for generating and amplifying Chinese state messaging.

Wolf warrior diplomats circulate these types of articles widely online to help create the image of robust support. Upon inspection, one may fail to notice the source of the information and risk lending credence to Chinese propaganda. For example, at a committee hearing on February 28, 2023, U.S. representative Matt Gaetz cited unsubstantiated information from a *Global Times* article without apparent knowledge of the source’s ties to the CCP. In 2020, the *Global Times* was designated as a “foreign mission” by the U.S. State Department for its adherence to promoting the interests of the CCP.

Working in tandem, China’s positivist and wolf warrior public diplomacy approaches are essential in setting the direction of the CCP’s propaganda strategy. The themes and messages crafted by political leadership in the CCP inform activities explored in the rest of this chapter. In addition, China’s propaganda efforts begin to shift from routine statecraft to public manipulation in the creation and control of media abroad. China employs three strategies to spread propaganda and control messaging about issues related to China in information environments overseas. First, China creates new media platforms in overseas markets, exercising control over the content, with varying levels of transparency. Second, it uses existing media platforms in foreign countries to promote its messaging through paid advertisements and content that often provide limited transparency to their Chinese origin. Third, China leverages access to its domestic market to aggressively censor foreign media and information ecosystems. Combined, these three strategies enable China to further spread propaganda and often hide its manipulation.

NEW MEDIA PLATFORMS

China’s growing influence in global information environments is partly a result of its expanded creation of Chinese-owned media platforms. This section explores China’s gains in the areas of television and social media. In recent years, the most significant example of China’s expanding media prowess has been the creation and proliferation of the social media platform TikTok. The idea for

TikTok began as a domestic Chinese video sharing app. ByteDance, its parent company, then reinvented the app for a worldwide audience. The United States is its largest market, including a multiyear marketing deal with the National Football League.²¹ TikTok's business model is to provide the users with a never-ending stream of short, fun videos. The user does not curate their own feed with likes or other active feedback. Rather the app monitors whether a user lingers on a video or passes it by and collects detailed information on the user's behavior surrounding a video. Its proprietary algorithm then feeds that user more content designed to maximize engagement with the app.

Through these feedback loops and logging user activity, TikTok gathers significant amounts of information about a huge number of users, allowing anyone with access to the data to construct not only broad facts about the user base but also highly detailed profiles about specific users. TikTok collects so much data on users that U.S. officials have gone so far as to characterize it as a foreign surveillance tool.²² As a result of its popularity and data collection capabilities, TikTok poses at least two threats.

First, the user data collected poses cybersecurity risks. China could use the app to seize the data or access the software of millions of users, including gaining access to the camera and microphone on users' mobile devices. Second, TikTok provides Beijing an opportunity to control information and promote propaganda to overseas audiences, with a keen understanding of how users respond to content and transparency. Documents revealed by the Guardian in 2019 showed how ByteDance sought to advance Chinese foreign policy with TikTok, in part by requiring TikTok employees to remove content about the Tiananmen Square massacre and Falun Gong.²³

Searches about the Hong Kong protests have returned few results.²⁴ In 2019, searches for specific politically sensitive terms, such as the hashtag "#antielab," indicated suppression of discussions on TikTok. The hashtag "#antielab" had more than 34,000 posts on Instagram but only about 11 posts on TikTok. The hashtags "#HongKongProtests" and "#HongKongProtestors," which served to rally support for the protests on Twitter, turned up either a single video or an error message on TikTok. Searching with Chinese characters returned similar results.²⁵ Such results have led to concerns that TikTok can filter out news unfriendly to China and shape Americans' views of the truth. Federal Bureau of Investigation (FBI) director Christopher

Wray remarked that he was "extremely concerned" about TikTok and about China using the app to both steal user data and shape public opinion.²⁶

TikTok's response to these criticisms is two-fold. First, TikTok claims that many of these policies have been rescinded since 2019. Second, TikTok reports that it is moving U.S. user data onshore with the help of Oracle's cloud and that it has not and will not provide that data to China.²⁷ TikTok announced Project Texas in 2021, which would wall off "protected" data for U.S. users, including phone numbers and birthdays.²⁸ In June 2022, TikTok claimed it was migrating all U.S. user traffic to Oracle Cloud Infrastructure, with data centers in the United States and Singapore as backups.²⁹ These moves were conducted with an eye toward successfully making it through examination by the Committee on Foreign Investment in the United States.

Social media is not the only medium where China has made a push to increase its influence through the creation of new information streams. China also uses its global television presence to broadcast a positive image of China into areas that could not otherwise afford digital television and inject a pro-Beijing viewpoint into media in the developed world. The top two global Chinese TV outlets are China Global Television Network (CGTN) and state broadcaster China Central Television (CCTV).³⁰ These state media outlets reach hundreds of millions of television viewers, radio listeners, and social media users abroad, and Freedom House reports that in many cases the outlets provide little to no transparency on who publishes the content.³¹ CGTN broadcasts in five languages and has hundreds of journalists stationed overseas.³² As one assessment concluded:

SinoVision, a Chinese-language TV broadcaster, and Qiaobao, one of the largest Chinese-language newspapers in the U.S., are subsidiaries of the Asian Culture and Media Group, an arm of the Chinese government. Staff at both places cut their teeth at the state-owned China News Service and are often dispatched to the U.S. for propaganda purposes. Once there, most of their stories on China, Sino-American relations, Taiwan, Hong Kong and related subjects are reproduced from state-owned media such as Xinhua and the People's Daily.³³

One can trace narratives through these news outlets, as vetted talking points get repeated. Chinese television outlets have a presence around the world, as solo entities and in joint partnerships. In Africa, Zimbabwe's state-run television and

CCTV signed an agreement in 2011 to share news programming.³⁴ In Kenya, a popular television service includes Chinese state television in its most affordable package but omits other international news outlets. In a small town in southern Kenya, a new recipient of cheap Chinese digital TV service said, “I didn’t know about China before. . . . I can say it’s good. They have changed this country in a big way, very fast.”³⁵ Guo Ziqi, the vice chairman of Chinese media company StarTimes, remarked that “Our aim is to enable every African household to afford digital TV, watch good digital TV and enjoy the digital life.”³⁶ But StarTimes is also heavily subsidized by the Chinese government and has a mandate to portray a rosy picture of China to Africans.

In Asia, the Thai News Network signed a deal with Xinhua in 2014 to broadcast the *China Report* program daily.³⁷ The Pakistan Television Corporation partnered with ZTE in 2017 to expand digital TV service to rural areas. ZTE issued a statement saying that the agreement “will cover collaboration across R&D of digital terrestrial television technologies, staff training, and content.”³⁸ Pakistan adopted the Chinese standard for digital television broadcasts in an event officiated by Xi Jinping and Pakistan’s former prime minister Nawaz Sharif. In Laos, Chinese aid facilitated the transition to digital transmission, with the state broadcaster subsequently signing an agreement with a Chinese media company to create joint content, including news programs. In Cambodia, a joint venture has been transmitting Chinese news on local Cambodian stations since 2017. Timor-Leste also agreed with two Chinese companies to embark on a digital television expansion program.³⁹

CGTN broadcasts in English, Spanish, French, Arabic, and Russian around the globe via satellite, cable, and over the internet. Other global examples of China’s reach include TV Peru’s Channel 7, which broadcast documentaries produced by CGTN about China as Lima hosted the Asia-Pacific Economic Cooperation in 2016. In Cuba, Huawei led the transition from analog to digital television. Portuguese TV launched a prime-time “China Hour” featuring content from Chinese state media, and a German public station aired a current affairs program called *Dialogue with China*, coproduced with a controversial CGTN host. In Africa and the Middle East, Chinese state media has also developed unique publications geared toward local populations.⁴⁰

China’s control over social media platforms and television networks overseas gives the CCP the opportunity to influence billions of individuals

with Chinese propaganda. By exporting information streams that it has the power to control, the CCP can spread a positive image of China and limit or otherwise manipulate negative narratives about China.

EXISTING MEDIA PLATFORMS

China’s second strategy to spread information and disinformation overseas is to use existing media platforms to host content that advances its political objectives. China’s print strategy has frequently pursued this approach, which China refers to as “borrowing the boat to reach the sea” (借船出海). The idea is to use existing outlets as a conveyance for Chinese propaganda. As Xi Jinping stated in 2016, “Wherever the readers are, wherever the viewers are, that is where propaganda reports must extend their tentacles.”⁴¹

In the United States, *China Watch* has appeared in the folds of the *Wall Street Journal*, *Washington Post*, *Los Angeles Times*, and *New York Times*. The paid advertising supplement, published by *China Daily*, has featured stories that depict the CCP’s response to the Covid-19 pandemic in a positive light, claim that the Hong Kong protestors are sponsored by the United States, and protest U.S. trade policy. The inserts generally come with a warning, with the one in the *Washington Post* clearly stating, “Content in this advertising section was prepared by China Daily, and did not involve the news or opinion staff of The Washington Post.”⁴² But criticism of giving the CCP a prominent outlet through which to broadcast its message has led many outlets to drop the insert, passing on millions in ad revenue.⁴³ Similar inserts have appeared in major newspapers in Spain, the United Kingdom, Australia, Argentina, Peru, Senegal, and India.⁴⁴

Chinese outlets also provide free content to partners, in particular Chinese-language papers serving Chinese diaspora communities. The *Financial Times* reported that there was a sharp uptick in content-sharing agreements in 2016 and 2017, with 200 Chinese-language publications around the world broadcasting content created by party-affiliated outlets.⁴⁵ However, content sharing is not exclusively limited to Chinese-language outlets. Chinese state news agencies provide content and photos free of charge to appear under the masthead of overseas publications. Freedom House reports that Xinhua has exchange agreements with local counterparts in Australia, Bangladesh, Belarus, Egypt, India, Italy, Laos, Nigeria, Thailand, and Vietnam.⁴⁶ Such

content often appears native to the independent publication. At best, the fine print identifies the source.⁴⁷ These types of content agreements also extend beyond print publications into television and radio programming.

Overall, China's approach of "borrowing the boat to reach the sea" is designed to exploit the popularity of existing platforms and co-opt the trust of consumers. Across all mediums, the content is designed to promote a positive image of China while obfuscating the country's involvement. By appearing in native outlets or as native content, Chinese propaganda is likely to deceive many consumers, who may fail to realize the information they are consuming is possibly biased or misleading.

CHINESE CENSORSHIP OVERSEAS

Beijing seeks to tightly control the image of China seen by its domestic audience and also seen by those abroad. To do so, the CCP wields a tight grip over the Chinese market to influence information environments globally. This section uses two case studies, the National Basketball Association (NBA) and Hollywood, to examine how the CCP leverages access to China's massive consumer base to influence foreign media to promote CCP narratives and self-censor to align with Chinese propaganda.

NATIONAL BASKETBALL ASSOCIATION

In October 2019, Houston Rockets general manager Daryl Morey posted a tweet that said: "Fight for freedom, stand with Hong Kong."

China was outraged. In the following days, nearly 170,000 tweets flooded out of China back at Morey, an effort the *Wall Street Journal* said "appears to be a coordinated harassment campaign."⁴⁸ Pro-Chinese government accounts mentioned Morey more than 16,000 times. Those accounts most likely were humans at keyboards—"a troll mob," according to Ben Nimmo, the head of investigations at Graphika Inc.⁴⁹ Approximately 4,700 of those replies included "NMSL," a Chinese acronym meaning "your mother is dead."⁵⁰ This high volume of activity is all the more anomalous given that Twitter is banned in China. Morey quickly deleted his tweet and posted an apology, but the situation continued to escalate.

At the time, the Rockets were the second-most popular team in China, but Chinese state priorities trumped fan support.⁵¹ Chinese state institutions

Figure 5.2

Daryl Morey Twitter Responses to Criticism



SOURCE: SCREENSHOT OF SINCE DELETED TWEET BY DARYL MOREY, TWITTER POST, OCTOBER 6, 2019, 5:18 P.M., [HTTPS://WEB.ARCHIVE.ORG/WEB/20191008092754/HTTPS://TWITTER.COM/DMOREY/STATUS/1181000809363857409](https://web.archive.org/web/20191008092754/https://twitter.com/dmorey/status/1181000809363857409)

cut ties with the Rockets, as did China's leading sportswear brand and the club's main sponsor in China, a bank.⁵² The Rockets' owner, who bought the team in part because of its market share in China, immediately distanced himself from Morey's tweet.⁵³ Then Chinese state media and Tencent, both of which held exclusive rights to broadcast NBA games in China, stopped airing NBA games.⁵⁴ Tencent resumed airing NBA games 11 days after the tweet—with the exception of games featuring the Rockets. When Morey moved to manage the Philadelphia 76ers in October 2020, that team was removed from Tencent's broadcasting.⁵⁵

Morey was not the only one to apologize. Numerous NBA officials and players scrambled to either distance themselves from Morey or describe the NBA as apolitical. Rockets star James Harden apologized and said, "We love China."⁵⁶ The NBA issued a statement in English that said: "We recognize that the views expressed by the Houston Rockets general manager Daryl Morey have deeply offended many of our friends and fans in China, which is regrettable. While Daryl has made it clear that this tweet does not represent the Rockets or the NBA, the values of the league support individuals' educating themselves and sharing their views on matters important to them." However,

a version translated to Mandarin and published on Weibo said that the league was “extremely disappointed” by the “inappropriate” tweet, which “severely hurt the feelings of Chinese fans.” The NBA spokesman said the English version was the “official” statement.⁵⁷

However, some U.S. political leaders on both sides of the aisle accused the NBA of bowing to China’s economic power and excusing Beijing’s human rights violations.⁵⁸ The relationship thawed temporarily in October 2020 when Chinese media broadcast the NBA Finals. The broadcast was accompanied by an announcement that the NBA had expressed goodwill and had “made active efforts to support the Chinese people in their fight against COVID-19.”⁵⁹ CCTV then renewed the blackout until March 2022, after the Beijing Olympics, when games unceremoniously began reappearing.

In the three-year gap in coverage, NBA team owners and players largely stayed silent while the league worked behind the scenes to repair the relationship. An ESPN in-depth investigation found that while the NBA’s presence in China was worth an estimated \$5 billion that was shared equally among the teams—including \$1.5 billion for Tencent streaming—many team owners also had “significant personal stakes” in China through their business interests.⁶⁰ As the investigation concluded: “ESPN examined the investments of 40 principal owners and found that they collectively have more than \$10 billion tied up in China—including one owner whose company has a joint venture with an entity that has been sanctioned by the U.S. government.”⁶¹

That same owner, Micky Arison of the Miami Heat, was a prominent advocate for human rights in the United States. In 2020, Arison described the Miami Heat’s commitment to social justice as “never-ending,” in the context of racial justice. ESPN cited Robert Kuhn, an adviser to multinational corporations operating in China and to Chinese political leaders, explaining this conundrum: “It’s a tension between those two poles . . . to see companies promoting social justice in the U.S. but staying silent on what would be perceived to be far worse issues in China. This is going to be an issue for the rest of our working lives.”⁶²

Not long after the Daryl Morey incident, Enes Kanter Freedom, who played for the Boston Celtics, publicly criticized human rights abuses in China. Kanter Freedom called on his teammates and others in the NBA to speak out against Chinese human rights abuses, and he decorated his game sneakers with phrases about Uyghurs, forced labor,

and related issues. Tencent dropped Celtics games in response. The NBA responded that Freedom was allowed to wear shoes advocating his causes and supported his right to speak out. However, Freedom told CNN in 2021 that he was heavily criticized for speaking out against China. “I’ve been talking about all the human rights violations and injustices happening in Turkey for 10 years, and I did not get one phone call,” he said. “I talk about China one day, and I was getting a phone call once every two hours.”⁶³ Freedom was traded in February 2022 to the Houston Rockets, who waived his contract less than a week later.⁶⁴ A Chinese journalist from *China Daily*, an English-language newspaper owned by the CCP, trolled Freedom. “Now you don’t play basketball,” the journalist said. “John Bolton can play you more.”⁶⁵

HOLLYWOOD

Arguably, China’s soft power has been most significant in its relationship with Hollywood. The size of the Chinese movie market can substantially influence the profitability of a film, Chinese censors let a limited number of films into its market each year, and those censors have a long and inconsistently implemented set of criteria for what makes a good movie. As a result, Hollywood producers will self-censor by removing any elements that could be perceived as critical of China. Producers sometimes also add elements that appeal to Chinese audiences and bureaucrats. As a report by PEN America, a nonprofit organization that supports artistic freedom and human rights, summarized, “The result is a system in which Beijing bureaucrats can demand changes to Hollywood movies—or expect Hollywood insiders to anticipate and make these changes, unprompted—without any significant hue or cry over such censorship.”⁶⁶

Chinese influence on Hollywood has escalated in the last decade, but the trendline began in the mid-1990s after Mao’s death. Beijing agreed to allow 10 imported movies a year, starting with *The Fugitive*. But it was *Titanic*’s box office numbers in China—with \$44 million in revenue—that made Hollywood take notice of the potential scale of the Chinese market.⁶⁷

Two movies about Tibet in 1997 demonstrated that Beijing had both the will and the muscle to influence the movie market. *Kundun*, produced by Disney, and *Seven Years in Tibet*, produced by Sony, both featured the Dalai Lama and his Tibetan homeland. Neither film ever appeared on Chinese screens, and Beijing banned both companies entirely from China.⁶⁸ While discussing his 2022 book *Red*

Carpet: Hollywood, China and the Global Battle for Cultural Supremacy with NPR, Erich Schwartzel described the following scene:

The executives at Disney . . . knew if they canceled the production [of *Kundun*] as the Chinese authorities had requested, they would have been tarred in the Hollywood community for squelching free expression, for muzzling Martin Scorsese. They knew that they would have a lot of domestic blowback if they did that, too. So they had to really thread the needle. And what they ultimately decided to do was release *Kundun* into theaters, but bury it. And so *Kundun* was released on Christmas Day on four screens, and then when it didn't perform well, the Disney executives used that lousy performance to justify not expanding it much further. And actually, despite all their efforts, they still were banned in China, and the then CEO Michael Eisner had to fly over to Beijing a year later and meet with officials and apologize. There's a fascinating transcript that exists of his meeting with a Chinese official in which he says, "The bad news is that the movie was released. The good news is that nobody saw it."⁶⁹

Hollywood's incentive to play to China's interests grew considerably in 2012 after then vice president Biden and his counterpart, then vice president Xi Jinping, negotiated a higher quota of 34 movies per year, along with a hike in the percentage of ticket sales that go to back to the studios.⁷⁰ By 2018, China surpassed the United States in quarterly box office revenue.⁷¹ In 2020, China officially surpassed the United States as the world's biggest box office.⁷² China had more than 80,000 screens, compared to approximately 39,000 in the United States.⁷³

Any film that hopes to capture some of this vast revenue must first get past Chinese censors in the Central Propaganda Department, the Ministry of State Security, the State Ethnic Affairs Commission, the Ministry of Public Security, the State Bureau of Religious Affairs, the Ministry of Education, the Ministry of Justice, the MFA, and numerous other bureaucratic entities.⁷⁴ In 2016, Beijing passed the Film Industry Promotion Law, including the following list of reasons content could be banned:

- Violations of the basic principles of the constitution, incitement of resistance to or undermining of implementation of the constitution, laws, or administrative regulations;
- Endangerment of the national unity, sovereignty or territorial integrity; leaking state secrets; endangering national security; harming national dignity, honor or interests; advocating terrorism or extremism;
- Belittling exceptional ethnic cultural traditions, incitement of ethnic hatred or ethnic discrimination, violations of ethnic customs, distortion of ethnic history or ethnic historical figures, injuring ethnic sentiments or undermining ethnic unity;
- Inciting the undermining of national religious policy, advocating cults or superstitions;
- Endangerment of social morality, disturbing social order, undermining social stability; promoting pornography, gambling, drug use, violence, or terror; instigation of crimes or imparting criminal methods;
- Violations of the lawful rights and interests of minors or harming the physical and psychological health of minors;
- Insults or defamation of others, or spreading others' private information and infringement of others' lawful rights and interests;
- Other content prohibited by laws or administrative regulations.⁷⁵

Article 36 of the same law goes further, saying that the Chinese state supports films that "transmit the glorious Chinese culture or promote core socialist values."⁷⁶ To reach these vague and arbitrary standards, studios have cast mainland Chinese actors, shot parts of films in China, and even invited Chinese regulators to visit their sets.⁷⁷ In the 2014 film *Transformers: Age of Extinction*, Mark Wahlberg's character withdraws money from a China Construction Bank ATM while in Texas. In another scene from the same film, a character buys Chinese protein powder at a Chicago convenience store.

One studio was shocked by the vague objection that got its film, *In Good Company*, banned. In the film, a young businessman gets a job and displaces his older boss. Chinese censors said that they would not allow a movie centered on a younger generation challenging the system.⁷⁸ The Marvel Studios film *Shang-Chi and the Legend of the Ten Rings* was designed with China in mind, but China banned the film—almost certainly for political reasons. Simu Liu, the lead actor in the movie, left China in the mid-1990s and criticized his former

country as a third world country whose people “were dying of starvation.”⁷⁹

With such themes getting films banned, film studios do not dare take on third rail topics, such as the Uyghur oppression, Taiwanese independence, or Hong Kong. As one Hollywood producer acknowledged: “All of us are fearful of being named in an article even generally discussing China in Hollywood.”⁸⁰ Another Hollywood producer put it bluntly: “It’s hard for people to speak on the record if they want to keep their jobs.”⁸¹ In an additional example of Chinese influence, Chloe Zhao was lauded by Beijing as an acclaimed director until an old interview surfaced where she said that in China “there are lies everywhere.”⁸² Beijing responded by deleting social media celebrations of her Oscar win, canceling the release of her celebrated film *Nomadland*, and banning the movie *Eternals*, which she directed.

China has also begun to produce higher-quality films, squeezing the space available for Hollywood blockbusters. In 2020, the top 25 highest-grossing movies of all time in the box office in China included only seven Hollywood films. The rest were produced in China or Hong Kong. One example of a made-in-China blockbuster was *Wolf Warrior 2*. As one U.S. academic wrote, the movie “hammers away at a single message: China is bringing security, prosperity, and modern health care to Africa, while the United States is bringing only misery.”⁸³ The movie made \$802 million, making it one of the highest-grossing films in Chinese history. Similarly, the movies *Operation Mekong* (2016) and *Operation Red Sea* (2018) describe Chinese soldiers as virtuous and brave and are explicitly anti-American.⁸⁴ In 2021, China released *The Battle at Lake Changjin*, a fictitious account of the 1950 Battle of the Chosin Reservoir during the Korean War. The movie, which centers around a conventional battle between U.S. and Chinese forces, garnered nearly \$1 billion at the worldwide box office, making it the highest-grossing Chinese film of all time.⁸⁵

In yet another example of Chinese influence in Hollywood, the U.S. actor John Cena, one of the stars of *F9* (from the “Fast and Furious” series), referred to Taiwan as a country—and then went to great lengths to apologize.⁸⁶ The producers had worked hard to position the movie for success in China. It was coproduced with the state-owned China Film Group Corp., and it premiered in China more than a month before it appeared in the United States, at a time suitable for the Chinese centenary celebrations.⁸⁷ But Cena, who was taking

Mandarin lessons, told a Taiwanese broadcaster in Mandarin that “Taiwan is the first country that can watch *F9*.”⁸⁸ Cena then issued a rambling apology in Mandarin on Weibo: “I made a mistake, I must say right now. It’s so, so, so, so, so, so important. I love and respect Chinese people . . . I’m very sorry for my mistakes. Sorry. Sorry. I’m really sorry. You have to understand that I love and respect China and Chinese people.”⁸⁹ *F9* then grossed \$136 million in its first weekend in China, more than double its North American box office take.⁹⁰

Executives in the NBA, Hollywood, and other businesses understand that China is watching them, including what their executives say in public. For anyone hoping to tap into China’s enormous consumer market, the deal is clear: align with the approved narratives of the CCP or jeopardize profits. In this way, the fear of losing access to the Chinese market advances the CCP’s propaganda efforts in foreign information environments.

LAWFUL POLITICAL INFLUENCE AND INFORMATION ACTIVITIES

In addition to targeting the media environments of foreign countries, China attempts to spread propaganda by directly influencing political leaders and institutions. China—like other nation-states—enlists overseas consultants, lobbyists, and public relations experts to conduct a wide range of information activities on its behalf. In many countries, political campaign financing and foreign agent registration laws are designed to prevent interference in domestic policy deliberations and elections. Such regulations include the Foreign Agent Registration Act (FARA) and the Lobbying Disclosure Act (LDA) in the United States, the Foreign Influence Transparency Scheme (FITS) and the Electoral Funding and Disclosure Reform Act in Australia, and the proposed Foreign Influence Registration Scheme (FIRS) in the United Kingdom.

Although governed by certain country-specific prohibitions and reporting requirements, mechanisms such as FARA, LDA, and FITS are primarily designed as disclosure statutes in that they are intended to ensure that government officials and the public are aware of the true source or sponsor of certain sources of information.⁹¹ As such, many of the public relations, lobbying, and other political activities of registered “agents of foreign principals” are not forms of covert influence, as the connection between the domestic “agent” and the “foreign principal” is a matter of public

record. Nevertheless, China and other countries recognize that adept navigation of these disclosure requirements provides an important vehicle for shaping policy, opinions, and broader discourse about issues of strategic concern.

While transparency regulations provide tools for governments and their citizens to identify direct connections between certain activities and their foreign sponsors, these regulations are often not set up to disclose incidents in which foreign agent activities have indirect or second-order impacts.

To evaluate the types of activities that Chinese actors undertake under transparency statutes, the CSIS research team focused on documents that are made available to the public under the United States' FARA and LDA statutes as well as documentation made available to the public pursuant to Australia's FITS program. Overall, these transparency statutes reveal the range of activities that are conducted by registered agents in the United States and Australia, which includes work for four general categories of foreign principals:

- **Category 1:** Chinese government establishments, including embassies and local consulates (which are required to be disclosed under FARA);
- **Category 2:** Organizations widely attributed to the CCP's united front efforts, including the China-United States Exchange Foundation and the China Council for the Promotion of International Trade (which are typically disclosed under FARA);⁹²
- **Category 3:** State-owned or state-affiliated enterprises, such as Huawei, Hikvision, DJI, and Bytedance (which could be disclosed under FARA or the LDA, depending on the type of activity); and
- **Category 4:** State-owned media franchises, such as *China Daily* and CGTN (which are typically disclosed under FARA).

In January 2023, for example, 15 Chinese "foreign principals" were actively registered under FARA, with a total of 22 U.S.-based "foreign agents" representing these entities.⁹³ Since 2017, a total of 38 Chinese foreign principals have registered under FARA, several of them repeatedly as they commissioned new work on China's behalf. Since 2010, a total of 75 FARA registrations have been associated with China, ranking Beijing seventh among all foreign powers, ahead of the eighth-place United Arab Emirates (64 registrations) and behind South

Korea and Turkey (tied at 78 registrations). U.S. entities engaged in certain lobbying activities are exempt from FARA if they opt to register under the LDA, as long as they are not lobbying on behalf of a foreign government or a foreign political party. Much of the lobbying activity that is conducted on behalf of a Chinese state-owned and state-affiliated enterprise is disclosed through the U.S. Congress's LDA reporting system rather than through FARA. Since 2005, a total of 116 Chinese-owned entities have registered lobbying activities under the LDA, which includes the U.S.-based lobbying activities of many high-profile Chinese technology companies, such as Hikvision, Lexmark, Lenovo, DJI, Bytedance, and Huawei.⁹⁴

The remainder of this section focuses on the activities undertaken on behalf of entities registered under FARA that fall under the first two categories referenced above. It is within the activities of these two types of foreign principals where an "influence the influencer" approach to Chinese propaganda is most pronounced, as will be described in specific examples below. Moreover, these activities are often different from those conducted on behalf of the entities included in the third and fourth categories. The connections between the foreign principal and the foreign agent are often much clearer, as the activities of the foreign agent are often conducted clearly under the banner of the foreign principal. Examples include the rebroadcast and distribution of Chinese state media as well as instances in which U.S. public relations firms may assist with brand awareness and marketing, such as in the case of a U.S. firm that managed Huawei's U.S.-based social media accounts.⁹⁵

The following example highlights how the Chinese government and organizations associated with the CCP's broader united front work navigate FARA requirements to conduct information operations and perception management activities that can be difficult to measure and complicated to attribute to China. In December 2021, a U.S.-based public relations firm registered as a foreign agent after signing a \$300,000 contract with the Consulate General of the People's Republic of China in New York to develop a social media campaign to promote the 2022 Beijing Winter Olympics. As stipulated in the contract, the Chinese government had the authority to approve all content generated in support of the campaign and directed the specific themes that the campaign should emphasize, including "Beijing's history, cultural relics, modern life of people, new trends, etc." and "any good things in China-US relations."⁹⁶ The U.S.-based public relations firm subsequently worked through an intermediary

firm to hire 11 social media influencers to conduct the consulate's social media campaign.

As disclosed at the conclusion of the contract, a total of 26 social media posts were paid for by the Chinese government that reached 4 million interactions across Instagram, TikTok, and YouTube. None of these social media posts needed to disclose the actual sponsor of the content, which was the Chinese government. Exacerbating the challenge surrounding this type of influence, the media firm working as China's foreign agent operated according to its obligations under FARA. It disclosed its activities to U.S. Department of Justice (DOJ), including the various individuals contacted pursuant to the work on behalf of the Chinese consulate. Nevertheless, the social media influencers hired as part of these efforts were not subject to the same disclosure requirements. Their social media posts needed no disclaimer that their posts had ultimately been paid for by China.⁹⁷ The millions of social media users who encountered the 26 sponsored posts could not have known that the posts were connected to—and paid for by—the Chinese government until the details of the campaign were filed with the DOJ in April 2022. This date came two months after the Olympics concluded.

CONCLUSION

This chapter explored several ways that China is extending the reach of its information and disinformation into foreign media and political environments, but it is by no means an exhaustive analysis. Though the tool kit for spreading information and disinformation is constantly evolving, China's goal remains the same: to increase Chinese power and influence and decrease U.S. power and influence. The CCP advances its goals through propaganda by promoting a positive view of China and suppressing and delegitimizing criticism. Without access to unbiased information, international audiences may fail to recognize and hold Beijing accountable for its part in controversial issues.

Although the effects of information and disinformation alone are difficult to measure, one can look for indicators of China's success. The CCP has successfully established dominance over Chinese-language media in the diaspora; created self-censorship in some Western industries, including Hollywood; and influenced content on some of the largest international social media platforms. However, there are limits to Beijing's propaganda efforts. China

has also orchestrated an aggressive intimidation and pressure campaign against multinational companies—including conducting police raids of U.S. companies Bain & Company and the Mintz Group—in China.⁹⁸ As U.S. Congressman Mike Gallagher remarked in April 2023, “The CCP's updated counter-espionage law sends a loud, clear signal to the world: there is no such thing as a private company in China. . . . Our business leaders need to take off their golden blindfolds and recognize that the recent police raids of American companies Bain and Mintz are not one-offs but part of a long, proud tradition of exploitation.”⁹⁹

Media outlets and digital platforms still publish content that is critical of China. In addition, views of China in the United States have become increasingly negative over the past several years, according to public opinion polls.¹⁰⁰ Unfavorable views of China are also high in numerous Indo-Pacific countries (such as South Korea, Japan, Australia, and India) and European countries (such as Sweden, the Netherlands, the United Kingdom, and Germany).¹⁰¹ Nevertheless, China's propaganda efforts should not be underestimated as the country continues to grow its sprawling tool kit to control information internationally.

Everyone must remember: no matter where you are, you are sons and daughters of China.

-Xi Jinping¹

THE UNITED FRONT



大家都要牢记, 无论身在何处, 你们都是中华儿女的一分子。

-习近平²

6

This chapter focuses on Chinese Communist Party (CCP) efforts to disrupt perceived security and reputational harm through “united front” work.

Used in this context, united front work involves activity to protect and bolster the image of China and the CCP by monitoring and countering criticism overseas. United front work includes widespread intimidation and harassment of Chinese students, diaspora communities, and critics of Chinese domestic and foreign policy on a global scale. It also includes activities conducted in support of China’s soft-power agenda, which seeks to influence individuals who are potentially well positioned to amplify China’s preferred messaging on political, economic, and academic issues. As Stanford University professor Larry Diamond summarized, “China is deploying classic Communist Party ‘united front’ tactics to penetrate and coopt the soft tissues of democracy—universities, think tanks, research centers, new media, the arts, corporations, community organizations, political parties, and local governments.”³

United front work has evolved under Xi Jinping as one of the cornerstones of the CCP’s efforts to conduct a wide range of political influence and information operations globally. The CCP’s main organization for conducting united front work is the United Front Work Department (UFWD). However, there are also dozens of organizations

with both direct and indirect links to the UFWD which are responsible for promoting CCP discipline on a global scale, focusing primarily on Chinese students and diaspora communities, and building bonds with influential global political, business, and academic leaders.

This chapter illustrates how united front work materializes across core elements of China’s political warfare strategy. It focuses on how the united front intersects with global institutions of higher learning, how the united front and its affiliates engage in overseas political influence and interference, and how the united front is deployed to extend the reach of the CCP and China into worldwide Chinese diaspora communities.

As this chapter argues, one of the most significant impacts of China’s overseas united front work is undermining the sovereignty of the countries where these activities take place. In democracies, united front activities often undermine the freedoms that Chinese students and diaspora communities are entitled to while residing in countries such as the United States, Canada, Australia, the United Kingdom, and many European states. China, often operating under the guise of various united front affiliated organizations, uses multiple tools to harass, intimidate, and punish perceived enemies overseas and their families in China. In other cases, united front activities undermine sovereignty by manifesting in varying levels of covert influence. Beijing—often operating through various united

front-affiliated organizations—is adept at complying with foreign influence transparency regimes in ways that often limit the public’s ability to fully understand the scope of Beijing’s activities. This chapter identifies several specific examples where existing U.S. laws governing foreign media, lobbying, and academic activities may not be capable of shedding sufficient light on Beijing’s engagement in these areas.

The remainder of this chapter provides an overview of the history of the united front and its resurgence under the leadership of Xi Jinping. It then analyzes available open-source evidence of overseas united front work in the areas of higher education, politics, and diaspora communities. Next, it closes with a broader analysis of the impact of these activities. As will be evident in all three of the case studies, broader united front work integrates efforts to make friends and punish enemies, with the primary focus—as described by Xi Jinping in early 2023—to build on the theme of “following the party unswervingly and forging ahead in the new era hand in hand.”⁴

THE UNITED FRONT’S HISTORIC IMPORTANCE TO THE CCP

The united front is deeply rooted in the idea of the modern People’s Republic of China (PRC) as a unitary party state, with the CCP overseeing all aspects of social, political, and economic life. The concept of the “united front” (统战), which is rooted in Leninism, has served a central role in the CCP since Mao Zedong described it as one of the party’s “three magic weapons” (三个法宝)—alongside armed struggle and party building—in 1939.⁵ Mao was writing of the CCP’s temporary alliances with Chiang Kai-shek and the Kuomintang nationalists in the 1920s and, as he wrote in 1939, during the Second Sino-Japanese War. The concept, as he envisioned it, emphasized unifying diverse elements under the central control and direction of the CCP. In the early years of the PRC, this included the establishment of dozens of party-affiliated organizations designed to exert control over the vast majority of Chinese citizens who were not members of the CCP.⁶ Although Chinese leaders since Mao have rhetorically highlighted the importance of the united front as a concept, the party’s commitment to such work languished for decades. It was not until the ascendance of Xi Jinping that united front work reemerged as a CCP priority, particularly as a key pillar of China’s efforts to expand its global influence. As this

chapter describes, the united front has reemerged under Xi as a key component of Chinese political warfare, with different elements operating under the broader banner of “united front work” overseas to shape perceptions, influence powerful friends, and intimidate and punish the CCP’s enemies.

Since taking power, Xi Jinping has reenergized and reformed united front work and made it a critical element of China’s domestic and foreign policies. This focus on united front work as part of his leadership should come as little surprise in light of his own prior writings on the subject. In 1995, while still a CCP official in Fujian province, Xi urged that united front efforts should be expanded and prioritized: “We believe that the work of overseas Chinese affairs in the new era should break through geographical boundaries, jump out of the scope of overseas Chinese affairs departments, and make it a major event of the party and governments at all levels, and a major event of common concern and participation of the whole society.”⁷ Once in power, Xi echoed Mao’s vision of united front work, including in a September 2014 speech to the Chinese People’s Political Consultative Conference, a key united front organ: “The united front is an important magic weapon for the Communist Party of China to win the cause of revolution, construction, and reform, and also to realize the greatness of the Chinese nation. An important magic weapon for revival.”⁸ These remarks were quickly followed by a reorganization of the party’s approach to united front work, which included the April 2015 release of new “Regulations on the Work of the United Front of the Communist Party of China,” hailed by the CCP as “the first intra-party regulation of our party on the work of the united front.”⁹ Ushering in this new era for the united front, in May 2015, Xi presided over the first United Front Work Conference in nine years. Notably, this convening represented the first time in the party’s history that the conference was held at the central, rather than national, level, a significant elevation in status within CCP governance. At this first ever “Central United Front Work Conference,” Xi made the overarching intent abundantly clear: “The policies implemented and the measures taken must be conducive to maintaining and consolidating the party’s leadership and ruling position.”¹⁰

Reflecting the enduring importance and continued evolution of united front work under Xi’s leadership, the united front regulations were revised again in late 2020.¹¹ Additionally, in a series of reorganizations that occurred in 2018 and 2019, Xi transferred several critical overseas responsi-

bilities from the Ministry of Foreign Affairs (MFA) and merged the Overseas Chinese Affairs Office into the CCP's primary united front organ—the UFWD. These moves consolidated many of the responsibilities for monitoring, influencing, and coopting diaspora communities into the UFWD.¹²

The scope of the CCP's united front work, both domestically and abroad, is massive, and a full accounting of the various entities through which the party and the Chinese government advance efforts through united front work would not be practical to include in this chapter. Moreover, the full scope of what formally distinguishes united front work from other efforts to promote the interests of the CCP is often blurry. As such, it is difficult to fully disaggregate China's approach to united front work from its broader global intelligence and information warfare activities. As reflected in the chapter on Chinese espionage operations (Chapter 3), there is significant overlap between China's efforts to monitor, co-opt, and intimidate overseas dissident groups and the priorities of united front work.

In many circumstances, various patterns of China's overseas activities cannot be attributed to a specific entity. For example, the Ministry of State Security (MSS), Ministry of Public Security (MPS), People's Liberation Army (PLA), Central Commission for Discipline Inspection, and various united front organizations engage in similar patterns of behavior, particularly when antagonizing overseas diaspora groups.

Several scholars have described the UFWD as a form of intelligence service. There are justified reasons for viewing the UFWD and the broader campaign of united front work through this lens. Zhou Enlai—an architect of China's intelligence and security apparatus—advocated for “nestling intelligence within the United Front” and “using the United Front to push forth intelligence.” As Zhou also reportedly pointed out, “intelligence work should be done by making friends and talking to each other, building bases, establishing relationships, and going deep into society.”¹³ These are all core elements of united front work in the modern era.

THE UNITED FRONT IN ACADEMIA

Over the past decade, concerns about China's influence within global higher education have steadily increased. This has included scrutiny

of the Chinese government-funded Confucius Institutes on campuses worldwide. The Chinese government established the Confucius Institute program in 2004. Hanban, a Chinese government agency chaired by a member of the Politburo and the vice premier of China, oversees the program. Its goals are to promote Chinese language and culture, support local Chinese teaching overseas, and facilitate cultural exchanges.¹⁴

However, Confucius Institutes have stifled open and free debate. Hanban hired and trained teachers to oversee academic courses within U.S. universities, and research proposals had to be approved by Hanban.¹⁵ Numerous examples of censorship began to emerge by Confucius Institutes across the globe—such as in Sweden, Portugal, Australia, and Canada—stifling discussion in classrooms and at conferences.¹⁶ Hanban instructed teachers in Confucius Institutes to prevent the discussion of issues that were politically taboo in China, such as the status of Taiwan, the 1989 Tiananmen Square massacre orchestrated by PLA forces, human rights, China's pro-democracy movement, and the status of China's beleaguered Uyghur population.¹⁷ Marshall Sahlins, an anthropology professor at the University of Chicago, argued that “by hosting a Confucius Institute, they [universities] have become engaged in the political and propaganda efforts of a foreign government in a way that contradicts the values of free inquiry and human welfare to which they are otherwise committed.”¹⁸

Some U.S. intelligence and law enforcement officials also expressed alarm that the MSS was using Confucius Institutes to recruit spies and collect intelligence on Chinese individuals in the United States. “The Chinese have multiple goals with Confucius Institutes, including to monitor Chinese communities in the United States and other Western countries,” said the Central Intelligence Agency (CIA)'s Mark Kelton. “The Chinese have also been interested in influencing the tone of debate on campuses and traditional espionage—including spotting and recruiting individuals.”¹⁹ James Olson, chief of counterintelligence at the CIA, explained that China's MSS “has an elaborate spotting program to identify those students who show political or cultural sympathy for China.”²⁰ By 2009, there were 90 Confucius Institutes housed at U.S. universities—including prestigious institutions such as Columbia, Stanford, and Chicago—and a total of 440 across the globe.²¹ But widespread national security and other concerns about Confucius Institutes led to a substantial reduction in the number of these entities operating on campuses in the United States and abroad.²²

Other united front activities targeting higher education include pro-China campaigns, particularly through various Chinese cultural and academic exchange initiatives. These united front activities integrate tools to intimidate and punish enemies, as Beijing deploys an increasingly strident and aggressive approach to shaping and controlling narratives around issues the CCP views as sensitive. These activities manifest in a wide range of global incidents—including in Australia, the United Kingdom, and the United States—in which Chinese government entities and proxies have engaged in acts of intimidation, harassment, and censorship targeting both Chinese nationals and students and faculty who are critical of Chinese policy on topics such as Taiwan, Hong Kong, Xinjiang, the South China Sea, and Tibet.

A key factor in the threat to higher education is the financial dependency that some universities have on various forms of Chinese funding. According to a U.S. Department of Education (DOE) database documenting foreign donations, China is the fifth-largest foreign source of financial contributions to U.S. universities, accounting for more than \$2.8 billion in grants and contracts since 1987. As acknowledged by the DOE in 2021, however, these numbers are “systematically underinclusive and inaccurate,” as existing obligations only require donations that exceed \$250,000 in a calendar year to be reported. The DOE referred to existing reporting as “unaudited, self-reported data” and suggested that “the public have real reason for concern that foreign money buys influence or control over teaching, research, and possibly even U.S. government policy.”²³ A 2019 U.S. Senate investigation corroborated the DOE’s contention, finding that nearly 70 percent of U.S. schools that received more than \$250,000 to establish Confucius Institutes did not report the donations to the DOE.²⁴

Foreign student tuition is also a critical source of revenue for many U.S. colleges and universities, as these students—including Chinese students—often pay full tuition. In some cases, such arrangements have created significant financial dependencies and, as fewer Chinese students have sought U.S. visas following the Covid-19 pandemic, many universities have experienced declines in Chinese student populations and the corresponding revenue. For several U.S. universities, the decline in Chinese students may have decreased revenue by more than \$20 million per year.²⁵

This level of financial dependence creates conditions where Chinese united front and information

activities may be more impactful. As discussed throughout this report, Beijing is increasingly weaponizing its global market power to control speech on topics that it deems sensitive. China’s ability to inflict financial harm has contributed to several university decisions to comply with Beijing’s efforts to suppress unwelcome narratives and debate. This includes incidents such as the University of Sydney’s 2013 effort to withdraw support for an on-campus speech by the Dalai Lama, despite having hosted a lecture the year before about the Dalai Lama that was sponsored by the campus’s Confucius Institute. After widespread negative attention, the university reversed course and allowed the speech.²⁶

Investigations in Australia, the United Kingdom, and the United States have uncovered several methods that the CCP leverages to shape perceptions and control speech on university campuses. Many of these threats reflect the long arm of the Chinese party-state, which works through multiple united front affiliated organizations—including Chinese Student and Scholars Associations (CSSAs), the Western Returned Scholars Association, and party cells on foreign university campuses—in coordination with components such as the MSS, MPS, and Central Commission for Discipline Inspection to monitor and threaten students suspected of speaking out on sensitive topics. Speaking before the Western Returned Scholars Association in 2013, Xi Jinping admonished: “Everyone must remember: no matter where you are, you are sons and daughters of China.”²⁷

As documented in a testimony before an Australian parliamentary committee and similar studies in the United States and United Kingdom, this policy stance has resulted in cases where Chinese students are harassed or intimidated by fellow students or reported to the Chinese consulate or embassy. Chinese law enforcement and security agencies assist by intimidating or threatening the China-based families of overseas students. Students have also been jailed after returning to China because of social media posts they made while studying abroad.²⁸

Efforts by the state security services and the CCP to exercise control over overseas Chinese students and discussions on the campuses where they study is augmented by various united front entities, such as the CSSAs that operate on hundreds of university campuses worldwide. While CSSAs provide important services to students studying abroad, they have also been directly tied to efforts to amplify Chinese messaging or suppress freedom

of expression. In one 2022 example, the CSSA at George Washington University launched a series of protests after posters created by an Australia-based Chinese dissident artist appeared on campus. The posters, which were designed to raise awareness of Chinese human rights abuses in connection to the 2022 Beijing Winter Olympics, were decried by the CSSA as “a naked attack on the Chinese nation” and purportedly reflected “extremely vicious attacks on all international students from China and Asian groups.”²⁹ The university’s president responded by ordering the posters removed. He later reversed this position after widespread condemnation because of the posters’ origin as a form of political protest.³⁰

CSSAs are often mobilized to denounce critics, stage counterprotests, or greet visiting Chinese dignitaries. A Chinese diplomat who defected to Australia in 2005 claimed that CSSAs “are in fact controlled by the Chinese [diplomatic] mission and are an extension of the Chinese communist regime abroad.”³¹ This contention is supported by various incidents, including disclosures on various CSSA websites and the acknowledged collaboration in 2017 between the CSSA at the University of California, San Diego and the Chinese Consulate in Los Angeles to protest the Dalai Lama speaking at the university’s commencement.³²

Although the CCP’s efforts to suppress freedom of expression and speech on global university campuses represent the most acute united front threat to higher education, united front work extends onto university campuses in other ways that are more reflective of China’s soft-power strategy. Globally, there are numerous groups—similar to the Confucius Institutes—that focus on promoting friendship and telling China’s story. One notable example of how these programs work can be observed in the activities of an organization associated with the united front known as the China-U.S. Exchange Foundation (CUSEF).

CUSEF was founded in 2008 by Tung Chee-hwa, a Hong Kong-based billionaire, “to encourage constructive dialogue and diverse exchanges between the people of the U.S. and China.”³³ Tung, a former chief executive of Hong Kong, is a vice chairman of the Chinese People’s Political Consultative Conference, the CCP body that provides overall strategic guidance to the UFWD. CUSEF sponsors several programs in the United States, some of which are disclosed under the Foreign Agents Registration Act (FARA). These include work conducted on behalf of CUSEF by a U.S. firm that arranges CUSEF-sponsored travel to China for presidents and students from historically Black colleges and universities (HBCUs), as well as to

manage a free Mandarin-language course of study for HBCU students.³⁴ Other CUSEF activities have included funding various initiatives, research, and events at universities and think tanks. Although some involved in these efforts attest that CUSEF put no specific conditions or limitations on funding, other experts such as Peter Mattis suggest the intent is to pursue “ecological change.” As Mattis noted, “If they cultivate enough people in the right places, they start to change the debate without having to directly inject their own voice.”³⁵

POLITICAL INFLUENCE AND INTERFERENCE

The soft-power approach to united front work of groups such as CUSEF is particularly relevant to CCP efforts to influence domestic political discourse in foreign countries. This includes additional work by CUSEF—working through another FARA-registered foreign agent—to arrange travel for former members of U.S. Congress to China “on educational trips to exchange views on U.S.-China relations.” In addition to facilitating travel, this representative works with CUSEF to engage with other influential Americans, such as current and former members of Congress and their staff and conducting “policy and political intelligence gathering and analysis on China issues.”³⁶

Another Chinese-affiliated entity, the U.S.-China Transpacific Foundation, works through the same U.S.-based representative to arrange travel to China for current congressional staff, paying for such travel pursuant to the Mutual Education and Cultural Exchange Act, which allows U.S. government personnel to accept travel paid for by foreign governments. These exchange visits are often co-sponsored by the Chinese People’s Institute of Foreign Affairs, which, according to its mission statement:

... [is] guided by Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era and Xi Jinping Thought on Diplomacy; is committed to “making friends for the country” by taking concerted actions with China’s overall diplomacy, expanding foreign exchanges, telling Chinese stories, promoting interaction between China and the rest of the world, and facilitating the building of a community with a shared future for mankind.³⁷

As such, the development of these exchange programs can be directly correlated to China’s broader united front work.

Beijing also pursues broader campaigns of foreign political influence and interference that are closely tied to the united front. In the United States, Australia, the United Kingdom, and across continental Europe, China conducts a range of political influence activities via several united front-affiliated organizations. In some circumstances, these activities can be interpreted as efforts in long-term seeding and influence. As Federal Bureau of Investigation (FBI) director Christopher Wray argued in 2022: “The Chinese government understands that politicians in smaller roles today may rise to become more influential over time. So they look to cultivate talent early—often state and local officials—to ensure that politicians at all levels of government will be ready to take a call and advocate on behalf of Beijing’s agenda.”³⁸

China’s efforts to influence domestic politics emerged as a firestorm after events in 2016 revealed several links between CCP money and Australian politicians. The most prominent case involved billionaire property developer Huang Xiangmo, who moved from China to Australia in 2011. In the weeks leading up to the 2016 federal elections, Xiangmo and Australian senator Sam Dastyari came under scrutiny after Dastyari spoke at a press conference organized by the Australian Council for the Promotion of Peaceful Reunification of China.³⁹ The council’s mission is to build relationships and promote messaging in Australia in support of the reunification of China and Taiwan. It is an official branch of the China Council for Promotion of Peaceful Reunification of China, which is a prominent component of the united front. In reference to territorial disputes in the South China Sea, Dastyari said at the press conference: “The Chinese integrity of its borders is a matter for China, and the role that Australia should be playing, as a friend, is to know, that with the several thousand years of history, thousands of years of history, where it is and isn’t our place to be involved.”⁴⁰ Dastyari’s remarks parroted a common CCP talking point and were in direct contradiction to the position taken by Labor Party shadow minister Stephen Conroy just the day before, who had sharply criticized China’s island building and pledged that a Labor government would support freedom of navigation operations.⁴¹

Dastyari initially denied making the remarks, but recordings released in 2017 confirmed that he did. Although no laws were broken, the event and Dastyari’s association with Xiangmo sparked political backlash that led to Dastyari apologizing and resigning from his position within the party. A series of ensuing media investigations revealed

that Xiangmo had previously paid legal bills for Dastyari and threatened to withhold a \$450,000 donation to the Labor Party if it did not soften its stance on China’s activities in the South China Sea.⁴² In the end, Dastyari resigned from parliament in December 2017 after it was revealed that he had alerted Xiangmo to the possibility that his phone was being monitored by Australian and U.S. intelligence agencies.⁴³ Huang Xiangmo’s Australian residency was canceled in 2019 over concerns about his political donations and connections to the united front.

In response to the Dastyari affair and other similar controversies, Australia passed a series of campaign finance, counter-interference, and espionage laws. In July 2022, a Chinese man accused of planning foreign interference was committed to stand trial in Victoria’s County Court.⁴⁴ Di Sanh Duong was the first person to be charged under Australia’s new foreign interference laws, and his case provides the first test of the scope of the law, which criminalizes the intent to interfere with Australia’s political institutions or support the intelligence activities of a foreign government.

Similar influence campaigns involving the united front have been identified in the United Kingdom. In January 2022, the United Kingdom’s Security Service (MI5) issued a rare interference alert to the UK parliament warning of a Chinese agent seeking to establish links between the CCP and current and aspiring members. Christine Ching Kui Lee was active in UK political circles for more than a decade, and her law firm made several sizeable donations to members of the UK government. Although none of Lee’s activities were explicitly illegal and she had been on MI5’s radar for several years, the formal alert was issued after she deliberately concealed her connection to the UFWD. Following MI5’s warning, Lee reportedly stepped down from leadership positions of her UK businesses. Speaking on the issue during a joint address with FBI director Christopher Wray in July 2022, director general of MI5 Ken McCallum said, “The UK is a free country and people are free to hold whatever opinions they choose. But if their advocacy of CCP positions is a consequence of hidden manipulation, I would prefer for them—and us—to be conscious of that.”⁴⁵

While the preceding U.S., Australian, and UK examples reflect how China successfully navigates the idiosyncrasies of these legal systems to conduct influence activities without breaking laws, the same cannot be said of other incidents—most notably recent reports of Chinese bribery in the

Solomon Islands. Recent controversies on the islands involving the country's current prime minister, Manasseh Sogavare, have caused political unrest and drawn concern from the United States and others.

Sogavare has served four terms as prime minister of the Solomon Islands. Two of his previous terms were cut short by no-confidence motions, and his current term began amid no less controversy. In 2019, he ran for parliament and eventually became the prime minister after several days of intense backroom negotiations. Shortly after taking office, Sogavare announced that the Solomon Islands would recognize the Chinese government in Beijing, despite having personally called for the UN General Assembly to recognize Taiwan just two years earlier.⁴⁶ This reversal led to accusations that Beijing had influenced Sogavare's return to office. Several members of parliament claim that they were approached with bribes from Beijing to support the decision to recognize China around the same time.⁴⁷ The deputy leader of the opposition, Peter Kenilorea, Jr., claimed he was made an offer of \$1 million to "say nice things about China" and that it was "an open secret that money is always involved in these things."⁴⁸

In late 2021, Sogavare survived another vote of no confidence. Ahead of the vote, the prime minister's office legally distributed \$2.49 million from a national fund to 39 of the parliament's 50 members.⁴⁹ The money in the fund was provided by the Chinese government, who agreed to continue the practice originally established by Taiwan.⁵⁰ Critics argued Sogavare was engaged in vote buying to remain in office and advance China's political interests.⁵¹ Four months later, Sogavare announced that the Solomon Islands had signed a security agreement with China, sparking fears that Beijing was moving closer to establishing military basing on the islands.⁵²

CONCLUSION

As this chapter noted, the activities implemented under the banner of the united front mirror broader patterns of activity that align with China's approach to political warfare. There is a clear pattern of harassment and intimidation that serves a key role in the activities of the united front. The CCP's overarching mission is to consolidate direction and control over all elements of Chinese society. Since the party's founding, the mission of exerting control over individuals and groups that

are not directly subordinate to the party has been the primary purpose of united front work. China's increasingly global ambitions, alongside the onset of the digital age, has dramatically expanded the areas that the party-state views as central to sustaining its unquestioned control over domestic and foreign discourse about China. It is in this area where China's repressive efforts under the banner of the united front are most corrosive.

Extending the party's arm beyond China's borders—to suppress freedom of expression implicitly or explicitly in countries where that freedom is a protected right—is a violation of sovereignty and responsible statecraft. Investigations across academia and civil society suggest that these efforts disproportionately affect diaspora communities, but they also extend beyond direct threats and into forms of self-censorship. In one example, 25 academics in Australia acknowledged that they were hesitant to speak on issues such as Xinjiang and Hong Kong out of fear that they would be recorded, doxxed, or harassed.⁵³ The stakes for diaspora communities are much higher. This can be observed across multiple lines of effort, including in activities carried out under Operation Fox Hunt (as noted in Chapter 3) and in the intimidation and threats that Chinese citizens and their families in the mainland endure when they are perceived as deviating from the party's strict control over thought and speech.

The impact of China's soft-power efforts under the banner of the united front is also difficult to measure. Nevertheless, the evidence suggests that Chinese money and influence can translate into favorable policies, even in Western-style democracies. These soft-power efforts include hundreds, if not thousands, of united front-connected groups that focus on shaping perceptions about China's views on issues of strategic importance, such as reunification with Taiwan, territorial rights in the South China Sea, democracy, and human rights.⁵⁴ Reflecting the integration of multiple tools of national power in support of Beijing's information warfare strategy, the soft-power elements of united front work augment China's public diplomacy, economic development, and perception management efforts.

Multiple investigations of political influence and interference in Europe further underscore how various state organs, such as elements of the Ministry of Commerce and MFA, align with non-state actors operating under various united front banners to build networks of influence at the national and subnational levels.⁵⁵ This includes synchronizing the domestic political activities of

overseas united front organizations (such as the All-China Federation of Returned Overseas Chinese, the Council for the Promotion of the Peaceful Reunification of China, and the Soong Ching Ling Foundation) with overseas state media and China's bureaucratic organizations (such as the MFA's Chinese People's Association for Friendship with Foreign Countries and the Ministry of Commerce's China Council for the Promotion of International Trade). Ultimately, these efforts are designed to promote positive perceptions of China's strategic efforts, focusing on cultivating influential voices and decisionmakers across all elements of society, often integrating economic benefits and other enticements like the bribes used in the case of the Solomon Islands.

"Constructing a maritime superpower" is an important component of the cause of socialism with Chinese characteristics in the new era, and is the essence of Xi Jinping's maritime strategy, which has been developed on the basis of thinking on the seas by successive generations of collective leadership.

-Jia Yu and Zhang Xiaoyi¹

IRREGULAR MILITARY ACTIONS



“建设海洋强国”是新时代中国特色社会主义的重要组成部分，是在历代领导集体海洋思想基础上发展而来的习近平海洋战略思想的精华。

-贾宇 张小奕²

Equipped with a spiral of sharp, gnawing metal teeth and measuring 140 meters (459 feet) in length and 2,800 tons in deadweight, the *Tian Kun Hao* is the largest ship of its kind in Asia.³ As the ship sets to work, it lowers its steel-tooth-lined cutter head into the sea floor—up to 35 meters below the surface—and tears apart the earth, breaking through anything from soft clay to solid rock at a rate of 6,000 cubic meters per hour.⁴ The resulting sand is pumped up and out of the water, then sent to be used in a variety of ways, from components of concrete and mortar for buildings to the foundations of artificial island chains. This operation, however, is far from just a technologically advanced construction project; it is also an example of political warfare.

This chapter examines Chinese irregular military activities, which are an important part of political warfare. As used here, irregular military actions consist of activities short of conventional warfare that are conducted by forces linked directly or indirectly to the state and that are designed to expand a country's influence and legitimacy. As highlighted later in this chapter, one example is the use of sand dredgers—rather than destroyers or battleships—to build islands in disputed territory and turn them into military bases. Irregular military activities appeal to China because they enable Beijing to expand its geopolitical power and influence—including terri-

torial claims—in a manner that avoids provoking major pushback from other states or escalation into conventional warfare. This chapter considers actors such as the People's Liberation Army (PLA), PLA Navy (PLAN), the PLA Air Force, the PLA Rocket Forces, and the People's Armed Forces Maritime Militia (PAFMM), as well as private security companies and other non-state actors.

China's irregular military capabilities are closely tied to the nation's growing emphasis on maritime power and reach, which is deeply rooted in its understanding of both Western and Chinese history. China views itself as one of the first nations to leverage the power and resources of the sea. Chinese historical accounts and state rhetoric typically trace this thread to Guan Zhong, a high-ranking philosopher who lived from approximately 720 to 645 BCE. He advised that the Qi state should pursue a “monopoly on mineral and maritime resources” (唯官山海为可耳), which led to comprehensive economic, political, military, and cultural development.⁵ Furthermore, the Chinese government completed a study in 2006, titled *The Rise of Great Powers*, that assessed the reasons for the ascent of nine Western nations to “great power” status. The study's conclusions linked state power to economic development resulting from trade and facilitated by naval power—highlighting the importance of maritime economic connections.⁶

As Xi Jinping argued to the Eighth Collective Study Session of the Chinese Communist Party (CCP)

Politburo in 2013, “Historical experience tells us that orienting to the ocean will lead to prosperity, while abandoning the ocean will lead to decline. A strong country is a strong maritime power, and a weak country is a weak maritime power.”⁷ He therefore argued in favor of building China into a maritime superpower, which would be strong and outward looking. It would aim to secure China’s local security and sovereignty claims as well as to expand and protect Chinese economic and geopolitical interests abroad.

As a result, China’s maritime strategy rests on the concepts of “near-seas defense” (近海防御) and “far-seas protection” (远海防卫). Although these ideas were publicized in 2015 as the strategy of the PLAN, they also appeared in earlier Chinese strategic documents and were largely inspired by the ideas of Mao Zedong and Alfred Thayer Mahan.⁸ Near-seas defense refers to efforts to secure and defend territorial claims, while far-seas protection encompasses “distant ocean mobile operations and non-warfare military activities” that serve to spread and protect Chinese geopolitical and economic influence globally.⁹ Chinese strategists have typically defined the far seas as the waters beyond the First Island Chain.¹⁰

The dichotomy between near and far seas does not imply full, systematic coordination of strategy, either within each realm or across the two. In fact, the concept of a “unified maritime strategy” (海洋战略) is relatively rare within Chinese strategic analyses, and coordination across maritime operations has only begun to improve in recent years.¹¹ The juxtaposition between near and far seas in this analysis also is not intended to imply that all irregular military activities must be maritime. Still, it is a useful framing device to understand how Beijing conceptualizes its spheres of power, particularly as the country increasingly turns to irregular activities both to enforce its territorial claims near the mainland and to spread influence and power abroad.

While many past analyses of Chinese irregular activities focus on Beijing’s activities in and around the South and East China Seas and territorial disputes with neighboring states, this chapter expands the scope of activities assessed to include military-linked channels through which Beijing advances geopolitical goals further abroad. This includes the role of private security companies in advancing China’s Belt and Road Initiative (BRI), research efforts that feed directly into Chinese strategic goals, and China’s newest international project: the Global Security Initiative.

Most of China’s irregular military activities rely on allegedly routine military activities and commercial entities, enabling Beijing to spread power and influence under a guise of deniability. The majority of these activities, including those that rely on civil-military fusion, are not illegal and can pass as routine economic activity, research, or statecraft. Xi Jinping perceives “civil-military fusion” (军民融合) as a key component of China’s strategic advancement.¹² In his address to the 19th Party Congress, he pledged to “deepen reform of defense-related science, technology, and industry, achieve greater military-civilian integration, and build integrated national strategies and strategic capabilities.”¹³ During his address to the 20th Party Congress, Xi similarly vowed to “better coordinate strategies and plans, align policies and systems, and share resources and production factors between the military and civilian sectors.”¹⁴ Furthermore, the emphasis on companies and other economically driven actors as tools of strategic advancement is also connected to China’s perception of economic development and advancements in technology as the key drivers of interstate competition.¹⁵

The number and diversity of these efforts are highly concerning and may become more threatening as China increasingly focuses on global ambitions, such as its newly formulated Global Security Initiative. While it is possible to comprehensively examine the state of Chinese activities in, for example, the South China Sea, it becomes increasingly difficult to track and counter the totality of Chinese political warfare efforts on a global scale. Still, the absence of centralized, strategic oversight to coordinate these diverse and deniable activities may limit their effectiveness.

This chapter draws on a variety of primary and secondary sources, including Chinese research publications, government white papers and press releases, and speeches by officials; analysis and data reported by U.S. and partner governments and research institutions; satellite imagery; and a new CSIS-created data set of Chinese private security companies operating abroad, including their locations and primary services.

The remainder of this chapter is divided into three main sections. The first section provides an overview of China’s primary near-seas activities, including the use of sand dredgers; coercion through military exercises, harassment campaigns, and forward deployments; the PAFMM; and electronic warfare. The second assesses China’s main far-seas activities, including private security companies, strategy-driven research, and the Global Security

Initiative. The final section provides a brief analysis of recent trends in Chinese irregular military activity and their implications for the United States and its partners.

NEAR-SEAS ACTIVITIES

China's near-seas activities primarily focus on maintaining or securing its claims of sovereignty in the South and East China Seas—the world's most contested waters. Despite Beijing's phrasing of near-seas *defense*, the majority of these activities are offensive, justified by the CCP as constituting a response to existential threats. In the same speech in which Xi Jinping declared that China would become a maritime superpower, he explained:

On the one hand, we must persist in resolving [territorial] disputes through peaceful methods and negotiation methods. . . . On the other hand, we must be prepared to deal with various complex situations, strengthen the building of forces for the protection of maritime rights and law enforcement, accelerate the pace of construction of a modernized navy, improve maritime rights protection capabilities, and resolutely safeguard China's maritime rights and interests. We love peace and adhere to the path of peaceful development, but we must never give up our legitimate rights and interests, let alone sacrifice our country's core interests.¹⁶

China is willing to push the boundaries of “peaceful methods” when disputes threaten what the state believes to be its legitimate and core interests. In order to avoid broader military escalation, however, China typically aims to maintain or secure its territorial claims through irregular means.

This section outlines four such irregular methods: the use of sand dredgers; military exercises, harassment campaigns, and forward deployments; the PAFMM; and electronic warfare. It examines the nature of these methods and their relationship with the Chinese government,

examples of recent activity, and the results and implications of their use to further China's near-seas goals. These military-linked activities are also frequently accompanied by actions in the legal and information spaces.

SAND DREDGERS

Sand dredgers, such as the *Tian Kun Hao* discussed at the beginning of this chapter, are specialized pieces of equipment that use cutter bars or drills on booms to break up the dirt and rock at the bottom of a body of water and then remove and transport the resulting sand and debris for processing and use in various construction projects.¹⁷ Figure 7.2 depicts the typical components of this process.

Prior to the 2017 unveiling of the *Tian Kun Hao*—described by its designers as a “magical island-maker”—the crown jewel of Beijing's dredging fleet was the *Tian Jing Hong*, which measures 127 meters (417 feet) long and weighs 2,400 tons.¹⁸ Over the past decade, this self-propelled cutter suction dredger spearheaded many of China's geographic construction projects in the disputed

Figure 7.1

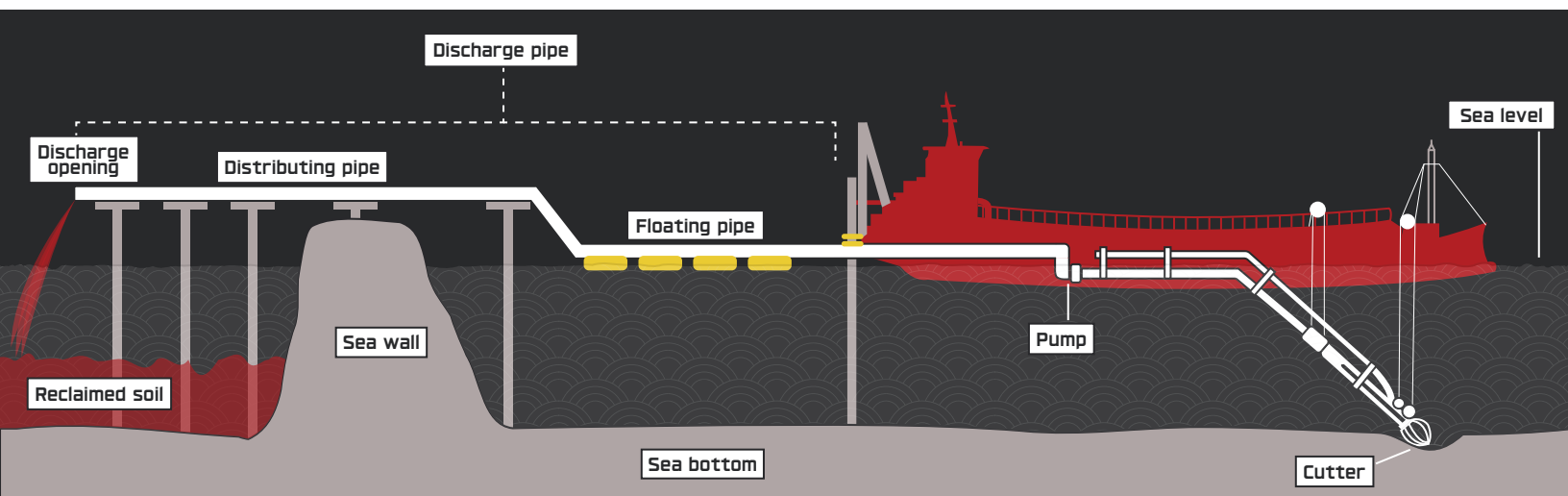
Disputed Territorial Claims in the South and East China Seas



SOURCE: CSIS RESEARCH AND ANALYSIS. NOTE: LINES DENOTING TERRITORIAL CLAIMS ARE NOT EXACT.

Figure 7.2

Diagram of a Common Sand Dredging Operation



SOURCE: CSIS RESEARCH AND ANALYSIS.

waters of the South China Sea. In addition to these enormous vessels, Beijing maintains a fleet of smaller dredging vessels.

Dredging activities in the water near China and disputed territories have been directly orchestrated by the Chinese government, and Beijing has defended these projects from international criticism across multiple domains. For example, after marine biologists in the United States and other nations criticized China's island-building project for having devastating effects on local ecosystems, the Chinese government repeatedly defended its efforts as being environmentally friendly.¹⁹ The State Oceanic Administration claimed in 2015 that during these projects, "ecological environmental protection and engineering planning, design, and construction are carried out simultaneously."²⁰ Similarly, a spokesperson for the Ministry of Foreign Affairs (MFA) claimed the following year that the construction activities "strictly follow the principle of conducting green project [sic]" and are "[b]ased on thorough studies and scientific proof."²¹ International scientific consensus indicates the opposite of these statements.²²

China has pursued two major types of activity using sand dredgers in recent years: artificial island construction and land theft.

First, China has used its dredgers to construct manmade islands in the East and South China Seas, which it then militarized as part of ongoing efforts to assert its claims of sovereignty. Settlements and military installations on these artificial

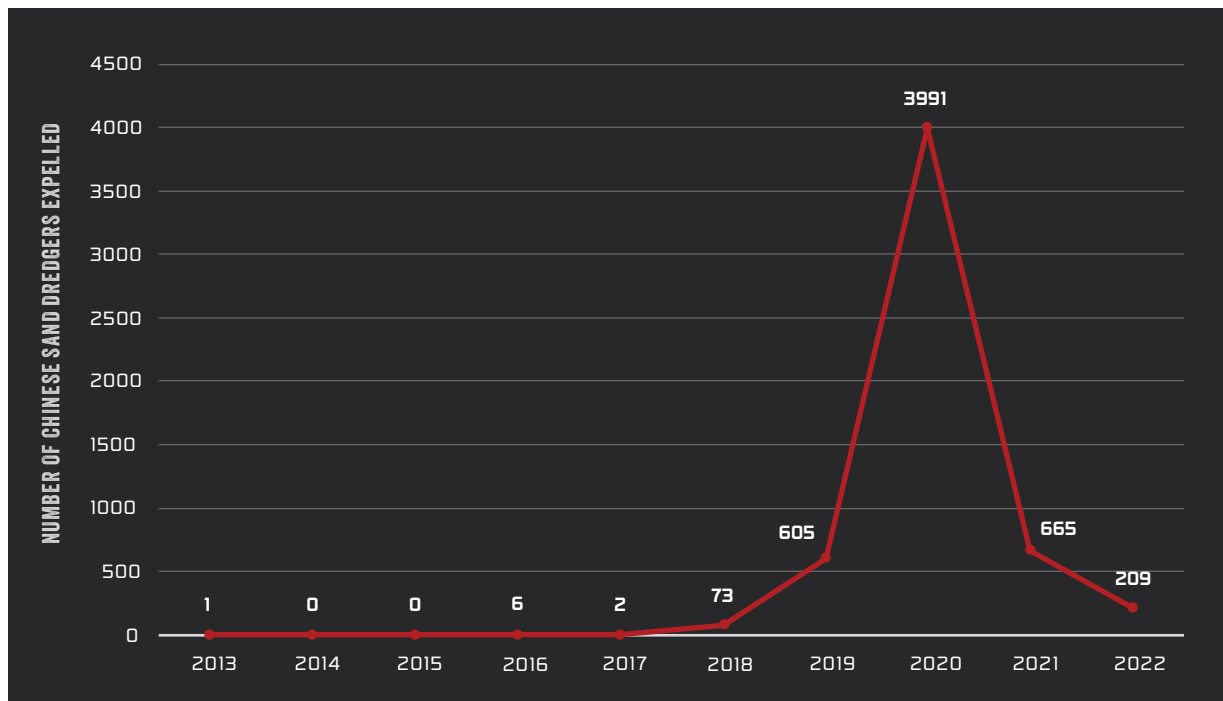
islands permit Beijing to expand the area in which it claims to hold exclusive economic zone (EEZ) jurisdiction. Since 2013, China has created 3,200 acres of land in the Spratly Islands.²³ For example, in early 2015, clusters of Chinese dredgers pulled sand from the seabed and deposited it onto the sparse, undeveloped atoll at Mischief Reef in the eastern Spratly Islands, an area reportedly rich in undeveloped gas and oil resources.²⁴ Once the land itself was constructed, China set to work establishing military facilities and equipment on the new artificial island, including an airfield and control tower, radar installations, HQ-9B surface-to-air missiles, and YJ-12B anti-ship cruise missiles.²⁵ Beijing has followed a similar process with other artificial islands in the area.

Second, China has used its sand dredgers to, quite literally, steal land over which it has asserted sovereignty. Driven largely by mainland cities' efforts to build skyscrapers and large-scale projects such as the construction of the Beijing Daxing International Airport, China has begun to meet its construction industry's demand for sand by directly harvesting it from Taiwanese coastal territory and outlying islands.²⁶ To fend off these Chinese incursions and thefts, the Taiwanese coast guard uses radar, watch, and patrol screens, and it has increasingly deployed large patrol ships over the past decade to deter and expel Chinese dredgers.²⁷

As shown in Figure 7.3, there was a dramatic increase in the number of Chinese sand dredgers expelled from Taiwanese waters in 2020, according to data compiled by the Taiwanese coast guard. In 2019,

Figure 7.3

Number of Chinese Sand Dredgers Expelled by the Taiwanese Coast Guard, 2013–2022



SOURCES: “表11-1 其他海巡績效統計—按月份分(續2完)” [TABLE 11-1 THE STATISTICS OF OTHER BUSINESS PERFORMANCE—BY MONTH (CONT.2, END)], 110年海巡統計年報 [110TH COAST GUARD STATISTICAL ANNUAL REPORT], 海洋委員會海巡署 [COAST GUARD ADMINISTRATION OF THE OCEAN AFFAIRS COUNCIL], ACCESSED NOVEMBER 4, 2022, [HTTPS://WWW.CGA.GOV.TW/GIOPEN/WSITE/PUBLIC/ATTACHMENT/F1649862332064.PDF](https://www.cga.gov.tw/GIOPEN/WSITE/PUBLIC/ATTACHMENT/F1649862332064.PDF); AND “表11-1 其他海巡績效統計—按月份分(續2完)” [TABLE 11-1 THE STATISTICS OF OTHER BUSINESS PERFORMANCE—BY MONTH (CONT.2, END)], 111年12月績效統計月報 [111TH DECEMBER PERFORMANCE STATISTICS MONTHLY REPORT], 海洋委員會海巡署 [COAST GUARD ADMINISTRATION OF THE OCEAN AFFAIRS COUNCIL], ACCESSED FEBRUARY 13, 2023, [HTTPS://WWW.CGA.GOV.TW/GIOPEN/WSITE/PUBLIC/ATTACHMENT/F1675667173017.PDF](https://www.cga.gov.tw/GIOPEN/WSITE/PUBLIC/ATTACHMENT/F1675667173017.PDF)

the coast guard reported 605 expulsions—already more than an eightfold increase from 2018. But in 2020, the total number of expulsions skyrocketed to 3,991. The number of incidents has decreased but remains higher than the historical norms, with 665 reported in 2021 and 209 in 2022.²⁸

Although there is no definitive explanation for the sudden increase in Chinese sand dredger expulsions in 2020, this surge correlates with a period of rapid infrastructure development in China driven by Covid-19 recovery policies. The resulting high demand for sand to facilitate construction projects could explain the timing of the peak in 2020. Following the outbreak of Covid-19, Chinese GDP dropped 6.8 percent in the first quarter of 2020—the largest year-on-year decrease it has ever experienced.²⁹ In April 2020, the Politburo requested efforts “expanding effective investment, strengthening investment in traditional and new infrastructure, expediting upgrades to traditional industry, and expanding investment in emerging strategic industries” in order to mitigate economic harms from the pandemic.³⁰ The Chinese government defined infrastructure broadly to

include information infrastructure, big data and computing capabilities, research and development, and more traditional construction projects, including railways, dams, undersea tunnels, and large-scale water transfer projects.³¹ This likely drove a significant increase in demand for sand to support construction efforts. China was likely already facing growing demand for sand due to other infrastructure projects with development timelines within this time period as well, such as the Xiamen Xiang'an Airport, which is expected to be completed in 2025.³²

The majority of these incursions have occurred in Penghu and Lienchiang Counties. Of the 3,991 expulsions by the Taiwanese coast guard in 2020, for example, 3,422 (86 percent) occurred in Penghu County and 552 (14 percent) occurred in Lienchiang County, while less than 1 percent of incidents in 2020 occurred elsewhere in Taiwanese waters.³³ The geographic positioning of these islands is significant both because their proximity to mainland China would make them early targets during a potential invasion of Taiwan and because it may provide clues to Beijing's intent. Lienchiang

Figure 7.4

Chinese Sand Dredging Operations and Military Installations at Mischief Reef, 2015–2020

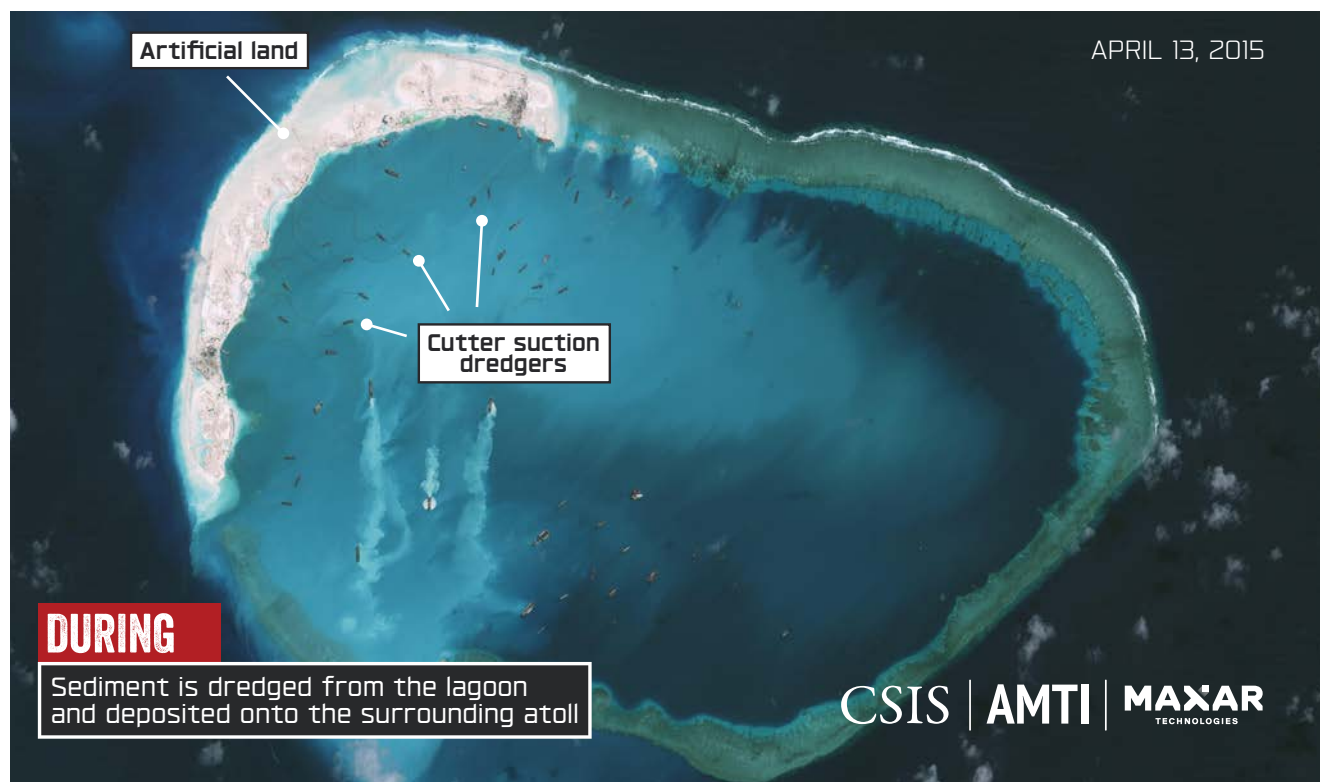
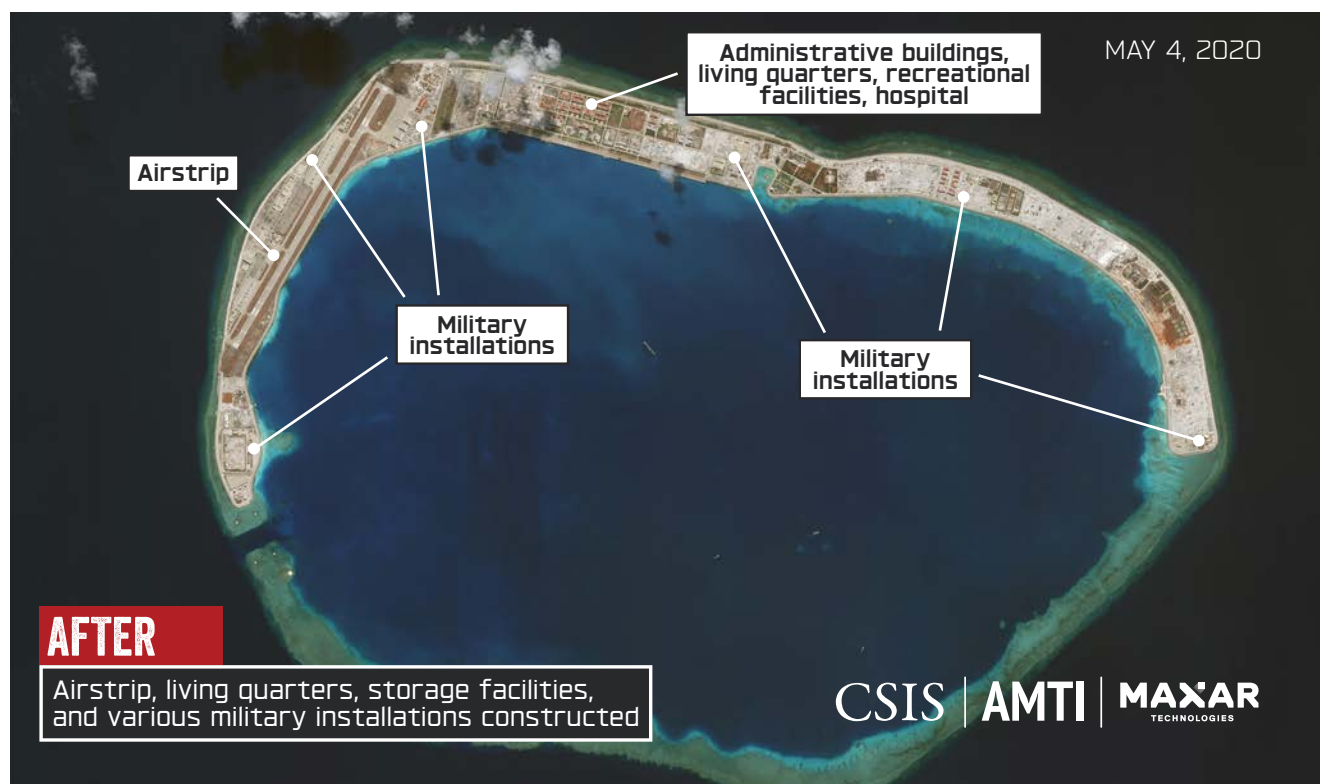


Figure 7.4

Chinese Sand Dredging Operations and Military Installations at Mischief Reef, 2015–2020



County—otherwise known as the Matsu Islands—is located northwest of Taiwan’s main island in the East China Sea, a short distance from Fuzhou on the Chinese coast. Penghu County, consisting of the Penghu Islands, is located in the Taiwan Strait approximately 50 km west of the main island. By violating Taiwanese waters in these two counties, China moderates the threat it poses—escalating tensions far less than if it routinely approached the main island—while still gaining efficient access to Taiwanese sand. Beijing is also involved in a secretive build-up on Myanmar’s Great Coco Island, including an expanded airstrip, aircraft hangars, and radar equipment.³⁴

Chinese island building advances Beijing’s goals to project military power and to defend or reassert sovereign claims, particularly in the South China Sea and surrounding waters. By expanding its presence and capabilities in the region, China aims to coerce other claimants to abandon their rights over maritime areas or islands in favor of Chinese control.³⁵ Furthermore, by establishing artificial islands with facilities and basing, China has expanded the reach of its claimed EEZs, which now ostensibly can be measured out from the shores of these islands as well. China continues to flout international laws

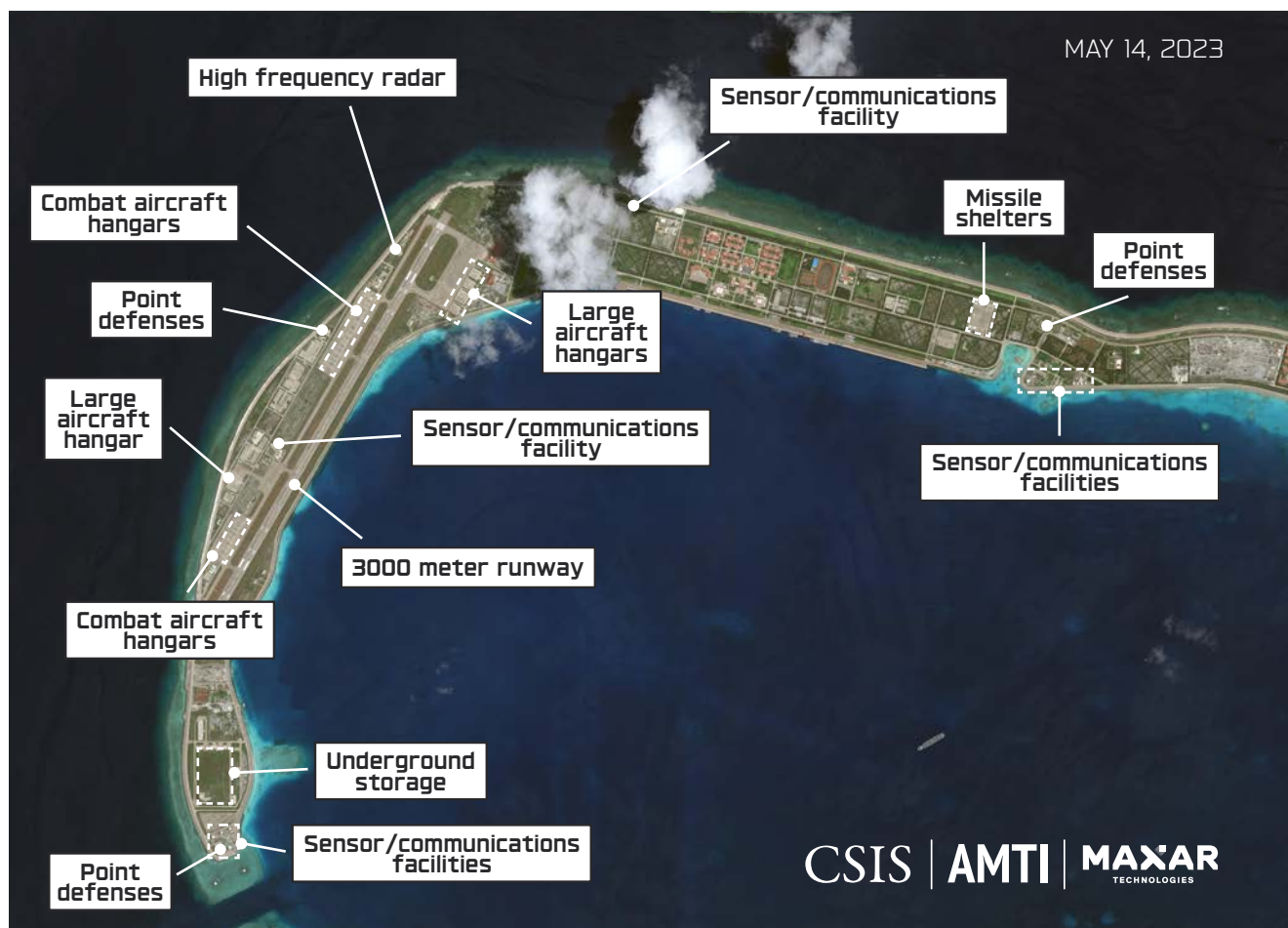
concerning sovereignty and maritime activities as part of a broader “lawfare” campaign to erode trust in the existing international order and norms and to instead shape the international legal environment to better fit its own needs. Lawfare involves the exploitation of international and domestic law to assert the legitimacy of a country’s claims.

Aside from accessing sand necessary for construction purposes—China uses 40 percent of global sand aggregates annually and has used more sand in the past four years than the United States has over the past century—the Chinese dredger incursions in Taiwanese waters are likely an effort to harass Taiwan, exhaust its civilian coast guard, and disrupt its economy.³⁶ In addition to losing sand—one of Taiwan’s most valuable maritime resources—Chinese dredger activities have forced Taiwan to divert and overextend coast guard patrols and monitoring, increase expenses to expand coast guard capabilities, and risk physical aggression when confronting intruding vessels.³⁷

Chinese dredging activities also have substantial negative impacts on the local ecosystem and may therefore violate Chinese commitments under the UN Convention on the Law of the Sea, which

Figure 7.5

Chinese Military Installations at Mischief Reef, 2023



it ratified.³⁸ This is not Beijing's first attempt to selectively apply the UN convention, and it serves as an example of Chinese lawfare. By continuing to violate international law, Beijing seeks to cast doubt on the interpretation or legitimacy of previously decided international legal standards and norms in pursuit of a new order of its own making.³⁹

MILITARY EXERCISES, HARASSMENT CAMPAIGNS, AND FORWARD DEPLOYMENTS

China regularly uses the threat and disruption that results from military exercises, harassment campaigns, and forward deployments to coerce and intimidate neighboring states and to assert its claims of sovereignty, all under the guise of routine military activity. This section describes the use of each of these activities to advance Chinese interests and provides examples of each.

First, China regularly conducts large-scale, cross-service military exercises that serve as a threat to other regional countries and that frequently block

sea and air lanes and disrupt commercial activity in the South China Sea.⁴⁰ These are often strategically timed to serve as retaliation or punishment. In August 2022, for example, Beijing initiated its largest-ever military exercise—including the use of fighter jets, military helicopters, anti-submarine aircraft, combat ships, and Dongfeng-class ballistic missiles—around Taiwan in response to U.S. House speaker Nancy Pelosi's visit to Taiwan, which China perceived as a violation of its sovereignty.⁴¹ This exercise served not only as an overt signal that China rejects Taiwan's sovereignty but also disrupted 18 flight paths as well as commercial shipping routes used by manufacturers of semiconductors and other electronics.⁴²

The PLAAF, PLAN, China Coast Guard (CCG), and other PLA-linked forces also conduct patrols and air operations—including with unmanned aircraft systems (UASs)—in disputed territories. Through these efforts, the Chinese military has regularly harassed commercial activities, including around the Spratly Islands, Taiwan Strait, and other locations

in the South China Sea. Beginning in June 2019, for example, CCG patrols harassed and initiated a standoff with Malaysian and Vietnamese vessels conducting surveying and drilling operations in oil and gas fields in the South China Sea.⁴³ The PLAAF has even buzzed—flown over very close and quickly—adversaries’ aircraft, including outside of Chinese airspace. In one case, described by U.S. Air Force brigadier general Pat Ryder in March 2023, a Chinese aircraft flew within 20 feet of a U.S. military plane while in international airspace.⁴⁴

Finally, China regularly forward deploys troops and equipment in disputed territories, including anchoring ships, particularly in the South China Sea. As part of this effort, it also establishes military or dual-use bases on constructed islands, as described earlier in this chapter. For example, Mischief Reef—depicted previously in Figure 7.3—has been fully militarized to include hangars, runways, seaports, warehouses, storage facilities, and radar systems. The facilities are equipped with HQ-9B surface-to-air missiles and YJ-12B anti-ship cruise missiles, close-in weapon system emplacements, Type 022 Houbei-class fast-attack boats, and other military equipment.⁴⁵ Similarly, the PLA has developed and staffed facilities along the disputed China-India border in the Ladakh region to prepare for future conflict, facilitate the logistics of troop and equipment transfers in the disputed region, and intimidate India. In the fall of 2022, for example, despite publicly coordinating with the Indian government for joint withdrawals from the Gogra-Hotsprings border area, China continued to develop and expand its long-term military presence 50 km south of the withdrawal point, at Pangong Tso.⁴⁶

PEOPLE’S ARMED FORCES MARITIME MILITIA

The PAFMM is a fleet of ostensibly commercial fishing ships that operate as an independent reserve force and serve as an “assistant to the PLAN” (解放军的助手) in the South China Sea.⁴⁷ China has used the PAFMM since at least 1974, when militia ships helped to seize the Paracel Islands from Vietnamese control. But the PAFMM escalated its aggression against competitor ships in the 2000s and increased its collaboration with other Chinese forces to enforce claims of sovereignty in the 2010s.⁴⁸ Since China completed a series of artificial island construction projects in the mid-2010s around the Spratly Islands, the PAFMM has regularly participated in law enforcement missions alongside the CCG and People’s Armed Police (PAP) in the region, including in efforts to harass and impede other nations’ commercial vessels.⁴⁹

Although the Chinese government has long defined its militia fleet as “an armed mass organization composed of civilians retaining their regular jobs,” it is important to understand the PAFMM as a direct tool of the government. The PAFMM works in close cooperation with the PLAN, and like all entities operating within China, it is ultimately an instrument for the Chinese government to use to pursue its interests.⁵⁰ Given that the PAFMM has not only survived but sustained a key role in Chinese operations in the South China Sea through an assortment of PLAN modernization efforts, some U.S. experts speculate that Beijing may continue to develop and rely on the PAFMM alongside its other PLAN and CCG forces, and it may even rely on the militia as a cheaper option for low-intensity operations.⁵¹

There are two main types of ships in the PAFMM: professional and commercial. Professional “Maritime Militia Fishing Vessels” (MMFVs, or 海上民兵渔船) are built and equipped for the purpose of carrying out maritime military missions on behalf of the Chinese government. The commercial vessels, or “Spratly Backbone Fishing Vessels” (SBFVs, or 南沙骨干渔船), are owned by small or medium enterprises located along the Chinese coast that meet certain size and power requirements to be eligible to participate in militia activities.⁵² SBFVs receive payment from the Chinese government to remain present in designated disputed waters—typically with minimal crew onboard to reduce costs since the resulting profit renders fishing activities unnecessary—and to assist the PLA as necessary.⁵³

Most vessels that constitute the PAFMM receive at least one type of central or local government subsidy. MMFVs receive subsidies for professional-grade construction, SBFVs receive subsidies for fuel if they operate around the Spratlys, and either type of vessel is eligible for subsidies that cover general construction, communication, navigation, and safety gear.⁵⁴

The PAFMM has grown more assertive over the past decade, and it regularly works alongside the CCG and in coordination with the PLAN to assert China’s sovereign claims in the South China Sea, particularly around the Spratly Islands. As many as 300 PAFMM vessels are active in the Spratly Islands on an average day, and they regularly trespass within EEZs, harass other vessels, and violate various other international laws.⁵⁵

The PAFMM allows China to assert and defend its sovereign claims, secure resources, coerce neighboring states, limit freedom of navigation, and extend its economic and military reach. These actions are all under the guise of civilian fishing

activity, which may limit the threat perception of China's adversaries or their ability to respond to PAFMM activities. Weaker states may hesitate to confront PAFMM vessels out of fear of provoking an aggressive response from China, while stronger powers may hesitate over the risk of inadvertently confronting a civilian vessel.⁵⁶

In early 2019, for example, a fleet of approximately 275 militia vessels surrounded Sandy Cay, a disputed set of three sand bars located near the Spratly Islands and between Thitu Island (occupied by the Philippines) and Subi Reef (occupied by China). To avoid the state-on-state escalation that would occur if an official CCG vessel that routinely patrols the area were to engage a Philippine vessel, civilian PAFMM vessels harassed Philippine ships in an attempt to coerce them to withdraw, which ultimately led the Philippines to denounce China in April 2019.⁵⁷ China refused to withdraw the vessels. But in March 2022, the Philippines launched efforts to begin pushing Chinese vessels out of the waters near Thitu and away from other segments of the Philippine EEZ.⁵⁸

PAFMM vessels are also ideally positioned to assist with intelligence-gathering operations. Their ongoing presence in contested regions enables these vessels to regularly collect intelligence and monitor adversaries' activities. Furthermore, in a combat scenario, their size and minimal signal broadcasts make PAFMM vessels difficult to detect, thus enabling them to conduct reconnaissance missions.⁵⁹

ELECTRONIC WARFARE

Beginning in roughly 2018, China expanded its use of electronic warfare to spoof and jam navigation systems in pursuit of its political interests. Spoofing refers to a technique in which an attacker generates a fake signal and tricks a receiver into believing that the signal is genuine. Jamming refers to the process of generating noise in a specific radio frequency in order to interfere with signals traveling to or from satellites. Broadly, these techniques pose navigational risks, can disrupt shipping lanes, and may conceal criminal activity.⁶⁰ The primary objectives of these activities appear to be to obscure imports and infrastructure in Chinese ports and to force shipping vessels and aircraft away from Chinese territorial claims in the South China Sea.

Beijing has used these types of electronic warfare both at domestic ports and throughout the South China Sea. Shipping vessels have reported patterns of Global Navigational Satellite System (GNSS) spoofing at more than 20 Chinese ports since 2019, including

Shanghai.⁶¹ With China's BeiDou Navigation Satellite System operational, Beijing may be emboldened to interfere more with GNSS since Chinese vessels can instead rely on BeiDou.⁶² Nearly three-quarters of these spoofing operations center on oil terminals, while the remainder include government offices and a major infrastructure company. This obfuscation may be an attempt to conceal imports of Iranian oil and the visits of high-profile government officials.⁶³ In the South China Sea, Chinese government and military facilities—including those installed on artificially constructed territory in locations such as the Spratly Islands and Mischief Reef—have routinely used jamming and spoofing technology since at least 2018 to obscure their presence and to redirect foreign vessels away from contested territory.⁶⁴

These types of electronic warfare technology could also create additional threats beyond the recorded spoofing and jamming incidents. For example, the Chinese military could use manipulated signals to draw a target vessel off course—a technique known as “meaconing”—and instead lure it to an alternative location for nefarious purposes.

FAR-SEAS ACTIVITIES

Chinese far-seas activities use tools similar to those employed in its near-seas operations. But rather than pursuing goals related to defense or sovereignty, these activities aim to advance China's geopolitical and economic reach worldwide, including in Latin America and Africa. This section outlines three such tools: private security companies, strategy-driven research, and the Global Security Initiative. It also examines the nature of these tools and their relationship with the Chinese government, their recent activities, and the results and implications of their use for China's global objectives.

PRIVATE SECURITY COMPANIES

Private security companies (PSCs) include organizations available for hire to provide security and protection services, typically for static personnel and assets or on escort trips. PSCs are not exclusively a Chinese phenomenon, but Beijing has increasingly used them in recent years to protect Chinese nationals and property abroad and to build security-based partnerships, particularly as it continues to expand its BRI investments.

Modern PSCs began to form in China in the early 1990s as a mechanism to protect mainland companies from theft and worker revolts.⁶⁵ Nearly three decades later, more than 5,000 PSCs operate within

China and employ roughly 3 million employees.⁶⁶ After China launched the BRI, both Chinese personnel and assets faced growing security challenges, and the demand for Chinese PSCs also increased globally. As the Chinese Ministry of Commerce explained in its 2018 update to the guidelines that regulate overseas enterprises and personnel:

With China's changing participation in global governance and the implementation of the "Belt and Road" cooperation initiative, the scale of China's outbound investment and cooperation is expanding, and the number of people going abroad each year is increasing. . . . The international situation is increasingly complex and volatile, and various kinds of overseas security risks occur from time to time, which not only affect the overseas operation of our enterprises, but also seriously threaten our overseas personnel. . . . Since 2012, security incidents against Chinese institutions and personnel in high-risk areas abroad have been frequent, and it is urgent to enhance and strengthen the security risk prevention capability of overseas institutions and personnel of Chinese enterprises.⁶⁷

Few of China's domestic PSCs had the capability to shift their work abroad, but the ones that did—roughly 20 companies—increasingly took advantage of the chance to contract with entities linked to the Chinese government and its BRI investments.⁶⁸ Most are relatively small—on the scale of a few hundred or a few thousand personnel—but expansion follows success, and in recent years some companies have grown by acquiring former competitors.⁶⁹ This section focuses only on the activities of Chinese PSCs operating abroad.

PSCs are technically distinct from private military companies (PMCs), which are military contractors for hire, more colloquially thought of as mercenaries.⁷⁰ In practice, however, the distinction can be murky. While PMCs are not legal in China, the CCP formally legalized PSCs in September 2009, and the following year the Ministry of Commerce released strict regulations and requirements to govern PSC activity.⁷¹

Even after the legalization of PSCs, however, legal restrictions on their activities abroad have remained murky. The Ministry of Commerce regulations predominantly govern PSCs' domestic activities. While there are legal restrictions on PSC activities abroad during active conflicts, typical overseas operations remain largely unregulated.⁷² One significant area of ambiguity is contractors' ability to carry firearms. Officially this is forbidden,

but the Chinese government has permitted some PSCs, such as Hua Xin Zhong An (Beijing) Security Services, to do so.⁷³

Chinese government agencies, state-owned enterprises (SOEs), and smaller entities that contract with SOEs regularly employ Chinese PSCs for protection and assistance in their overseas ventures. The size and scope of PSC foreign deployments grew over the past decade alongside BRI activities. Amid this expansion and the heightened demand for security services abroad, the Chinese government and insurance sector began to organize the PSC sector into a more formal, professionalized marketplace. International presence and experience will likely be seen as a boon for professionalizing PSC personnel, many of whom are PLA or PAP veterans who lack the knowledge and managerial skills needed to succeed or Singaporean contractors lacking language fluency and cultural knowledge.⁷⁴ Since the private security sector and the PLA are undergoing reform simultaneously, it is possible that the Chinese government will coordinate further development and restructuring efforts for each to make the two more interoperable.

The Appendix provides examples of major Chinese PSCs that operate outside of China, sample locations in which they have been reported to operate, the types of services they provide, and some of their known clients. This list is not exhaustive, but it is representative of major PSC entities and activities based on open-source information.

As the Appendix indicates, most Chinese PSC activity is focused on supporting other Chinese entities as they operate abroad, with an emphasis on economic and development activities. The companies' tasks focus on defensive security services—including physical security, security training, and security escort services—and consulting on logistics, risk assessment, and emergency response. In Kyrgyzstan, for example, "Zhongjun Junhong" (中军军弘安保集团) has provided security services since 2016, when the car bombing at the Chinese embassy in Bishkek raised concerns about regional security.⁷⁵ Most recently, the PSC contracted with the China Railway Group, which is working to establish the China-Kyrgyzstan-Uzbekistan Railway.⁷⁶ Similarly, in Kenya, "Beijing DeWe Security Service Group" (德威国际安保集团) provides security for China's embassy, and additional support for Chinese-backed development projects in Kenya comes from Zhongjun Junhong, "China Security Technology Group" (中国安保技术集团), "Frontier Services Group" (先锋服务集团), and "Shandong Huawei Security Group" (山东华威保安集团).

The support role of Chinese PSCs stands in stark contrast to Russian PMCs, which often serve as proxies and force multipliers for Moscow, with a growing emphasis on offensive combat training and operations.⁷⁷ As a result, Chinese PSC operations are understudied in the United States and other Western countries. Rather than directly pursuing political and military goals as a substitute for formal military forces, Chinese PSCs facilitate economic and political influence through a security pathway. Chinese security and training services are yet another way to spread trust and influence abroad, particularly with nations that Beijing is already courting through diplomatic and economic partnerships. Even if the activities conducted by a given PSC are not directly related to China's geopolitical goals, they present an additional threat vector that allows Beijing to build nontraditional security and political relationships through market forces. Simultaneously, PSC activities protect Chinese business and economic interests—providing both an additional benefit and a plausible justification for their routine use.

Most significantly, the use of PSCs to secure Chinese personnel and assets enables the longevity of Beijing's BRI investments, most of which are in medium- to high-risk locations in which there has historically been little direct investment. The demand for security services is also unlikely to go away. Regions with heavy BRI presence, including Southeast, Central, and South Asia and East Africa, continue to face instability related to weak governance, terrorism, civil war, and interstate conflict.⁷⁸ Beyond the security threats in these areas, Chinese firms risk being targeted as a result of cultural differences, poor working conditions, or negative externalities of their projects.⁷⁹ By securing its assets in these regions, China is able to continue to reap the benefits of its economic investments—which are explored in greater detail in the next chapter.

STRATEGY-DRIVEN RESEARCH EFFORTS

Although government-supported scientific research is routine and not typically defined as a form of warfare, the CCP's control over the military and all government initiatives has allowed it to operationalize common research methods to gain military intelligence and influence directly connected to its strategic goals. This section details two such efforts: the use of weather balloons and scientific instruments to conduct long-range surveillance, and the use of maritime research efforts to advance China's strategic goals in the Arctic region.

Long-Range Surveillance

Chinese long-range surveillance efforts disguised as scientific research burst into the public eye on February 2, 2023, when the U.S. government publicly identified what appeared to be a weather balloon violating U.S. air space as a high-altitude Chinese surveillance platform.⁸⁰ However, this was not an isolated incident. Similar balloons had passed over the United States in previous years, though none had previously lingered as long as this balloon.⁸¹

U.S. intelligence officers have linked some of these balloon incidents to a broader PLA-led aerospace program that uses airships and balloons, which have been detected operating over five continents.⁸² In the wake of the February 2023 incident, the U.S. government imposed restrictions on U.S. companies with links to the program, effectively denying the PLA use of U.S. technology for future surveillance efforts.⁸³ Still, most of the technology and resources used by the PLA for this project come from a Chinese company that participates in the nation's civil-military fusion initiative, through which private commercial entities develop and produce technology and equipment for the PLA.⁸⁴

Chinese satellites are growing in sophistication and provide extensive coverage of targets of interest within the United States and other countries. Still, balloons and airships offer some advantages: they are cheaper than satellites and can provide persistent overwatch from within the atmosphere, enabling them to gather certain types of information. Additionally, their wayward paths make them more difficult to track, and if they are detected, their appearance as standard weather balloons offers the PLA plausible deniability to conceal surveillance efforts.⁸⁵

Strategy-Driven Maritime Research

China's recent maritime research activities have included an emphasis on seabed resources and polar exploration, both of which will advance Chinese strategic priorities in addition to scientific knowledge. These focuses are aligned with Xi Jinping's instruction to the Eighth Collective Study Session of the CCP Politburo that "[i]t is necessary to carry out in-depth scientific investigations in open ocean and polar regions, carry out deep-sea and far-off-shore surveys and research . . . and make preliminary preparations for the utilization of ocean and polar resources."⁸⁶ The Chinese government controls most of these research efforts, thereby giving the CCP influence over research priorities. The Chinese Ministry of Natural Resources (MNR) owns and operates the

majority of out-of-area oceanographic research vessels that constitute the state's National Marine Research Fleet. The MNR, which reports to the State Council, formed in March 2018 as a merger of the former Ministry of Land and Resources; State Oceanic Administration; National Bureau of Surveying, Mapping, and Geological Information; and miscellaneous components of several other agencies.⁸⁷ In addition to the MNR, the Chinese Academy of Sciences and the China Ocean Mineral Resources R&D Association operate ships within the fleet, as do various Chinese universities.⁸⁸

Deep-sea surveys for energy resources and minerals—particularly polymetallic nodules and sulfides and cobalt-rich ferromanganese crusts—are one of the primary focuses of Chinese maritime research activities. China has focused its resource exploration efforts within a set of four zones in which it obtained contract rights from the International Seabed Authority. These include two areas southeast of Hawaii, one east of Guam, and another southeast of Madagascar.⁸⁹ China's focus on identifying and exploiting natural resources is tied to both its economic goals and ambition to become a global maritime superpower.⁹⁰ By securing a wealth of seabed resources, China can secure its monopoly over rare-earth minerals that are key components of advanced weapons systems and other advanced technology, improve its technological and economic standing, and potentially gain an important advantage in its competition with the United States.⁹¹

China has also increased its research focus on the polar regions, likely as a result of China's Arctic ambitions and strategic interests. In January 2018, the State Council Information Office published a white paper titled "China's Arctic Policy." The white paper claimed that:

... geographically, China is a 'Near-Arctic State,' one of the continental States that are closest to the Arctic Circle. ... China is also closely involved in the trans-regional and global issues in the Arctic, especially in such areas as climate change, environment, scientific research, utilization of shipping routes, resource exploration and exploitation, security, and global governance.⁹²

China's growing strategic emphasis on the Arctic stems from its perception of the region as yet another theater for global competition.

China has used state-led research efforts to assert its presence in the Arctic and to establish sites capable of collecting intelligence on activities in the region. China maintains two permanent Arctic research

stations, in Svalbard and Iceland. Although Beijing established a satellite ground station at the Esrange Space Center in Sweden in 2016, the Swedish Space Corporation declined to renew China's contract to operate the station in 2020 amid reports of the research initiatives' links to the PLA and intelligence-collection activities.⁹³ These reports are consistent with U.S. assessments that China uses its Arctic engagements to conduct dual-use research in support of military and intelligence objectives.⁹⁴ Moreover, this is a strategy Beijing has explicitly praised—the 2020 *Science of Military Strategy* identifies the mixing of civilian and military tasks in the polar regions as an ideal method for great powers to "achieve a polar military presence."⁹⁵

The Polar Research Institute of China, which operates under the oversight of the MNR, conducts much of China's polar research with its icebreaking research vessel, *Xuelong* (*Snow Dragon*). The *Xuelong* completed its ninth Arctic expedition, which covered 12,500 nautical miles, in 2018. In the course of this trip, the research team deployed China's first unmanned ice station in the Arctic as well as various types of unmanned observation equipment.⁹⁶ In 2019, the Polar Research Institute participated in the Multidisciplinary Drifting Observatory for the Study of Arctic Climate (MOSAiC) expedition—the largest in history—alongside teams from Germany, Russia, and Sweden.⁹⁷ Other research institutes, including the MNR's First and Second Institutes of Oceanography, also conduct research expeditions to the polar regions.

GLOBAL SECURITY INITIATIVE

The various methods through which China asserts its military and security influence abroad—including those discussed in this chapter as well as international outreach and partnerships pursued by Chinese law enforcement—will likely tie together in Beijing's Global Security Initiative (GSI). The GSI focuses on expanding China's involvement in international security governance and conflict resolution, and it serves as a link between Chinese domestic security policy and foreign policy.⁹⁸

Xi Jinping announced the GSI in his opening remarks at the Boao Forum for Asia Annual Conference in April 2022, explaining that this initiative proposed:

... to stay committed to the vision of common, comprehensive, cooperative and sustainable security, and work together to maintain world peace and security; stay committed to respecting the sovereignty and territorial integrity of all countries, uphold non-interference in internal affairs, and respect the independent choices of

development paths and social systems made by people in different countries; stay committed to abiding by the purposes and principles of the UN Charter, reject the Cold War mentality, oppose unilateralism, and say no to group politics and bloc confrontation; stay committed to taking the legitimate security concerns of all countries seriously, uphold the principle of indivisible security, build a balanced, effective and sustainable security architecture, and oppose the pursuit of one's own security at the cost of others' security; stay committed to peacefully resolving differences and disputes between countries through dialogue and consultation, support all efforts conducive to the peaceful settlement of crises, reject double standards, and oppose the wanton use of unilateral sanctions and long-arm jurisdiction; stay committed to maintaining security in both traditional and non-traditional domains, and work together on regional disputes and global challenges such as terrorism, climate change, cybersecurity and biosecurity.⁹⁹

Xi's announcement of the GSI was largely overshadowed at the time by the Russian invasion of Ukraine, but the Chinese government continued to develop the concept. For example, researchers at the China Institutes of Contemporary International Relations—a think tank affiliated with the MSS that exerts strong influence over state and party foreign policy decisions—conceptualized the GSI as an effort to demonstrate “China’s shouldering responsibilities as a major country.” An important goal was to respond to traditional and non-traditional security challenges and to ensure “continuation and development of China’s traditional culture and wisdom and an integration and innovation of international security thinking with Chinese characteristics” and the “sublation and transcendence of Western security theory.”¹⁰⁰

In February 2023, the Chinese MFA released a white paper outlining the core principles of the GSI and the ways in which China will promote bilateral and multilateral security cooperation with foreign governments and international institutions within the GSI framework.¹⁰¹ While much of the description provided in this paper is presented through rhetoric that emphasizes peace, inclusion, and cooperation, Beijing’s priorities imply that one of the central objectives of the GSI is to shape global security norms in pursuit of China’s own interests. While China plans to work alongside partner nations and organizations to pursue peaceful resolutions to global security challenges, Beijing will likely operationalize this initiative to

promote Chinese technologies and security strategies to foreign governments.¹⁰² As this initiative becomes more established, it may lead Beijing to expand the use of some of its other military and security tools. For example, PSCs may be deployed to resolve security threats in a more active posture rather than serving only as guardians of Chinese personnel and assets.

CONCLUSION

There are several key takeaways from these irregular military activities, which are an important part of Chinese political warfare. Beijing relies on commercial entities and plausibly routine military activities to further its geopolitical goals, uses legal violations and new sovereign claims to erode international norms and standards, and spreads influence and projects power capabilities through its irregular military actions. While the scale and scope of these activities are concerning, the effectiveness of Beijing’s campaigns to spread geopolitical influence and assert territorial claims is somewhat limited.

First, it is notable that most security-based irregular activities rely on ostensibly commercial actors or routine military activities, providing Beijing with plausible deniability while still advancing its geopolitical goals and influence. In Chinese strategic thinking, this concept is known as military-civil fusion: “economic and social development takes into account military needs, and national defense and military modernization are deeply integrated into the economic and social development system. The strategic thinking of military-civilian integration is the inheritance and development of military-civilian dual-use, military-civilian integration, and military-civilian ideas.”¹⁰³ Military-civil fusion strategies date back to Mao Zedong, but Xi Jinping has significantly increased China’s emphasis on both this concept and the role of the military in statecraft.¹⁰⁴

Unlike nations such as the United States, whose civil-military relationships involve cooperation between separate entities, the Chinese government makes no distinction between civilian and government interests or control. Rather, it relies on a state-led “all-of-society” approach in which all actions and goals must strive to advance the interests of the CCP and in which the military is prioritized above civil concerns.¹⁰⁵ Even the private in “private security company” is a misnomer. In China, the CCP ultimately controls all enterprises, and all companies must work toward the state’s

goals. The Chinese government also requires that all security companies are either state-owned sole proprietorships or that more than half of the company's capital be state-owned.¹⁰⁶ Although commercial, political, and military assets are innately united in the Chinese political context, this is not necessarily the case in the countries that China targets with its irregular action, putting other nations in a more challenging legal position when determining responses to Chinese aggression. Nonetheless, it is often difficult to distinguish whether the CCP has directed commercial expansion abroad or if it is seizing the opportunity to capitalize on existing commercial interests both regionally and abroad—or some combination of the two.

Second, China intentionally and repeatedly violates international norms and legal standards during its irregular military activities—either directly or through the operations of Chinese corporations. These infractions include EEZ incursions and other challenges to national sovereignty, economic and environmental harms, and violation of international agreements governing maritime activities (including those which China has ratified). These activities raise substantial regional concerns about sovereignty, economic rights and access, environmental protection, and freedom of movement. China likely will also continue to use lawfare strategies to challenge international law, established global norms, and the rules-based international order in favor of a reimagined system tailored to Beijing's own needs and ideology.¹⁰⁷

Third, Chinese irregular military actions allow Beijing to project influence—whether benevolently through research cooperation or coercively through violations of sovereignty and theft of resources—and economic and military strength. None of these actions are intended to start a regular military conflict. In Xi Jinping's words, the Chinese government seeks to “resolutely safeguard China's maritime rights and interests” and build the nation into a “maritime superpower.”¹⁰⁸ Irregular action to reinvent geographic boundaries, influence opinion, and mold international norms in China's favor allows the state to advance its own strategic and political objectives at relatively low risk.

The [Belt and Road] Initiative is harmonious and inclusive. It advocates tolerance among civilizations, respects the paths and modes of development chosen by different countries, and supports dialogues among different civilizations on the principles of seeking common ground while shelving differences and drawing on each other's strengths, so that all countries can coexist in peace for common prosperity.

-Action Plan on the Belt and Road Initiative'



ECONOMIC COERCION

坚持和谐包容。倡导文明宽容, 尊重各国发展道路和模式的选择, 加强不同文明之间的对话, 求同存异、兼容并蓄、和平共处、共生共荣。

-推动共建丝绸之路经济带和21世纪海上丝绸之路的愿景与行动'

This chapter examines Chinese economic coercion, which is a key component of political warfare.

As Linda Robinson argues in her study of modern political warfare, the “tactic of economic subversion can be seen in the overlap of the diplomatic/political (routine diplomacy) and economic (trade) spheres. Political is often—but not necessarily—carried out covertly, but it must be undertaken outside the context of conventional war.”³ U.S. diplomat George Kennan similarly noted that economic measures are an important tool of political warfare to weaken an adversary short of armed conflict.⁴

Economic coercion is a tool of political warfare as old as diplomacy itself and not one unique to China. Indeed, Pericles issued the Megarian Decrees in the 5th century BCE, blocking Megara’s traders from Athenian markets in an attempt to reincorporate the city-state into the Athenian empire.⁵ The United States has also employed these tools during the Cold War.⁶ The rapid rise of China’s economy, as well as its role as the world’s largest manufacturer and the world’s largest economy on a purchasing power parity basis, affords it unprecedented economic power to use for diplomatic and political ends.⁷

The Chinese government views economic competition over emerging technologies as a central pillar of competition with the United States.⁸ Within that context, Beijing views the ability to influence global standards and leverage economic partnerships

as a means to shape the economic “battlefield” to gain an advantage over the United States and other competitors.

China is particularly well placed to employ coercive economic tools due to several features of its economic system beyond its sheer size. Chinese leaders have both the willingness and ability to employ domestic capital for political ends by, for example, directing the investment of its numerous state-owned enterprises.⁹ This extends to China’s private firms as well. One survey of China’s 100 largest private firms by revenue found that 95 of their founders or de facto heads belonged to Chinese Communist Party (CCP) organs, a decision that signals allegiance to China and maintains important relationships with state political agents.¹⁰ Because of the networked nature of China’s economic sector that encompasses levers of state power, China faces fewer obstacles to directing capital flows in coercive ways than in more liberal market systems. Moreover, international perception of Chinese markets enhances the efficacy of Chinese economic coercion. For example, many international industries and states simply view the Chinese domestic market as too large to forego and conclude that China’s meteoric economic growth will impose large future costs should an industry go against China in the present.¹¹

Economic coercion is multifaceted, and elements of it are captured in adjacent terms such as “geo-economics” and “economic statecraft.” As used

in in this chapter, economic coercion is defined as the implied, threatened, or actual imposition of economic costs in order to weaken a target.¹² A state, in this case China, can use a variety of economic levers as part of political warfare. This may include implementing trade restrictions, such as sanctions and boycotts, or taking an action that inflicts negative second-order economic effects, such as imposing limits on the number of Chinese tourists to a country. While these tools are regularly employed as part of standard international trade, the key to classifying these actions as economic coercion is through their explicit or implicit linkage to the Chinese government's desire to expand Beijing's influence and legitimacy, as well as weaken its adversaries.

The Chinese government routinely employs various forms of economic coercion to overtly or covertly encourage political and economic dependence on China, shape standards and norms in line with CCP goals and philosophy, and punish or deter activities that run counter to its own political interests. These strategies largely seek long-term impacts, but the steady development of relationships with Chinese companies and government financial entities portends that the economic dimension of Chinese political warfare will be long-lasting and potentially highly impactful. Unlike some of China's more overt acts, most forms of economic coercion can be plausibly

denied as routine statecraft, and many—such as direct investments or provision of affordable technology—are beneficial to partner nations. With these Chinese economic activities accepted and even encouraged, Beijing is likely to continue expanding its irregular economic playbook in the years to come.

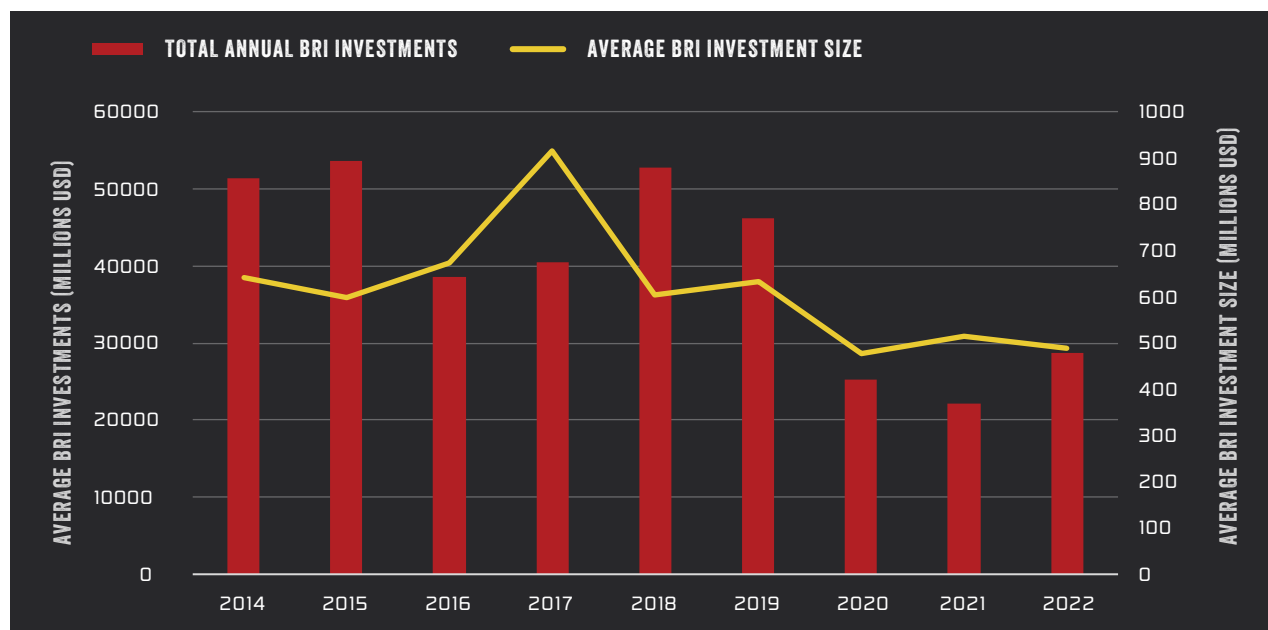
This chapter explores economic coercion as practiced by China as a method of political warfare. This chapter asks two main questions: How is economic coercion understood and employed by Chinese policymakers? And what are its effects on the conduct of international politics? To do this, the chapter explores Chinese economic coercion in three contexts: Belt and Road Initiative investments, the expansion of the Digital Silk Road, and international political disputes. It concludes with key takeaways related to economic coercion as a tool of Chinese political warfare.

BELT AND ROAD INITIATIVE

Xi Jinping launched the Belt and Road Initiative (BRI, 一带一路)—originally known as the One Belt, One Road Initiative—during state visits to Kazakhstan and Indonesia in 2013. During his September 2013 speech at Nazarbayev University in Kazakhstan, Xi proclaimed:

Figure 8.1

Annual BRI Investments, 2014–2022



SOURCE: DEREK SCISSORS, "CHINA GLOBAL INVESTMENT TRACKER," AMERICAN ENTERPRISE INSTITUTE (AEI), ACCESSED MAY 2023, [HTTPS://WWW.AEI.ORG/CHINA-GLOBAL-INVESTMENT-TRACKER/](https://www.aei.org/china-global-investment-tracker/).

In order to make the economic ties between European and Asian countries closer, the mutual cooperation deeper and the development space wider, we can build the “Silk Road Economic Belt” together with an innovative cooperation model. This is an important project that will benefit all the people along the route. We can start from the following aspects, leading from point to point, from line to line, and gradually form a large regional cooperation.¹³

By 2022, Beijing had reached BRI development agreements with more than 140 nations.¹⁴ However, as Figure 8.1 demonstrates, annual investments in BRI projects have been lower since 2020 than in the preceding years.

This section explores three ways in which China uses the BRI to coerce partners: leveraging political support as an unofficial condition for economic partnership, using large sums of debt to China as leverage, and capitalizing on the appeal of bilateral debt relief.

INVESTMENTS LEAD TO POLITICAL INFLUENCE

China’s BRI agreements allow it to reinforce existing partnerships and forge new relationships that result in additional international political support, including through the disruption of existing relationships between partner countries and Taiwan. How overtly China exchanges BRI investments for political influence varies by country type. The exchange is most overt in developing countries, where China provides development finance and in return receives political support on issues such as Taiwan, Tibet, and Xinjiang. However, Chinese efforts to gain political influence often change as partners’ economies become more advanced. In states with mid-sized economies, China typically uses state-owned enterprises and investment funds to garner influence, while in advanced economies China’s leverage depends on state-backed funds and private investors.¹⁵ In less subtle cases, a country may quickly reverse its positions on issues of interest to China in conjunction with BRI agreements, clearly demonstrating the political gains that Beijing secures alongside its development endeavors.

Panama, for example, severed all diplomatic relations with Taiwan and strongly endorsed the One-China Principle in June 2017.¹⁶ This switch—which Taiwan perceived as a significant setback to its diplomatic goals in the region—was quickly rewarded. In November 2017, Panama became the first country in the Americas to join the BRI when it reached an agreement with China to support

the construction of the Panama-Chiriquí Railway. During the same year, the Panamanian government awarded contracts to Chinese companies to construct a cruise terminal at the Pacific end of the Panama Canal and a container port and liquid natural gas plant at the Atlantic end. Various development projects along the canal continued to receive heavy investments from Chinese firms in subsequent years.¹⁷

Similarly, in September 2019, the Solomon Islands ended its relationship with Taiwan and established official ties with China. Shortly thereafter, four cabinet officials who had opposed the switch were removed from office, and a fifth resigned.¹⁸ Within weeks, Prime Minister Manasseh Sogavare traveled to Beijing and signed five memorandums of understanding (MOUs), including a formal BRI partnership agreement. China agreed to construct a multimillion-dollar stadium for the 2023 Pacific Games and infrastructure projects in support of the redevelopment of the Solomons’ most lucrative gold mine. In addition, the state-owned conglomerate China Sam Enterprise Group signed an agreement with the Tulagi provincial government for exclusive rights to the entirety of the island territory, though this agreement was later overturned.¹⁹ Subsequent agreements between China and the Solomon Islands have included the deployment of Chinese law enforcement and military personnel and a contract for Huawei to construct telecommunications towers.²⁰

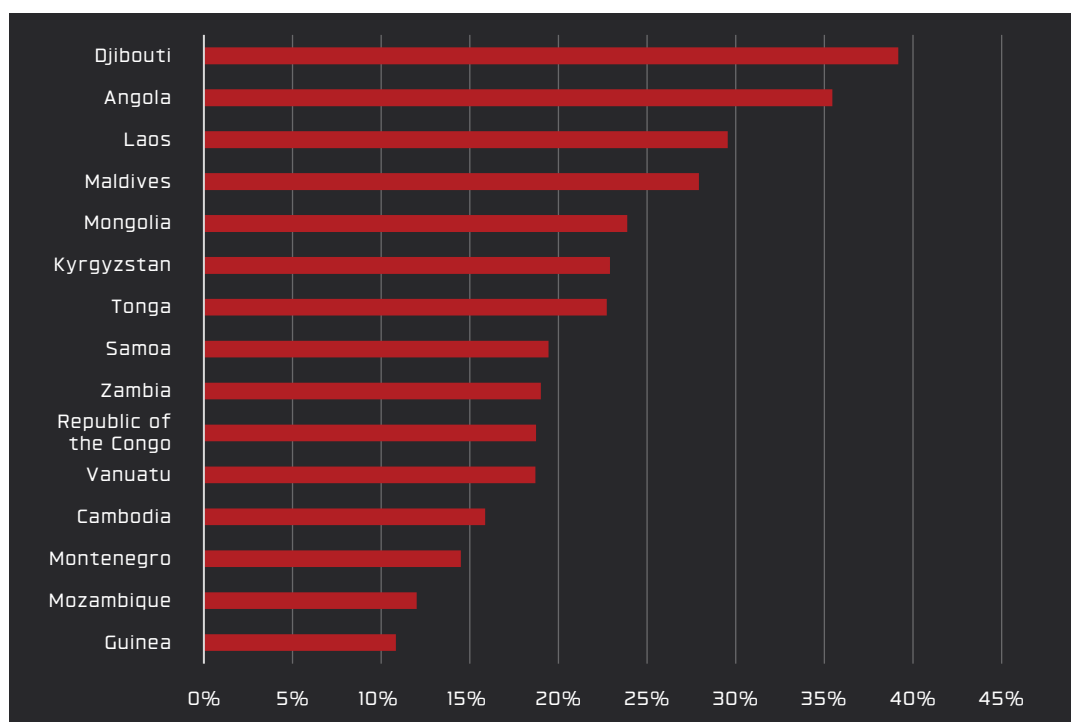
Shifts in policy positions in partner countries may or may not be mandated by their MOUs with China; they can also result from political pressure to maintain positive relationships and avoid reprisal from China. For an example of how China responds when one of its partners takes political actions that run counter to its interests—such as violating the One-China Principle—see the discussion of Lithuania later in this chapter.

DEBT TRAPS AND FINANCIAL LEVERAGE

By 2020, China had lent roughly \$1.5 trillion in loans and grants to more than 150 countries—making it the world’s largest creditor, with claim to more than 5 percent of global GDP.²¹ As China’s BRI vision came to life, however, there were strings attached. Chinese loans not only often mandate the use of Chinese workers, result in ineligibility for multilateral financial management mechanisms, and demand political support for China, they have also sometimes pulled recipients into a “debt trap,” whereby the existence of the debt itself can be used as leverage for China to secure its own political

Figure 8.2

Long-Term Debt to China as a Percentage of Gross National Income (GNI), 2022



SOURCE: "INTERNATIONAL DEBT STATISTICS," DATABANK, WORLD BANK, ACCESSED JANUARY 27, 2023, [HTTPS://DATABANK.WORLDBANK.ORG/SOURCE/INTERNATIONAL-DEBT-STATISTICS](https://databank.worldbank.org/source/international-debt-statistics).
NOTE: THIS FIGURE INCLUDES THE 15 COUNTRIES WITH THE LARGEST RATIO OF LONG-TERM CHINESE DEBT TO GNI.

or economic gains. The 15 BRI partner countries most in debt to China, as measured by the ratio of long-term debt owed (to China) to gross national income (GNI), are detailed in Figure 8.2. Angola, which has the second-highest debt to GNI ratio, also has the second-largest total debt owed to China—it owed \$22 billion in 2021.²²

Large debts to China leave countries vulnerable to manipulation. In 2021, due to the country's large debt owed to China, Laos approved a 25-year concession agreement between Électricité du Laos and China Southern Power Grid Company that allows the latter, a majority Chinese-owned company, to control the Laotian national power grid, including electricity exports. Hydropower accounts for more than four-fifths of Laotian electricity generation, and the concession agreement may also impact the country's dams and water resources.²³

Perhaps the most well-known example of this "debt-trap diplomacy" is that of Sri Lanka. After the government defaulted on Chinese loans for the development of the Hambantota port, the Sri Lankan government granted China a 99-year lease for control of the port and 15,000 acres of surrounding land in December 2017.²⁴ In the years since, China's leverage over Sri Lanka has only

strengthened. With its debt crisis growing, Sri Lanka accepted a \$3 billion loan from China in 2020 to manage its existing debts, opting for the easier path of Chinese support over International Monetary Fund debt restructuring or the austerity measures required by the Paris Club.²⁵

There is an ongoing debate among Western analysts over how intentionally malicious Chinese lending is and whether "debt trap" is a fair descriptor. Researchers have correctly pointed out that each case of lending is nuanced, with many partner nations seeking Chinese investment and multiple factors contributing to financial distress.²⁶ Regardless of the level of premeditation, however, Chinese loans—including their uniquely opaque and restrictive terms—create political and economic leverage that China uses to shape the geopolitical environment to its advantage.²⁷

DEBT RELIEF AND FORGIVENESS

Beijing has historically limited debt relief options available to its partners, including explicitly forbidding participation in some international debt management efforts, such as the Paris Club, as one of the terms of its BRI contracts.²⁸ When it does engage in debt relief or forgiveness, Beijing prefers to operate through bilateral arrangements

to maintain control of all terms and conditions.²⁹ Recently, economic stresses related to the Covid-19 pandemic increased both the demand for and frequency of approval for debt relief or forgiveness—agreements that can improve international perception of China and incentivize BRI partner countries to continue economic partnerships with China. Some analysts have assessed that these decisions may specifically aim to manage the “public relations nightmare” of claims of debt-trap diplomacy.³⁰

In his 2021 speech at the Forum on China-Africa Cooperation, Xi Jinping announced that “China will exempt African LDCs [least developed countries] from debt incurred in the form of interest-free Chinese government loans due by the end of 2021.”³¹ This forgiveness applied to 23 interest-free loans to 17 African countries. According to estimates from the Global Development Policy Center at Boston University, the total sum of the debt forgiven was likely between \$45 million and \$610 million.³²

In addition to the debt cancellation from the Forum on China-Africa Cooperation, there are three other primary mechanisms for debt relief from China: the G20 Debt Service Suspension Initiative (DSSI), contributions to the International Monetary Fund’s Catastrophe Containment and Relief Trust, and ad hoc debt relief. Within each of these mechanisms, Beijing may opt to relieve debts through renewal and refinancing, reprofiling and rescheduling, restructuring, or either partial or full forgiveness.³³ In September 2022, for example, China agreed to restructure Ecuador’s debt by extending the maturity of loans from the China Development Bank and the Export-Import Bank of China until 2027 and 2032, respectively, resulting in relief of \$1.4 billion until 2025.³⁴

DIGITAL SILK ROAD

First introduced as part of the standard connectivity plan for the BRI in 2015, the Digital Silk Road (DSR) aims to spread and synthesize Chinese efforts related to telecommunications, e-commerce, hardware, software, big data, artificial intelligence and machine learning (AI/ML), the Internet of Things, and other digital infrastructure and norms.³⁵ In his speech at the 2017 Belt and Road Forum for International Cooperation, Xi Jinping officially described the DSR as the technological component of the BRI, saying that China “should pursue innovation-driven development and intensify cooperation in frontier areas such as digital econ-

omy, artificial intelligence, nanotechnology and quantum computing, and advance the development of big data, cloud computing and smart cities so as to turn them into a digital silk road of the 21st century.”³⁶ Figure 8.3 provides details about the five main categories of DSR efforts as well as each category’s primary components and examples of Chinese companies that further Beijing’s goal of technological dominance and influence.

Unlike the primary BRI investments, DSR projects are driven by private companies. Nonetheless, these companies maintain close ties to the CCP, including with regard to both goals and objectives and, in many cases, the ability to access or exploit the access granted by the technologies they sell. Still, coordination and information sharing in this ecosystem remain inconsistent and decentralized.³⁷

This section examines China’s DSR-related goals and strategies as they apply to software, hardware, and digital infrastructure as well as global standards for emerging technology. Chinese efforts to shape public opinion and the information environment are explored in greater detail in the information and disinformation chapter (Chapter 5) of this report.

SOFTWARE, HARDWARE, AND INFRASTRUCTURE

As part of the DSR, Chinese companies have expanded their presence in the markets for software, hardware, and technological infrastructure. These different products give Beijing the ability to compete with U.S. and other Western companies in all levels of the internet technology stack, as seen in Figure 8.4.³⁸ This means that Chinese companies not only provide software, applications, and services but also control the very systems that process, store, and transmit data. While user applications such as social media platforms, games, and shopping services spread influence and collect some data, control of hardware and infrastructure permits Beijing more complete access to data and surveillance as well as control over the continuation of services.

The risk of exploitation is greatest when Chinese technology companies control multiple—or all—layers of the internet technology stack. For example, after funding, designing, and helping to construct the African Union (AU) headquarters in Addis Ababa, Ethiopia, Beijing controlled the building’s networks, software, and hardware, including security camera systems. In 2018, the French newspaper *Le Monde* broke allegations that China had used this access to regularly obtain confidential AU data and recordings.³⁹ Beijing denied the accusation, and the AU maintained

Figure 8.3

The Five Categories of Digital Silk Road Efforts

CATEGORY	COMPONENTS	EXAMPLES
Finance	Digital financial infrastructure and payment platforms	Alipay; WeChat Pay
Infrastructure	Cables, cellular networks, cloud storage and infrastructure, content delivery networks, data centers, satellites, sensors, 5G	BeiDou Navigation Satellite System, China Electronics Technology Group Corp. (CETC), Hengtong Group, Huawei, Inspur, ZTE
Policy	Digital governance and standards	China Governance 2035
Public Opinion	News and entertainment media, online cultural exchange platforms, social media, video games	ByteDance, NewsDog, Perfect World, Tencent Games, WeChat
Trade	E-commerce, shipping and logistics	Alibaba, JD.com (Jingdong), Pinduoduo/Temu, Shein

SOURCE: FUDAN UNIVERSITY DIGITAL BELT AND ROAD CENTRE, *DIGITAL SILK ROAD BLUEBOOK* (SHANGHAI: FUDAN UNIVERSITY, 2018); BRIGITTE DEKKER, MAAIKE OKANO-HEIJMANS, AND ERIC SIYI ZHANG, *UNPACKING CHINA'S DIGITAL SILK ROAD* (THE HAGUE: CLINGENDAEL INSTITUTE, 2020), [HTTPS://WWW.CLINGENDAEL.ORG/SITES/DEFAULT/FILES/2020-07/REPORT_DIGITAL_SILK_ROAD_JULY_2020.PDF](https://www.clingendael.org/sites/default/files/2020-07/report_digital_silk_road_july_2020.pdf); AND PETER RAYMOND, "THE GLOBAL EXPANSION OF CHINESE TECHNOLOGY PLATFORMS," (PRESENTATION, CSIS, WASHINGTON, DC, NOVEMBER 14, 2022).

its relationship with Chinese companies to avoid damaging its relationship with Beijing.⁴⁰ With little having changed, China was once again detected stealing data and camera footage from the AU headquarters in 2020.⁴¹

GLOBAL STANDARDS FOR EMERGING TECHNOLOGY

In addition to seeking market dominance and control of information, Beijing's DSR efforts also emphasize the importance of establishing and shaping global standards and norms for emerging technology that are in line with the CCP's interests. Beijing has a broader agenda than simply ensuring that its companies are well positioned to compete in emerging markets. Standards carry with them norms and values, including in relation to issues of contention between the Chinese government and Western democracies, such as free speech, privacy, and surveillance. For example, Chinese companies working on AI and the Internet of Things have advanced facial recognition and surveillance technology, which the Chinese government routinely uses to monitor and suppress political dissidents and ethnic minorities.⁴² Chinese efforts to set standards to their preferences—in other words weighted toward authoritarian states' ability to surveil populations and against personal freedoms—will allow greater freedom for Beijing to operate both at home and around the globe.

In October 2021, the CCP released its "National Standardization Development Outline," a white paper that laid out near- and long-term goals (to 2025 and 2035, respectively) for technological standardization. Colloquially known as "China Standards 2035," the document called for the nation to:

Strengthen standards research in key technical fields. Conduct standardized research in artificial intelligence, quantum information, biotechnology, and other fields. Utilizing the integration of informatization and industrialization for new generation information technology with broad potential for future applications such as big data, blockchain, healthcare, new energy, new materials, etc. China will simultaneously deploy technological research and development in coordination with research on and formulation of standards and their promotion in industry, to accelerate the pace of industrialization for new technologies.⁴³

In pursuit of these goals, China has both expanded its participation in international standards-setting processes and has sought to establish new avenues for standards development. For example, Chinese companies such as ZTE and Huawei have been heavily involved in the development processes for international standards related to 5G and the Internet of Things.⁴⁴ Outside of the mainstream standardization community, China has also explored the notion of developing its own Belt and Road Standards Forum as a parallel alternative.⁴⁵

As Beijing prioritizes the expansion of initiatives such as the DSR, which aim to reshape global norms and standards, the best opportunity for the United States and its allies to counter Chinese strategy may be to establish a united democratic alternative. This is further complicated by differences in standards and inconsistent priorities between other leading nations, including the United States and EU members.⁴⁶

Figure 8.4

U.S. and Chinese Companies Competing in the Internet Technology Stack

	SOFTWARE/HARDWARE GROUPINGS	GENERAL EXAMPLES	U.S.-BASED COMPANIES	PRC-BASED COMPANIES
APPLICATION LAYER	Software applications	Internet platforms (e.g. social media, websites, mobile apps), machine-learning engines (from cloud providers), content handlers	Facebook, Google, Amazon, Apple, Microsoft, PayPal, Zoom, Salesforce, Adobe	Baidu, Alibaba, Tencent, JD.com, ByteDance, Ant Group, Megvii, iFlytek, CloudWalk, SenseTime, YITU, Ping An Tech, Inspur, Huawei, CETC
	Storage and software infrastructure	Content delivery networks, cloud storage and infrastructure	Cloudflare, Akamai, Google, Microsoft, Amazon, IBM, Oracle, Apple	Alibaba, Tencent, ByteDance, Ping An Tech, Inspur, Huawei, CETC
NETWORK LAYER	Hardware	Satellite navigation, networking hardware, sensor hardware, semiconductors, mobile wireless networking equipment	Cisco, Juniper, Global Positioning System (GPS), Google, Amazon, Apple, Nvidia, AMD, Texas Instruments, Qualcomm, Broadcom, Intel, Microsoft, IBM	Huawei, ZTE, BeiDou, Nuctech, Meiya Pico, Hikvision, Uniview, Dahua, Megvii, iFlytek, SenseTime, DJI, Huawei's Hisilicon, SMIC, CETC
PHYSICAL LAYER	Carrier infrastructure	Submarine cables, fiber-optic networks, mobile wireless network carrier equipment (5G base stations)	AT&T, Sprint, Verizon, Cogent, Comcast, Facebook, Google, Amazon, Microsoft, T-Mobile US	Hengtong, China Mobile, China Telecom, China Unicom, PEACE cable Ltd, Huawei, CETC

SOURCE: SAMANTHA HOFFMAN AND NATHAN ATTRILL, "SUPPLY CHAINS AND THE GLOBAL DATA COLLECTION ECOSYSTEM," AUSTRALIAN STRATEGIC POLICY INSTITUTE, POLICY BRIEF REPORT NO. 45/2021, JUNE 2021, [HTTPS://S3-AP-SOUTHEAST-2.AMAZONAWS.COM/AD-ASPI/2021-06/SUPPLY%20CHAINS.PDF?VERSIONID=56J-TTBXYXVSMUHQIOT5QSSR92ADAZH](https://S3-AP-SOUTHEAST-2.AMAZONAWS.COM/AD-ASPI/2021-06/SUPPLY%20CHAINS.PDF?VERSIONID=56J-TTBXYXVSMUHQIOT5QSSR92ADAZH).

ECONOMIC SANCTIONS AND PUNISHMENT IN POLITICAL DISPUTES

China frequently employs coercive economic sanctions to punish nations for taking political or economic actions that contradict Beijing's interests and to incentivize policies that are more in line with China's goals. While it sometimes uses traditional sanctions in higher-impact cases, Beijing frequently relies on implicit sanctions, informal boycotts, and regulatory actions to compel states to adhere to its demands.⁴⁷ Figure 8.5 highlights examples of Chinese use of economic punishments to attempt to coerce more favorable outcomes in political disputes since 2000. The types of activities that most frequently provoke this response from Beijing include economic restrictions impacting Chinese companies, political activities that threaten Chinese claims of sovereignty, and arms sales and security activity. This section provides brief examples of each.

RESTRICTIONS ON CHINESE COMPANIES

Other states' restrictions on the activities of Chinese companies—particularly technology companies involved in the DSR, such as Huawei—have increasingly provoked economic punishment by China. After the Australian government banned Huawei and ZTE from providing technology for 5G networks in 2018, for example, Beijing responded with both formal and informal trade restrictions on imports such as barley, beef, coal, lobster, and wine.⁴⁸ The Chinese-Australian relationship further soured in 2020 when Australia called for an international probe into the origins of the Covid-19 pandemic.⁴⁹ Ultimately, however, Chinese restrictions on Australia caused only modest and short-term economic impact.⁵⁰

Despite some modest economic harms, this case demonstrates the mixed effects of this strategy, as China's punishment campaign against Australia may have harmed Australian attitudes toward China. Researchers at the University of Adelaide estimated that Australia forwent \$4.9 billion in export revenues due to Chinese restrictions between

Figure 8.5

Examples of Chinese Economic Punishment, 2000–2022

YEAR(S)	TARGET COUNTRY	REASON
2003	North Korea	Pressure to join trilateral meeting on nuclear disarmament hosted in Beijing
2007	Vietnam	South China Sea territorial dispute
2008	Vietnam	South China Sea territorial dispute
2008	France	Disruption of Olympic torch relay amid pro-Tibet demonstrations
2009	France	President meets with Dalai Lama
2010	United States	Arms sales to Taiwan
2010	Japan	Japanese coast guard detained a Chinese trawler captain
2010	Norway	Liu Xiaobo, a Chinese dissident, received the Nobel Peace Prize
2012	United Kingdom	Prime minister meets with the Dalai Lama
2012	Japan	Japan announces plans to purchase three of the main Senkaku Islands
2012–2016	Philippines	Dispute over Scarborough Shoal territorial claims
2013	Lithuania	President meets with the Dalai Lama
2016	Taiwan	Pro-independence president elected
2016	Mongolia	Dalai Lama visit
2016–2017	South Korea	THAAD deployment
2017	Palau	Recognition of Taiwan
2018	Australia	Huawei and ZTE bans
2018–2019	Canada	Arrest of Huawei finance director
2019	United States	Arms sales to Taiwan
2019	United States	Escalation of trade war
2020	Australia	Call for investigation into the origins of Covid-19
2020	Czech Republic	Diplomatic visit to Taiwan
2020	United Kingdom	Huawei ban; citizenship eligibility for Hong Kong residents
2021–2022	Lithuania	Establishment of a Taiwanese Representative Office

SOURCE: VIDA MACIKENAITE, "CHINA'S ECONOMIC STATECRAFT: THE USE OF ECONOMIC POWER IN AN INTERDEPENDENT WORLD," *JOURNAL OF CONTEMPORARY EAST ASIA STUDIES*, 9, NO. 2 (2020): 108–26, DOI:10.1080/24761028.2020.1848381; DAVID UREN, "ECONOMIC COERCION: BOYCOTTS AND SANCTIONS—PREFERRED WEAPONS OF WAR," AUSTRALIAN STRATEGIC POLICY INSTITUTE, OCTOBER 15, 2020, [HTTPS://WWW.ASPI.ORG.AU/REPORT/ECONOMIC-COERCION-BOYCOTTS-AND-SANCTIONS-PREFERRED-WEAPONS-WAR](https://www.aspi.org.au/report/economic-coercion-boycotts-and-sanctions-preferred-weapons-war); CHARLES MILLER, "EXPLAINING CHINA'S STRATEGY OF IMPLICIT ECONOMIC COERCION: BEST LEFT UNSAID?," *AUSTRALIAN JOURNAL OF INTERNATIONAL AFFAIRS* 76, NO. 5 (2022): 507–21, DOI:10.1080/10357718.2022.2061418; AND CHRISTINA LAI, "ACTING ONE WAY AND TALKING ANOTHER: CHINA'S COERCIVE ECONOMIC DIPLOMACY IN EAST ASIA AND BEYOND," *THE PACIFIC REVIEW* 31, NO. 2 (2018): 169–87, DOI:10.1080/09512748.2017.1357652.

July 2020 and February 2021.⁵¹ Yet marked shifts in Australian public opinion of China also coincided with the economic dispute. Polling conducted by the Lowy Institute found that Australian public opinion toward China became increasingly negative as the China-Australia economic relationship deteriorated. In 2020, 41 percent of Australians polled perceived China as a security threat, and 55 percent saw China as an economic partner. This shifted against China in 2021, when 63 percent of participants saw China as a security threat and only 34 percent viewed China as an economic partner.⁵²

Nonetheless, this type of response also provides Beijing with the credibility to influence other states' decisions simply by threatening to do the same to them if they act against Chinese companies.

For example, in 2019, as Germany contemplated excluding Huawei from its next-generation 5G network, the Chinese ambassador to Germany warned that "there will be consequences. The Chinese government will not stand idly by" and threatened action against the German automotive industry, which relies heavily on Chinese markets.⁵³ Germany relented and declined to prohibit Huawei, which by late 2022 accounted for 59 percent of German 5G radio access network equipment.⁵⁴

CHALLENGES TO SOVEREIGNTY

China has also used economic coercion against countries in response to actions that challenge perceptions of Chinese sovereignty, including issues of political legitimacy and territorial control. Examples include supporting the governments or

people of Taiwan, Tibet, and Hong Kong; disregarding Chinese territorial claims in the South China Sea; supporting political dissidents; and criticizing Beijing's record of human rights violations.

For example, in July 2021, the Lithuanian Ministry of Foreign Affairs announced that Taiwan would establish a “Taiwanese Representative Office” in Lithuania later that year.⁵⁵ While the office does not have diplomatic accreditation, it functions as a *de facto* embassy—similar to the Taipei Economic and Cultural Representative Office in the United States. The decision to permit the office to use the name “Taiwan” rather than “Taipei” sparked fierce condemnation from Chinese authorities. In August 2021, Beijing recalled its ambassador to Lithuania and demanded that the Lithuanian ambassador be recalled as well, charging that the decision to support Taiwan “severely undermines China’s sovereignty and territorial integrity.”⁵⁶ As Lithuania allowed the creation of the Taiwanese Representative Office to move forward, its economic and diplomatic relationship with China continued to deteriorate. China suspended Lithuanian visas and restricted trade between the two countries, including by delisting Lithuania as a country of origin and directly prohibiting imports of Lithuanian beef, dairy, and alcohol.⁵⁷

China also introduced secondary sanctions against firms that purchase products from Lithuanian companies. This development provoked criticism from the Lithuanian tech industry, which was most heavily impacted. For example, Kristijonas Vizbaras, cofounder of the laser manufacturer the Brolis Group, complained that the laser industry had “been sacrificed for this ‘value-based’ policy,” and unless the situation changed, companies like his would no longer be able to operate in Lithuania.⁵⁸

ARMS SALES AND SECURITY ACTIVITY

Finally, China has enacted other coercive economic measures in response to defense and security activities that undermine Chinese goals or have the capacity to threaten Chinese territorial claims. Examples include arms sales, security cooperation negotiations or agreements, and military deployments.

In some cases, Beijing has responded with targeted sanctions on arms manufacturers. For example, after the United States approved a \$2.2 billion arms sale to Taiwan in 2019—including 108 M1A2T Abrams tanks, 250 Stinger missiles, and other equipment—China responded with sanctions against the U.S. manufacturing companies involved in the deal.⁵⁹

Typically, however, these measures target other nations to compel them to decline security assistance from the United States and its allies or to otherwise de-escalate military activities that could potentially constrain Chinese interests. When South Korea—in partnership with the United States—deployed the Terminal High Altitude Area Defense (THAAD) missile defense platform in 2016 to guard against North Korea, China lodged an official diplomatic complaint against South Korea, imposed restrictions on South Korean tourists, forced the closure of a company involved in securing the THAAD deployment site, cut subsidies, and generated additional regulatory hurdles for South Korean companies.⁶⁰ China’s economic punishment against South Korea dragged into the following year, until South Korean president Moon Jae-in relented to Beijing’s pressure and publicly affirmed that his country would follow the “Three Nos” policy. President Moon Jae-in promised that South Korea would not deploy additional THAAD systems, would not participate in a missile defense network led by the United States, and would not enter into a trilateral military alliance with the United States and Japan.⁶¹

CONCLUSION

Economic coercion is a viable means of political warfare. In addition to the direct geopolitical gains China secures through economic coercion—including leverage and the spread of influence—Beijing also uses these forms of outreach to create dependencies on China, particularly in the developing world. Examples include vying for relationships with U.S. partners. Despite India’s close security relationship with the United States, China has cultivated a strong economic relationship with India. Affordability is India’s primary concern with regard to emerging technologies, so the Indian government relies on Chinese companies for a large portion of its data and telecommunications equipment and infrastructure.⁶² As long as China remains able to offer cheap options to developing countries, these countries will depend on Chinese technologies and will be motivated to maintain positive relationships with Beijing.

As China’s wide range of coercive economic activities demonstrate, economic competition likely will involve an integrated, whole-of-society approach, including policy and norms, information, finance and trade, infrastructure, and all layers of the technology stack. At the same time, China likely will continue to wield both investments

and economic punishments such as sanctions to keep partner nations invested in the Chinese global economic project, dependent on Beijing's support and infrastructure, and behaving in line with Chinese sovereign claims and geopolitical goals. Beijing is likely to continue to focus on economic tools useful for economic competition, particularly if some of its more overtly malicious pathways are challenged or restricted.

The most comprehensive and serious challenge to U.S. national security is the PRC's coercive and increasingly aggressive endeavor to refashion the Indo-Pacific region and the international system to suit its interests and authoritarian preferences.

-U.S. National Defense Strategy (2022)¹



COUNTERING CHINA

The PRC is the only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it. Beijing has ambitions to create an enhanced sphere of influence in the Indo-Pacific and to become the world's leading power.

-U.S. National Security Strategy (2022)²

China is engaged in extensive and aggressive political warfare across the globe, including in the U.S. homeland.

These actions are perpetrated by such organizations as the People's Liberation Army (PLA), Ministry of State Security (MSS), Ministry of Public Security (MPS), Ministry of Industry and Information Technology, United Front Work Department, and Ministry of Foreign Affairs. A wide range of non-state or quasi-state actors, from hacktivists to private security companies, support the official acts of the state. The primary tools of Chinese political warfare include:

- **Intelligence Operations:** China's intelligence services, such as the MSS and MPS, are engaged in extensive intelligence activity to expand Chinese power and influence. In examining over 100 Chinese espionage cases directed at the United States or U.S. entities, this report concludes that the United States has suffered substantial losses in terms of trade secrets, military technology, sensitive data on U.S. citizens, classified U.S. government information, and harassment of individuals—including members of the Chinese diaspora—residing in the United States.
- **Cyber Operations:** Chinese organizations, including units within the PLA, are involved in an aggressive cyber campaign against

corporations, universities, government agencies, media, think tanks, nongovernmental organizations, and other targets to advance China's interests. On the economic front, these efforts are designed to help China leapfrog ahead of the West by skipping the extensive and time-consuming research and development phases for new technologies. Chinese cyber operations are also designed to enable influence campaigns on domestic and international audiences, collect information, assist with potential offensive military campaigns, and improve China's artificial intelligence and big data analytics capabilities.

- **Information and Disinformation Operations:** China is engaged in numerous activities overseas—including in the U.S. homeland—to influence decisionmaking and popular support to gain a competitive advantage. Beijing seeks to tightly control the image of China abroad, including by influencing companies, organizations, and individuals that criticize China, from the National Basketball Association to Hollywood studios. While there has been self-censorship in Hollywood to avoid antagonizing Beijing, the two most successful movies of all time in China both involve wars against the United States: *The Battle at Lake Changjin* (2021) and *Wolf Warrior 2* (2017).³

- **United Front Work:** The CCP is involved in numerous efforts to extend its reach overseas through united front work, which involves activity to protect and bolster the image of China and the CCP. Led by the United Front Work Department, this activity has targeted U.S. universities, news media, ethnic Chinese abroad, and others inside of the United States and other countries.
- **Irregular Military Actions:** The PLA, PLA Navy, PLA Air Force, PLA Rocket Forces, People's Armed Forces Maritime Militia, and private security companies linked to China are involved in widespread efforts to expand Chinese influence. These organizations are involved in near-seas activities (which focus on securing Chinese interests in such areas as the South and East China Seas) and far-seas activities (which are global in scope). According to CSIS estimates, there are nearly two dozen Chinese private security companies operating overseas, including in Africa, the Middle East, Asia, and Latin America.
- **Economic Coercion:** China is increasingly engaged in the threat or imposition of economic sanctions or inducements to influence decisionmaking to gain a competitive advantage. There are a wide range of examples of Chinese economic coercion, such as the Belt and Road Initiative (BRI) and the Digital Silk Road (DSR). The latter aims to create—and use as political leverage—Chinese global expansion in telecommunications, e-commerce, hardware, software, big data, artificial intelligence and machine learning, the Internet of Things, and other digital infrastructure and norms across the globe.

China has several strategic goals in conducting these activities. The most important include preserving the CCP, expanding Chinese power and influence, and weakening the United States as part of balance-of-power competition. China's broader strategy aims to pursue modernization to expand its military might, economic power, and technological prowess; improve its governance; and revise the international order in support of Beijing's system of governance and national interests. In addition, China also conducts political warfare—rather than armed conflict—in an attempt to *avoid* conventional war and limit security concerns from other countries.

The rest of this chapter examines ways that the United States and its partners can compete with

China below the threshold of conventional warfare. It asks: What options do the United States and its partners have to counter Chinese political warfare?

While the United States has been slow to identify the broad range of Chinese activities and has failed to develop a systematic strategy to oppose them, this chapter outlines several core components of a strategy to counter Chinese political warfare and compete more effectively. U.S. policy should include checking China's global expansion by competing on a sustained basis; encouraging a progression toward a pluralistic political system in China that respects human rights; developing economically viable alternatives to Chinese influence over third countries, in particular in the global south; and engaging in diplomatic negotiations with China to keep communication channels open and reach agreements that protect and enhance U.S. interests where feasible.⁴

The rest of this chapter focuses on five steps that are critical to compete with China below the threshold of conventional warfare.

LEVERAGE DEMOCRATIC PRINCIPLES AS AN ALTERNATIVE TO CCP AUTHORITARIANISM

Competition today is to a great extent a balance-of-power struggle between rival political, economic, and military *systems*. China under Xi Jinping is one of the most authoritarian countries in the world, according to the nonpartisan organization Freedom House; eschews a free press; and has become more sophisticated and aggressive in using coercive tactics to shape media narratives and suppress reporting that is critical of China and the CCP.⁵

China has blocked information by creating a “Great Firewall.” As one human rights report concluded in 2022, “China was the world's worst environment for internet freedom for the eighth consecutive year.”⁶ China's digital firewall has blocked or censored hundreds of thousands of websites, apps, and services that the government has assessed contain content unfavorable to China, including Google, YouTube, Instagram, Reddit, Wikipedia, WhatsApp, LinkedIn, and numerous virtual private network providers.⁷ The country has detained and jailed journalists, human rights activists, religious leaders, and civilians for sharing online content

critical of the Chinese government. It has also tightened control over China's technology sector and enforced rules that require digital platforms to utilize their algorithms to promote CCP ideology.⁸ China has also increasingly attempted to expand its authoritarianism on digital networks across the globe, triggering what some have termed "digital authoritarianism."⁹ As one declassified U.S. intelligence assessment concluded, "China and other authoritarian governments are using cyber espionage, attacks, and influence operations to extend the coercive reach of their ideological enforcement and political control efforts beyond their borders. In some cases, they are impinging on Western democracies' sovereignty and interests to enhance their domestic stability."¹⁰

The United States and its democratic partners have categorically different systems. Freedom—of the ballot box, the press, religion, and commerce—is at the core of Enlightenment values. As the English philosopher John Locke argued, reason "teaches all mankind, who will but consult it, that being all equal and independent, no one ought to harm another in his life, health, liberty, or possessions."¹¹ The United States' democratic principles are outlined in the preamble to the Constitution: "to form a more perfect Union, establish justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity." The United States and its partners should counter Chinese political warfare by supporting these democratic principles and combating authoritarianism across the globe and on all forums, from digital platforms and the internet to corporate boardrooms, educational institutions, and the halls of government.

However, there are several pitfalls that U.S. policymakers need to avoid. First, they need to stay clear of the McCarthyism of the 1940s and 1950s, which involved false or unproven public accusations of subversion and treason. Countering China's intelligence operations, information and disinformation operations, united front work, economic coercion, and other activities—including in the U.S. homeland—is critical. But it must be based on facts, judicial oversight, and democratic principles. Such evidence must also be transparently communicated to the American public, who are increasingly the target of China's operations, particularly in the information and commercial spheres. Second, the United States needs to avoid taking actions overseas that are inconsistent with U.S. democratic principles and are bound to be counterproductive and ineffective. During the Cold

War, for example, the United States was involved in overthrowing—or attempting to overthrow—several regimes (such as Iran in 1953, Guatemala in 1954, and Chile in 1973) and orchestrating covert action programs (such as the 1983 mining of several Nicaraguan harbors) that ultimately undermined U.S. interests.¹²

UNDERSTAND CHINA

The next step is to better understand how China views competition with the United States. What are China's objectives in utilizing political warfare? What are its main instruments? What vulnerabilities and weaknesses of China can be exploited?

As this report highlights, a close analysis of Chinese activity indicates that Beijing has conducted a broad political warfare campaign against the United States and its partners across the globe. To conduct these actions, Beijing invests substantial resources in understanding the United States, including in translating documents and exploring the contours of U.S. culture and politics. The China International Communications Group, which is owned and operated by the CCP's Central Propaganda Department, distributes the CCP line on numerous issues to overseas audiences, directs research on foreign media, and conducts language training programs. The English-language training market in China was approximately \$75 billion in China in 2022.¹³ Some analysis estimates that the market for English-language training in China will increase by over \$70 billion between 2021 and 2025.¹⁴ In contrast, the market size for all language instruction in the United States was only \$1.5 billion in 2022.¹⁵ Even though China has a much larger population than the United States, Beijing still spends roughly 14 times more per capita on English language training than the United States does on *all* language training.¹⁶ More broadly, the U.S. government and private sector have failed to invest in the language skills and expertise to effectively compete with China.

U.S. leaders during the Cold War would have been horrified at this discrepancy. The U.S. government invested significant resources in conducting information campaigns and translating Soviet documents into English. Among the most important organizations was the Foreign Broadcast Information Service, which monitored, translated, and disseminated massive amounts of news from the Soviet Union and Warsaw Pact countries. Researchers, activists, journalists, policymakers,

and the public relied on its invaluable translations. When the Cold War ended, however, the United States slashed the budgets for these types of organizations. In 2019, the U.S. government shut down all outside access to the Open Source Enterprise, the successor of the Foreign Broadcast Information Service.

There is still time to change. One step is to build a twenty-first century open-source information service.¹⁷ The United States should start by having the Open Source Enterprise, embedded in the Central Intelligence Agency (CIA)'s Directorate of Digital Innovation, make its translations of Chinese material publicly available, as the Foreign Broadcast Information Service did during the Cold War. In the absence of such efforts, the private sector has taken the lead in translating Chinese material, though China has made access to material more difficult by expanding its anti-espionage laws and restricting overseas access to China-based data sources.¹⁸ For national security issues, some of the best examples are CSIS's *Interpret: China*, the Center for Security and Emerging Technology at Georgetown University, and the Department of the Air Force's China Aerospace Studies Institute.¹⁹

STRENGTHEN DEFENSE

An important component of U.S. strategy needs to be conducting more effective defensive measures against Chinese political warfare. As used here, *defense* refers to efforts to deter, resist, blunt, and mitigate attacks from an adversary.

One example is cyber. U.S. policymakers need to continue to develop a concerted effort to establish a cyber doctrine for the United States and consider how the United States' capabilities stack up against China's capabilities. An initial comparison reveals that China holds an advantage in one key area: the capability to hold critical infrastructure at risk. The obvious and urgent conclusion is that the United States must focus on bolstering its cyber defenses. It is currently too easy for an adversary such as China to hold at risk elements that make the U.S. economy and U.S. society function.

An unclassified assessment is unable to compare the most exquisite cyber tools in each nation's arsenal, but the U.S. government should run classified simulations on how China might fight in the cyber domain and how the United States might defend itself, evaluating variables such as the availability of the Global Positioning System, internet connectivity around the United States, and

redundancy of communications infrastructure in a time of conflict.

Establishing cyber norms of behavior is also worthwhile, even if China refuses to accede. Norms should include a rejection of state-based internet protocol theft for financial gain, privacy protection for citizens, and a prohibition on targeting of critical infrastructure that supports civilian populations. Ideally, scientific exchanges would be protected across borders, with free flow of data. The 2015 agreement between U.S. president Barack Obama and Chinese leader Xi Jinping failed to create these norms, but global views have evolved. A group of like-minded nations might be willing to speak out against China's approach and even impose costs on Beijing for undermining common-sense norms. As part of this norm-setting effort, the United States should prioritize blocking Beijing's attempt to take control of standards-setting bodies such as the International Telecommunication Union, which is the UN agency for information and communications technologies. The last election for head of the International Telecommunication Union was a big win for democratic values, but China has been pursuing a strategy of bureaucratic takeovers for years.

China holds an additional advantage in its years-long pursuit of diverse datasets. It can use that data for training artificial intelligence/machine learning (AI/ML) systems or for learning how to manipulate U.S. public opinion. China's even more comprehensive collection of data on its own population is also a ready-made roadmap to Chinese public sentiment. Targeting that internal tracking data for intelligence collection could provide a roadmap to public sentiment within China on topics from internal discontent to views on a conflict with the United States.

The United States and its partners should also work to pull even and surpass China in two critical technologies: AI/ML and quantum computing. The United States needs a revamped approach to acquiring and incorporating AI/ML capabilities in its military and intelligence planning and must establish rules for when AI/ML capabilities should be used in conflict scenarios. The faster the United States understands this technology and sets guardrails, the less likely China will be able to define the field and write the rules. In addition, the United States and its partners should undertake a sprint in quantum computing, which is a critical technology that could break current encryption and create stronger future encryption. The capability to read even encrypted data creates an incentive

for massive theft of information today for readability tomorrow. Post-quantum encryption will be necessary to deter and counter such an effort.

Another useful example is influence campaigns. In the United States, the creation and strengthening of the Foreign Agents Registration Act (FARA) made it possible to disclose details of several Chinese and other foreign information activities. While FARA is a useful tool for illuminating some behavior, it is by no means comprehensive. It is accompanied by separate reporting structures and databases for the Lobbying Disclosure Act (LDA) and the Department of Education's Section 117 disclosures, neither of which include detailed descriptions of the activities that were carried out at the behest of a foreign sponsor. Beijing has demonstrated its ability to navigate Western transparency and openness to its advantage. For example, this report documented how Beijing worked within the different confines of U.S., Australian, and UK law to advance its information interests. In the context of united front work, China generally adheres to the letter of the law, but has found ways to exploit gray areas or areas where the law is silent.

An additional challenge is developing countermeasures to combat China's transnational repression of its citizens and diaspora communities. The tool kit for achieving these ends is limited. The Federal Bureau of Investigation (FBI) and Department of Justice (DOJ) have demonstrated some resolve in expanding the number of cases they are willing to pursue, including indicting a Chinese student, Xiaolei Wu, in 2022 on charges that he stalked and threatened a democracy activist in Boston.²⁰ However, there are limited incentives to report such activity or protections for those who do so, particularly for foreign students and visitors who intend to return to China or have close family living in China. Many of the prominent stories of China's transnational harassment focus on a few vocal activists. Yet there is ample evidence that these high-profile examples account for a small amount of the intimidation and suppression of free speech and academic freedom that often goes unreported out of fear of consequences for oneself and one's family. Moreover, Chinese diaspora populations—rather than Chinese government entities—are often heavily involved in harassing and threatening other members of the diaspora.²¹

Xi Jinping and the CCP have repeatedly and clearly expressed a belief that their rules legitimately extend to Chinese citizens wherever they reside or travel. Identifying the right mechanisms to deter such behavior, through a combination of punishment,

awareness, and policy, is a key challenge for Western democracies to uphold the tenets of freedom of expression and to protect their sovereignty from Chinese aggression and authoritarianism.

One of the most effective examples of a strong defense is the growing opposition to Confucius Institutes. By 2009, there were 90 Confucius Institutes housed at U.S. universities—including prestigious institutions such as Columbia, Stanford, and the University of Chicago—and a total of 440 across the globe.²² But the Confucius Institutes quickly became a lightning rod for controversy. At the University of Chicago, more than 100 professors signed a petition calling on the university to terminate its contract with Hanban.²³ Bruce Lincoln, the Caroline E. Haskell distinguished service professor of the history of religions at the University of Chicago, helped lead the charge, arguing that the institute was a potentially dangerous “sort of arrangement where an entity outside the university . . . is in effect seriously influencing who's teaching and what's taught under our name and inside our curriculum.”²⁴ By 2023, Confucius Institutes had largely disappeared on U.S. college and university campuses, with only a dozen remaining.²⁵

Not surprisingly, China has shifted to other programs, such as the Thousand Talents Plan, to recruit experts in science and technology. Some academics, such as Charlie Lieber, chair of Harvard University's Department of Chemistry and Chemical Biology, were arrested and convicted in connection with lying to federal authorities about affiliation with the Thousand Talents Plan.²⁶ Other countries, such as Canada, have also expressed alarm at China's attempts to infiltrate universities and other institutions through the Thousand Talents Plan and other programs.²⁷ As the Canadian Security Intelligence Service concluded: “[F]oreign talent recruitment programs are used to advance the economic and strategic objectives of foreign states at the expense of Canada's national interests. The Thousand Talents Plan is an example of academic talent plans that are used to advance foreign states' interests.”²⁸

In sum, the United States can take several steps to strengthen defense against Chinese political warfare:

- **Toughen Cyber Resilience:** The Office of the National Cyber Director and the Cyber Infrastructure and Security Agency, which sits within the Department of Homeland Security, have made tremendous strides building consensus around strengthening cyber defenses within the U.S. government

and in the private sector. But more dramatic action will be necessary to incentivize—and perhaps regulate—better cybersecurity.

- **Increase Federal Counterintelligence Resources:** Boost FBI, DOJ, and Department of Homeland Security (DHS) resources to conduct Chinese counterintelligence operations against the MSS, MPS, PLA, United Front Work Department, and other organizations. The FBI is particularly swamped with Chinese counterintelligence cases, according to CSIS discussions with the FBI. The FBI should be given additional resources to hire more counterintelligence agents and intelligence analysts, including Mandarin-proficient personnel.

- **Expand State and Local Counterintelligence Activities:** There is a growing need to supplement U.S. federal efforts by expanding state and local efforts. New Jersey, for example, has stepped up counterintelligence efforts under the New Jersey Office of Homeland Security and Preparedness. The Analysis Bureau in New Jersey has devoted greater resources to analyzing Chinese intelligence and disinformation activities, including through cooperation with the FBI. The Analysis Bureau has also added a critical infrastructure analysis section to analyze Chinese and other foreign threats and advocate for better operational security practices. New Jersey has also distributed its products to local law enforcement agencies and the general public to increase awareness.²⁹ These efforts should be widespread across states.

- **Declassify Intelligence Analysis:** There is an urgent need to increase public awareness of the Chinese threat to the U.S. homeland by declassifying more information and analysis from the U.S. intelligence community, FBI, DHS, Department of State, Department of Defense, and Department of Treasury. There have been some useful examples, such as the National Intelligence Council's declassified "Cyber Operations Enabling Expansive Digital Authoritarianism."³⁰ But these cases are few and far between. In the 1980s, for instance, the CIA and FBI released a range of intelligence products on Soviet political warfare as part of congressional hearings.³¹ Along these lines, Congress can play an increasingly important role in raising public awareness through hearings, analytical products, and other

activities—including through the Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party.

- **Crack Down on Sensitive Technology:** There is a growing urgency to mitigate the threat from China's intelligence collection and information operations on technology platforms through a combination of executive, legislative, and judicial steps. For example, TikTok should be banned from all state and local devices—not just federal ones—because it allows China to access the devices, including information, microphones, and cameras. There is also a need to contextualize public education efforts with concrete examples of negative impacts or threats to the U.S. public. This is increasingly important because China's irregular activities directly target citizens in the United States and other Western countries via popular online social media, gaming, and e-commerce platforms, many of which are accompanied by China's own information campaigns that extol these platforms' benefits.
- **Increase Private Sector Awareness:** Intensify U.S. government interactions with corporations, educational institutions, think tanks, and other entities about China's influence and coercive activity. Chinese influence campaigns have targeted a wide range of U.S. organizations and companies, including Hollywood movie studios and the National Basketball Association. Consequently, there is an urgent need for the FBI, DHS, and intelligence community to increase interactions with targeted institutions and to educate their personnel about evolving Chinese methods and practices.
- **Strengthen FARA and Related Efforts:** There is a continuing need to further strengthen FARA and other efforts, including the Lobbying Disclosure Act and the Department of Education's Section 117 disclosures, to counter Chinese and other foreign influence. Examples might include providing civil investigative demand authority to the Department of Justice, increasing penalties for non-compliance with registration requirements, and repealing or modifying FARA exemptions.

CONDUCT OFFENSIVE MEASURES

In a letter to U.S. painter and Revolutionary War veteran John Trumbull, George Washington wrote that “offensive operations, often times, is the surer, if not the only . . . means of defence.”³² Political warfare with China should not only involve playing defense but also conducting offensive measures in such areas as information and cyber operations.

As used here, *offense* refers to efforts to coerce or weaken an adversary. An offensive campaign should be based, in part, on leveraging U.S. democratic strengths and exploiting China’s weaknesses, including the vulnerabilities inherent to its attempt to suffocate political liberty, freedom of expression and the press, free-market capitalism, and freedom of religion. The fundamental goal of China’s leadership is to retain and solidify their absolute power and to eliminate any effective opposition to their authority.

U.S. offensive policy toward China should focus on thwarting China’s expansionism, power, and influence as well as encouraging a more pluralistic political and economic system in China and its partners. One example of offense is in the cyber domain. The United States should have a consistently updated set of options for action and retaliation in the cyber domain. While escalation dynamics in and through the cyber domain are still up for debate, limiting activity to cyber could prove de-escalatory in a crisis. If cyber effects are predictable and damage is targeted, cyber tools can be an effective way to send a message. However, the United States and China also need to establish consistent crisis communications channels so that the two capitals can message intent effectively if a cyber operation meant to be limited and de-escalatory has unpredicted effects.

More broadly, the United States and its partners should proactively highlight examples of China’s malign activity, human rights abuses, and corruption. Some of the best work may come from legislators, investigative journalists, academics, and corporate executives. Indeed, China has significant weaknesses and vulnerabilities that can be exploited. Examples include the BRI and DSR, which frequently aim to control information in ways that benefit China, burden foreign countries (including with debt), and rely on Chinese labor rather than local workers. China’s goal is generally to force governments and corporations to respect and defer to Chinese interests in current and future actions.³³

China has also engaged in significant human rights abuses. Examples include China’s involvement in the arrest, torture, and assassination of defectors, political opponents, and those investigating or prosecuting corruption and human rights abuses (such as journalists and lawyers). In addition, Chinese corruption and cheating scandals are pervasive. China has paid bribes to foreign officials to gain access to their country, and corruption is often critical for promotion in the CCP and military. China has also been embroiled in massive doping scandals with its athletes, including for the Olympics.

Overall, the United States should consider several recommendations to strengthen the offense in light of Chinese political warfare:

- **Weaken the Great Firewall:** The United States needs to increase resources and support to programs that provide technological and other assistance to individuals and organizations inside and outside China to break through the Great Firewall. These programs should include U.S. government agencies—such as the State Department, Defense Department, and intelligence community—as well as nongovernmental organizations and the private sector. Populations generally want access to other sources of news, not just information from state-controlled media.
- **Establish a Multilateral Bloc to Counter Chinese Economic Coercion:** Combating and deterring Chinese economic coercion will likely require a collective effort by the United States, Australia, South Korea, Japan, and other countries—including in Europe. Participant countries should be prepared to sanction China in response to Chinese threats or actions that do not conform to World Trade Organization rules and are aimed at meeting Chinese political goals unrelated to trade. In addition, participant countries could create a collective compensation fund for losses and offer alternative export or import markets to divert trade in response to Chinese sanctions.³⁴
- **Increase Private Sector Competitiveness in Emerging Technology:** Develop a public-private partnership designed to compete more effectively with China in emerging technology in such areas as the Global South. As noted in this report, China has developed an aggressive strategy to spread Chinese

technology through the DSR. The United States and allied and partner governments should develop a coordinated approach to support U.S. and allied companies that seek to compete in these same regions, such as Google, Amazon, Apple, and Microsoft.

- **Establish a U.S. Inter-Agency Body to Coordinate Offensive Actions:** The U.S. government's China policy is still stovepiped across such areas as diplomacy, defense, economics, and intelligence. The National Security Council should create a body that coordinates strategy and operations across U.S. government agencies designed to identify Chinese vulnerabilities and exploit them. The United States needs to proactively weaken Chinese power, influence, and relationships overseas. There are several models from the Cold War that are worth examining, such as the Active Measures Working Group.

These actions will not be easy. China will respond aggressively and fiercely to any campaign designed to undermine its authoritarianism and exploit the vulnerabilities in its political and economic systems. Chinese leaders may threaten its critics, including by withholding money to—or conducting offensive cyberattacks and other actions against—corporations, educational institutions, think tanks, and other individuals and organizations. Chinese citizens and their families may be intimidated, imprisoned, tortured, or even killed.

Offensive operations will also require leveraging defectors, émigrés, and dissidents from China—including intellectuals and scientists—for information campaigns. Soviet and Eastern European defectors and dissidents were an important tool in political warfare during the Cold War and a critical source of information. Their testimonies were helpful in constructing powerful, emotional, and truthful narratives that undermined the Soviet Union and its ideology. Defectors such as Stanislav Levchenko and Ladislav Bittman also provided critical insights into how active measures worked and how to fight back.³⁵ The United States needs to find opportunities to effectively identify and exploit defectors and dissidents.

Political warfare involves taking risks. In some cases, as with the CIA's covert support to Poland's Solidarity during the 1980s, codenamed QRHELPFUL, those risks paid off by weakening the Soviet Union and its partners.³⁶ But in other cases, such as in Iran and Guatemala, the United States made

significant mistakes that ran contrary to its democratic principles. Because of these risks, some U.S. officials will strongly resist engaging in offensive activities that attempt to exploit China's weaknesses and vulnerabilities. While it is important to weigh the pros and cons of specific actions, the United States would never have succeeded in undermining Soviet power and influence without taking risks that exploited its adversary's vulnerabilities. The same is true for China moving forward.


A MULTILATERAL APPROACH

An effective strategy against Chinese political warfare requires the assistance of U.S. partners. For example, Australia blocked the purchase of Huawei 5G telecommunications gear for its national network and was an outspoken critic of China's human rights abuses and anti-democratic practices. But the threat from China against U.S. partners is likely to be persistent. As a report by the UK's Intelligence and Security Committee of Parliament concluded, "China's size, ambition and capability have enabled it to successfully penetrate *every sector* of the UK's economy, and—until the Covid-19 pandemic—Chinese money was readily accepted by [His Majesty's Government] with few questions asked."³⁷ In many cases, the United States will need to train, advise, and assist state and non-state actors across the globe to balance against China—and to work by, with, and through its partners.³⁸

The United States can build from existing arrangements, such as the Quadrilateral Security Dialogue (or Quad, which includes Japan, Australia, India, and the United States); treaty alliances with Australia, Japan, South Korea, the Philippines, and Thailand; defense relationships with Taiwan, New Zealand, Vietnam, and other countries; and the Australia-United Kingdom-United States (AUKUS) partnership. Another example is the Minerals Security Partnership, which includes Australia, Canada, the European Union, Finland, France, Japan, Norway, South Korea, Sweden, and the United Kingdom. This partnership aims to bolster and safeguard the supply of nickel, cobalt, lithium, copper, and rare-earth metals.³⁹

In response to Chinese economic coercion, the United States and its partners in the Indo-Pacific should also develop a new strategy of "collective resilience."⁴⁰ Key countries, such as Australia, Japan, the United States, and South Korea, should be prepared to cut off—and threaten to cut off—

China's access to vital goods when Beijing acts against any member. The goal should be to deter Chinese predatory activity and compel Beijing to stop if it does conduct economic coercion.



A more effective U.S. and partner strategy needs to begin with a recognition that competition with China is inescapable. The authoritarianism and illiberalism at the root of China's political and economic system is antithetical to Western Enlightenment values. Competition is, to a great extent, a struggle over ideologies and systems. Much is at stake, including the shape, make-up, and power of political norms, the international trading system, multilateral security organizations, and international institutions.⁴¹ China is vulnerable to a strategy that exploits the weaknesses of its authoritarian government at home and abroad by encouraging democratic reforms, opening up financial markets, and undermining the state's control of information. Such a strategy requires playing better defense and offense.

This is not to say that cooperation is impossible or even unpalatable. Competition and cooperation are not zero-sum. China will hopefully remain an important trading partner in the future and a critical market for U.S. and multinational companies. China's economy is growing, its manufacturing sector is the largest in the world by a wide margin, its population of 1.4 billion is an attractive market for U.S. companies, and it boasts 400 million millennials—five times as many as the United States.⁴² China and the United States also share common interests in climate change, nonproliferation, global energy markets, counterterrorism, trade, and other areas. Not all competition is bad. Athletes, companies, spelling bee contestants, students, and even universities compete with each other. Healthy competition can benefit everyone.

The United States and other democratic countries should ultimately take solace that democracy—with all its flaws and inconsistencies—is still an enviable form of government. As Winston Churchill remarked: "Many forms of Government have been tried, and will be tried in this world of sin and woe. No one pretends that democracy is perfect or all-wise. Indeed it has been said that democracy is the worst form of Government except for all those other forms that have been tried from time to time."⁴³ Churchill's words are a helpful reminder that the United States' democratic principles are its strongest weapons against Chinese political warfare.

ABOUT THE AUTHORS

Seth G. Jones is senior vice president, Harold Brown Chair, and director of the International Security Program at the Center for Strategic and International Studies (CSIS). He also teaches at Johns Hopkins University's School of Advanced International Studies (SAIS) and the Center for Homeland Defense and Security (CHDS) at the U.S. Naval Postgraduate School. Prior to joining CSIS, Dr. Jones was the director of the International Security and Defense Policy Center at the RAND Corporation. He also served as representative for the commander, U.S. Special Operations Command, to the assistant secretary of defense for special operations. Before that, he was a plans officer and adviser to the commanding general, U.S. Special Operations Forces, in Afghanistan (Combined Forces Special Operations Component Command–Afghanistan). In 2014, Dr. Jones served on a congressionally mandated panel that reviewed the FBI's implementation of counterterrorism recommendations contained in the 9/11 Commission Report. He is the author of *Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare* (W.W. Norton, 2021), *A Covert Action: Reagan, the CIA, and the Cold War Struggle in Poland* (W.W. Norton, 2018), *Waging Insurgent Warfare: Lessons from the Vietcong to the Islamic State* (Oxford University Press, 2016), *Hunting in the Shadows: The Pursuit of al Qaeda since 9/11* (W.W. Norton, 2012), and *In the Graveyard of Empires: America's War in Afghanistan* (W.W. Norton, 2009). Dr. Jones has published articles in a range of journals, such as *Foreign Affairs*, *Foreign Policy*, and *International Security*, as well as newspapers and magazines like the *New York Times*, *Washington Post*, and *Wall Street Journal*. Dr. Jones is a graduate of Bowdoin College and received his MA and PhD from the University of Chicago.

Emily Harding is deputy director and senior fellow with the International Security Program at CSIS. She joined CSIS from the Senate Select Committee on Intelligence (SSCI), where she was deputy staff director. In her nearly 20 years of government service, she has served in a series of high-profile national security positions at critical moments. While working for the SSCI, she led the committee's multiyear investigation into Russian interference in the 2016 elections. During her tenure on the committee, she also served as the subject matter expert on election security, counterintelligence and associated cybersecurity

issues, and the Middle East. She began her career as a leadership analyst at CIA, and then became a manager of analysts and analytic programs. During a tour at the National Security Council, she served as executive assistant to the deputy national security adviser for global democracy strategy and then as director for Iran, where she led interagency efforts to create innovative policies drawing on all elements of national power. After leaving the White House, she served on a team running the first Office of the Director of National Intelligence-led presidential transition, where she was responsible for liaising with both campaigns and briefing the incoming administration on a wide range of intelligence topics. Harding holds a master's degree in public policy from Harvard University's Kennedy School of Government and a bachelor's degree in foreign affairs from the University of Virginia.

Catrina Doxsee is an associate director and associate fellow for the Transnational Threats Project at CSIS, where she analyzes international and domestic terrorism and the irregular activities of countries such as Iran, Russia, and China. Outside of CSIS, she is a member of the editorial board for the Irregular Warfare Initiative at the Modern War Institute at West Point and was the 2021 counterterrorism fellow at Young Professionals in Foreign Policy. Prior to joining CSIS, Ms. Doxsee worked as an associate policy analyst at the Migration Policy Institute. She has also conducted research at the Philip Merrill Center for Strategic Studies at Johns Hopkins and the U.S. Treasury Department's Middle East and North Africa Office. She previously served for two years in AmeriCorps as a refugee resettlement caseworker in Pittsburgh. Ms. Doxsee holds a BA in history, with a concentration in military history, from the University of Chicago and an MA in strategic studies and international economics from the Johns Hopkins School of Advanced International Studies.

Jake Harrington was the intelligence fellow in the International Security Program at CSIS, where his research focused on emerging technology, strategic competition, irregular warfare, cybersecurity, and intelligence operations. Before CSIS, he worked for more than 10 years at the Federal Bureau of Investigation (FBI). At the FBI, Mr. Harrington was an intelligence analyst in the Counterterrorism and Counterintelligence Divisions and served as a special assistant to several senior FBI officials. From 2018 to 2020, he advised the FBI's chief information officer on enterprise technology modernization, data

analytic strategy, and cybersecurity matters. He also completed a joint duty assignment as legislative liaison officer at the Office of the Director of National Intelligence (ODNI). In this position, he managed the congressional engagement portfolio for the National Counterterrorism Center (NCTC), the National Counterintelligence and Security Center (NCSC), and other ODNI components. He holds a master's degree in international relations and international economics from the Johns Hopkins University School of Advanced International Studies and a bachelor's degree in political science from Davidson College. He is a recipient of an FBI Director's Award, an FBI Medal of Excellence, an ODNI National Counterintelligence and Security Award, and an Office of the Secretary of Defense Medal for Exceptional Public Service.

Riley McCabe is a program coordinator and research assistant for the Transnational Threats Project at CSIS. His research focuses on military operations, emerging technologies, and the irregular warfare activities of countries such as Russia and China. Riley has previously supported the work of the intelligence fellow, the fellow for future war, gaming, and strategy, and the Risk and Foresight Group at CSIS. He holds a BA from Occidental College in diplomacy and world affairs.

APPENDIX¹

Examples of Chinese Private Security Companies Operating Abroad

COMPANY NAME	SAMPLE LOCATIONS	TYPES OF TASKS PERFORMED	SAMPLE CLIENTS
Beijing DeWe Security Service Group (Dulwich Group, DWSS) (德威国际安保集团)	Australia, Cameroon, Canada, Chad, China, Democratic Republic of the Congo, Djibouti, Ethiopia, Gabon, Kenya, Nigeria, South Sudan, Thailand, United Kingdom*, United States*	Explosives removal, maritime escort, personnel security, physical security, risk assessment, security consulting, security design, security technology protection, security training, surveillance	China Communications Construction Company, China Development Bank, China National Petroleum Corp., China Petroleum and Chemical Corp., China Poly Group Corp., China Roads and Bridges Corp., China State Construction Engineering Corp., China Three Gorges Corp., Chinese embassies in Kenya and Madagascar, Hanban, Industrial and Commercial Bank of China, Chinese Ministry of Commerce, Chinese Ministry of Education, Chinese Ministry of Foreign Affairs, Poly-GCL Petroleum Group Holdings, Sinopec
China Security & Protection Group (北京中安保实业有限公司)	Cambodia, China, Kyrgyzstan, Laos, Malaysia, United Arab Emirates, United States*	Event security, maritime escorts, personnel security, physical security, risk assessment, security training, transportation security	Beijing Security Association, China Security and Fire Co. Ltd., Papua New Guinea Commercial Commissioner's Office, Public Security Bureau of Xinyuan County, Xinjiang
China Security Technology Group (中国安保技术集团)	Algeria, Angola, Cambodia, China, Gulf of Aden, Gulf of Guinea, Iraq, Kenya, Lamu Port-South Sudan-Ethiopia Transport (LAPSSET) corridor, Mozambique, Nigeria, Pakistan, Sri Lanka, Uzbekistan, Zimbabwe	Armed maritime and land escort, equipment supply, intelligence analysis, personnel security, physical security, risk assessment, security design, security technology protection, security training	CCCC Fourth Harbor Engineering Co., Ltd., China-Brazil Petrochemical Co., Ltd., China Construction Group Third Engineering Bureau, China Gezhouba Group, China Oceanwide Online (Uzbekistan insurance platform), China Power Construction Group Co., Ltd., Chinese embassies in Sri Lanka and Mozambique, Chinese shipping fleets, Grand Tai Peru SAC, Huawei Technologies Pakistan, Jiangsu Energy International Co., Sengwa power plant (Zimbabwe)
Chinese Overseas Security Services (中国海外保安集团)	Argentina, Cambodia, China, Djibouti, Ethiopia, Indonesia, Iraq, Jordan, Laos, Malaysia, Mozambique, Pakistan, Somalia, South Africa, Sri Lanka, Thailand, Turkey, Zambia	Anti-terrorism training, BRI projects protection, event security, maritime escort, personnel security, physical security, risk assessment, security consulting	Chinese factories in special economic zones, Chinese-funded overseas enterprises, Chinese embassy in Somalia
China Shield Consulting Service (中安华盾咨询服务有限公司)	Bangladesh, China, Kazakhstan, Pakistan, Thailand, United States*	Armed escort, event security, personnel security, physical security, risk assessment, security consulting, security technology protection	Agricultural Bank of China, AO "COII Kyzer" (leading private security provider, formerly part of the Kazakhstan Ministry of International Affairs), Bank of China, China Construction Bank, China Merchants Bank, China-Thailand Economic and Trade Cooperation Exchange Conference
Frontier Services Group (先锋服务集团)	Bermuda, Cambodia, China, Democratic Republic of the Congo, Indonesia, Iraq, Kenya, Laos, Malta, Mozambique, Myanmar, Nigeria, Somalia, South Africa, South Sudan, Uganda, United Arab Emirates	Aviation rescue, cargo and logistics protection, emergency rapid response, insurance package services, logistics channel construction, personnel security, physical security, risk assessment, security strategy design, security technology protection, security training	Chinese state-owned enterprises in aviation, oil and gas, logistics, road construction, transportation, and medical evacuation, DRC Chinese Enterprises Association, Laos Ministry of Public Security Railway Police Department, Xinjiang Production and Construction Corps

COMPANY NAME	SAMPLE LOCATIONS	TYPES OF TASKS PERFORMED	SAMPLE CLIENTS
Hanwei International Security Services	China, Iraq, Laos, Myanmar, Nigeria, Pakistan, Papua New Guinea, South Africa, Sri Lanka	Antipiracy and counterterrorism training, cargo transportation escort, equipment supply, intelligence analysis, maritime escort, oil drilling platform protection, personnel security, physical security, risk assessment, security consulting	China National Petroleum Corp., Chinese-funded enterprises, Shanghai Duan and Duan (Chongqing) Law Firm
Hua Xin Zhong An (Beijing) Security Service (HXZA) (华信中安集团)	China, Djibouti, Egypt, Gulf of Aden, Gulf of Guinea, Pakistan, Somalia, Sri Lanka	Advanced security technology supply for surveillance and early warning capabilities, armed maritime escort, armed security aboard ships, event security, maritime logistics, personnel security, physical security, risk assessments, security consulting, security technology protection	China Ocean Shipping Co., COSCO SHIPPING Development (formerly China Shipping Container Lines) fleets, Chinese television crew covering a kidnapping of two Chinese nationals in Quetta, Pakistan
Shandong Huawei Security Group (山东华威保安集团)	China, Kenya, South Africa	Emergency rapid response, event security, physical security, protection of mines and oil installations, risk assessment, security compliance, security consulting, security training	Chinese-owned mining companies, Huawei, MSS Security Group (joint venture), PetroChina, Raid Private Security (joint venture), Rostec (Russian state-owned conglomerate) (strategic cooperation agreement), Sinopec
VSS Security Group (伟之杰安保集团)	China, Iraq, South Sudan, Sudan	Armed maritime escort, emergency rapid response, personnel protection, physical security, ransom and kidnapping management, risk assessment, security compliance, security consulting, security technology protection, security training	PetroChina, China Machinery Engineering Corp., China National Petroleum Corp.
Xinjiang Shamo Teweï (新疆沙漠特卫)	China, Kazakhstan	Event security, personnel protection, physical security, property patrol, security training	Overseas Chinese corporations, Chinese engineering firms
Zhongjun Junhong (中军军弘安保集团)	Afghanistan, Cambodia, China, Comoros, Georgia, Ghana, Gulf of Aden, Gulf of Guinea, Gulf of Persia, Iraq, Kenya, Kuwait, Kyrgyzstan, Laos, Madagascar, Malacca Strait, Malaysia, the Philippines, Red Sea, South Africa, Sri Lanka, Sulu Sea, Taiwan, Tanzania, Thailand, United Arab Emirates, United Kingdom*	Anti-piracy consulting, armed maritime escort, maritime logistics, overseas emergency rescue, physical security, risk assessment, security technology protection, security training, unarmed offshore platforms escort, weapon configuration	Overseas Chinese-funded enterprises, China Railway No. 5 Engineering Group, China Road and Bridge Corp., Chinese embassy in Bishkek, Guangdong Precious Metal Refinery, Huawei Technologies, Jufeng Industry Group Co. Ltd., Sanmenxia Luqiao Construction Group, Sinohydro Bureau 16, Zijin Mining Group

* INDICATES BRANCH OFFICE LOCATION RATHER THAN ONGOING OPERATIONS.

ENDNOTES

- 1 George F. Kennan, "The Inauguration of Organized Political Warfare," Office of the Historian, History and Public Policy Program Digital Archive, April 30, 1948, <https://history.state.gov/historicaldocuments/frus1945-50intel/d269>.

Executive Summary

- 1 Xi Jinping, "Full Text: 2023 New Year Address by President Xi Jinping," Embassy of the People's Republic of China in the United Kingdom of Great Britain and Northern Ireland, December 31, 2022, http://gb.china-embassy.gov.cn/eng/zqyw/202212/t20221231_10999475.htm.
- 2 习近平 [Xi Jinping], "国家主席习近平发表二〇二三年新年贺词" [President Xi Jinping Delivered A New Year's Message in 2023], 中华人民共和国国务院公报 [State Council Gazette of the People's Republic of China], no. 1, serial no. 1792, (January 10, 2023), https://www.gov.cn/qongbao/content/2023/content_5736705.htm.
- 3 Authors' interview with FBI agent, June 2023.
- 4 George F. Kennan, "The Inauguration of Organized Political Warfare," Office of the Historian, History and Public Policy Program Digital Archive, April 30, 1948, <https://history.state.gov/historicaldocuments/frus1945-50intel/d269>.
- 5 Xi Jinping, "Full Text: 2023 New Year Address by President Xi Jinping," Embassy of the People's Republic of China in the United Kingdom of Great Britain and Northern Ireland, December 31, 2022, http://gb.china-embassy.gov.cn/eng/zqyw/202212/t20221231_10999475.htm.
- 6 Kennan, "The Inauguration of Organized Political Warfare."

1. Introduction

- 1 Xi Jinping, "Hold High the Great Banner of Socialism with Chinese Characteristics and Strive in Unity to Build a Modern Socialist Country in All Respects: Report to the 20th National Congress of the Communist Party of China," CGTN, October 16, 2022, <https://news.cgtn.com/news/files/Full-text-of-the-report-to-the-20th-National-Congress-of-the-Communist-Party-of-China.pdf>.
- 2 习近平 [Xi Jinping], "高举中国特色社会主义伟大旗帜 为全面建设社会主义现代化国家而团结奋斗——在中国共产党第二十次全国代表大会上的报告" [Hold High the Great Banner of Socialism with Chinese Characteristics and Strive in Unity to Build a Modern Socialist Country in All Respects: Report to the 20th National Congress of the Communist Party of China], 新华社 [Xinhua News Agency], October 25, 2022, https://www.gov.cn/xinwen/2022-10/25/content_5721685.htm.
- 3 While definitions vary of such terms as gray zone actions, irregular warfare, asymmetric activities, and unrestricted warfare, they are similar to what this report defines as political warfare. On these other terms see, for example, Bonny Lin et al., *Competition in the Gray Zone: Countering China's Coercion Against U.S. Allies and Partners in the Indo-Pacific* (Santa Monica, CA: RAND, 2022), https://www.rand.org/pubs/research_reports/RR594-1.html; Kathleen H. Hicks et al., *By Other Means, Part I: Campaigning in the Gray Zone* (Lanham, MD: Rowman & Littlefield, 2019), <https://www.csis.org/analysis/other-means-part-i-campaigning-gray-zone>; Seth G. Jones, *Three Dangerous Men: Russia, China, Iran and the Rise of Irregular Warfare* (New York: W.W. Norton, 2021);

- Charles Horner, Andrew S. Erickson and Ryan D. Martinson, eds., *China's Maritime Gray Zone Operations* (Annapolis, MD: Naval Institute Press, 2019), <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=8072&context=nwc-review>; Lyle J. Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War* (Santa Monica, CA: RAND, 2019), https://www.rand.org/pubs/research_reports/RR2942.html; David Knoll, Kevin Pollpeter, and Sam Plapinger, "China's Irregular Approach to War: The Myth of a Purely Conventional Future Fight," Modern War Institute, April 27, 2021, <https://mwi.usma.edu/chinas-irregular-approach-to-war-the-myth-of-a-purely-conventional-future-fight/>; Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," National Defense University, *Prism*, vol. 7, no. 4, 2018, 31-47, <https://ccn.edu/news/article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/>; and Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Brattleboro, VT: Echo Point Books and Media, 1999).
- 4 U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China* (Washington, DC: Office of the Secretary of Defense, 2021), 1, <https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF>.
 - 5 The National Defense Strategy briefly touched on gray zone activity, including Chinese gray zone activity. U.S. Department of Defense, *2022 National Defense Strategy of the United States of America* (Washington, DC: U.S. Department of Defense, 2022), <https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF>.
 - 6 See, for example, Mark F. Cancian, Matthew Cancian, and Eric Heginbotham, *The First Battle of the Next War: Wargaming a Chinese Invasion of Taiwan* (Washington, DC: CSIS, 2023), <https://www.csis.org/analysis/first-battle-next-war-wargaming-chinese-invasion-taiwan>.
 - 7 Some exceptions on aspects of political warfare include Lin, *Competition in the Gray Zone*; Hicks, *By Other Means, Part I*; Jones, *Three Dangerous Men*; Horner, Erickson and Martinson, eds., *China's Maritime Gray Zone Operations*; Ross Babbage, *Winning Without Fighting: Chinese and Russian Political Warfare Campaigns and How the West Can Prevail*, Vol. I (Washington, DC: Center for Strategic and Budgetary Assessments, 2019), <https://csbaonline.org/research/publications/winning-without-fighting-chinese-and-russian-political-warfare-campaigns-and-how-the-west-can-prevail>; Morris, *Gaining Competitive Advantage in the Gray Zone*; and Knoll, Pollpeter, and Plapinger, "China's Irregular Approach to War."
 - 8 On the focus of irregular and gray zone activity predominantly on PLA activities see, for example, Lin, *Competition in the Gray Zone*; Peter Layton, *China's Enduring Grey-Zone Challenge* (Canberra: Air and Space Power Centre, 2021), <https://airpower.airforce.gov.au/publications/chinas-enduring-grey-zone-challenge>; James Siebens and Ryan Lucas, *Military Operations Other Than War in China's Foreign Policy* (Washington, DC: Stimson Center, 2022), <https://www.stimson.org/2022/military-operations-other-than-war-and-chinas-foreign-policy/>; and Yamaguchi Shinji, Yatsuzuka Masaaki, and Momma Rira, *China's Quest for Control of the Cognitive Domain and Gray Zone Situations* (Tokyo: National Institute for Defense Studies, 2022), http://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2023_A01.pdf.
 - 9 See "Interpret: China," CSIS, <https://interpret.csis.org/>.
 - 10 For some of the best works on political warfare, see Hal Brands, *The Twilight Struggle: What the Cold War Teaches Us about Great-Power Rivalry Today* (New Haven, CT: Yale

University Press, 2022); Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020); Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND 2018), https://www.rand.org/pubs/research_reports/RR1772.html; Hal Brands and Toshi Yoshihara, "How to Wage Political Warfare," *The National Interest*, December 16, 2018, <https://nationalinterest.org/feature/how-wage-political-warfare-38802>; Charles T. Cleveland et al., *An American Way of Political Warfare: A Proposal* (Santa Monica, CA: RAND, 2018), <https://www.rand.org/pubs/perspectives/PE304.html>; Paul A. Smith, Jr., *On Political War* (Washington, DC: National Defense University Press, 1989), <https://apps.dtic.mil/sti/pdfs/ADA233501.pdf>; Benjamin Jensen, "The Cyber Character of Political Warfare," *Brown Journal of World Affairs* 24, no. 1 (Fall/Winter 2017): 159–72, <https://www.istor.org/stable/27119085>; Carnes Lord and Frank R. Barnett, eds., *Political Warfare and Psychological Operations: Rethinking the U.S. Approach* (Washington, DC: National Defense University Press, 1989); Max Boot and Michael Doran, "Political Warfare," Council on Foreign Relations, Policy Innovation Memorandum No. 33, June 7, 2013, <https://www.istor.org/stable/resrep05693>; and David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (New York: Oxford University Press, 2020).

- 11 Brands, *The Twilight Struggle*, 103. Emphasis added.
- 12 Rid, *Active Measures*, 9.
- 13 See, for example, Lin, *Competition in the Gray Zone*; Hicks, *By Other Means, Part I*; Morris, *Gaining Competitive Advantage in the Gray Zone*; and Hoffman, "Examining Complex Forms of Conflict."
- 14 George F. Kennan, "The Inauguration of Organized Political Warfare," Office of the Historian, History and Public Policy Program Digital Archive, April 30, 1948, <https://history.state.gov/historicaldocuments/frus1945-50intel/d269>.
- 15 Kennan eventually expressed strong reservations about the United States' use of political warfare. See, for example, George F. Kennan, *The Kennan Diaries*, ed. Frank Costigliola (New York: W.W. Norton, 2014), xxix.
- 16 Jensen, "The Cyber Character of Political Warfare," 160.
- 17 U.S. Department of Defense, *Irregular Warfare (IW): Joint Operating Concept (JOC)* (Washington, DC: September 2007), 7–9, <https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc-iw-v1.pdf>.
- 18 On the functions of a state see, for example, Francis Fukuyama, *State-Building: Governance and World Order in the 21st Century* (Ithaca, NY: Cornell University Press, 2004).
- 19 See, for example, Hoffman, "On Not-So-New Warfare."
- 20 See, for example, 姜玉坤 阎永峰 [Mei Yushen and Yan Yongfeng], "沈阳军区某集团军拉开 '三战' 序幕" [A Certain Army of the Shenyang Military Region Pulls Back the Curtain on the 'Three Warfares'], *中国青年报* [*China Youth Daily*], July 17, 2004; and 侯宝成 [Hou Baocheng], "政治工作为什么要加强对 '三战' 的研究 [Why Political Work Should Step Up the Study of the 'Three Warfares']," *解放军报* [*PLA Daily*], July 29, 2004.
- 21 Sun Tzu, *The Art of War*, trans. by Samuel B. Griffith (New York: Oxford University Press, 1971), 77. Emphasis added.
- 22 Some individuals, such as Frank Hoffman, have argued that "political warfare" is a redundant term since, as Clausewitz insisted, all warfare is political. However, the concept of political warfare refers to activities below the threshold of conventional warfare, which generally do *not* include direct

violence and brute force. This is an important distinction since Clausewitz argues that war is "an act of violence intended to compel our opponent to fulfill our will." See Frank Hoffman, "On Not-So-New Warfare: Political Warfare vs. Hybrid Threats," *War on the Rocks*, July 28, 2014, <https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/>; and Carl von Clausewitz, *On War*, ed. Anatol Rapaport (New York: Penguin, 1968), 101.

- 23 Jude Blanchette, "Party of One: The CCP Congress and Xi Jinping's Quest to Control China," *Foreign Affairs*, October 14, 2022, <https://www.foreignaffairs.com/china/party-one-ccp-congress-xi-jinping>.
- 24 Kilcullen, *The Dragons and the Snakes*, 26.
- 25 See, for example, Cai Xia, "The Weakness of Xi Jinping: How Hubris and Paranoia Threaten China's Future," *Foreign Affairs*, vol. 101, no. 5, September/October 2022, <https://www.foreignaffairs.com/china/xi-jinping-china-weakness-hubris-paranoia-threaten-future>.

2. The Strategic Logic of Chinese Political Warfare

- 1 倪桂桦 朱锋 [Ni Guihua and Zhu Feng], "拜登政府对华战略竞争的态势与困境" [The Situation and Dilemmas of the Biden Administration's Strategic Competition with China], *亚太安全与海洋研究* [*Asia-Pacific Security and Maritime Affairs*], trans. Interpret: China, original work published January 26, 2022, <https://interpret.csis.org/translations/the-state-and-dilemmas-of-the-biden-administrations-strategic-competition-with-china/>.
- 2 Ibid.
- 3 On a comprehensive history of asymmetric actions see Max Boot, *Invisible Armies: An Epic History of Guerrilla Warfare from Ancient Times to the Present* (New York: W.W. Norton, 2013).
- 4 See, for example, *The Seven Military Classics of Ancient China*, translated by Ralph D. Sawyer (Boulder, CO: Westview Press, 1993).
- 5 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Brattleboro, VT: Echo Point Books and Media, 1999), 182.
- 6 Quoted in Justin Katz, "Xi Likely 'Not Aware' of All Chinese Gray Zone Operations, U.S. Intel Officer Says," *Breaking Defense*, April 5, 2023, <https://breakingdefense.com/2023/04/chinas-xi-likely-not-aware-of-everything-his-security-forces-do-us-navy-intel-commander-says/>.
- 7 See, for example, Xi Jinping, "Hold High the Great Banner of Socialism with Chinese Characteristics and Strive in Unity to Build a Modern Socialist Country in All Respects, Report to the 20th National Congress of the Communist Party of China," CGTN, October 16, 2022, <https://news.cgtn.com/news/files/Full-text-of-the-report-to-the-20th-National-Congress-of-the-Communist-Party-of-China.pdf>.
- 8 Ibid.
- 9 Peter Layton, *China's Enduring Grey-Zone Challenge* (Canberra: Air and Space Power Centre, 2021), <https://airpower.airforce.gov.au/publications/chinas-enduring-grey-zone-challenge>; and Timothy Thomas, *The Chinese Way of War: How Has it Changed?* (McLean, VA: MITRE, June 2020), <https://apps.dtic.mil/sti/pdfs/AD1114504.pdf>.
- 10 Zhongqi Pan, "Guanxi, Weiqi and Chinese Strategic Thinking," *Chinese Political Science Review* 1, no. 2 (2016): 303–21, doi:10.1007/s41111-016-0015-1.
- 11 王子晖 [Wang Zihui], "'斗争'！习近平这篇讲话大有深意" ['Struggle'! Xi Jinping's Speech Was Very Meaningful], *新华* [Xinhua], September 4, 2019, <http://www.xinhuanet.com/>

- [politics/xxixs/2019-09/04/c_1124960210.htm](https://www.scmp.com/economy/china-economy/article/3025725/xi-jinping-rallies-china-decades-long-struggle-rise-global); Also see Zhou Xin and Sarah Zheng, "Xi Jinping Rallies China for Decades-long 'Struggle' to Rise in Global Order, amid Escalating US Trade War," *South China Morning Post*, September 5, 2019, <https://www.scmp.com/economy/china-economy/article/3025725/xi-jinping-rallies-china-decades-long-struggle-rise-global>; and Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era," (speech, 19th National Congress of the Communist Party of China, October 18, 2017, November 4, 2017), https://www.chinadaily.com.cn/china/19thcpcnationalcongress/2017-11/04/content_34115212.htm.
- 12 Xi Jinping, "New Asian Security Concept for New Progress in Security Cooperation," (speech, Fourth Summit of the Conference on Interaction and Confidence Building Measures in Asia, Shanghai Expo Center, May 21, 2014), https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zjih_665391/201405/t20140527_678163.html.
 - 13 Bonny Lin et al., *Competition in the Gray Zone: Countering China's Coercion Against U.S. Allies and Partners in the Indo-Pacific* (Santa Monica, CA: RAND, 2022), v, https://www.rand.org/pubs/research_reports/RRA594-1.html.
 - 14 On balancing, see Kenneth N. Waltz, *Theory of International Politics* (New York: Addison-Wesley Publishing, 1979); Hans J. Morgenthau, *Politics among Nations: The Struggle for Power and Peace, Fourth Edition* (New York: Alfred A. Knopf, 1967); John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: W.W. Norton, 2003); and Stephen M. Walt, *The Origins of Alliances* (New York: Cornell University Press, 1987).
 - 15 Mearsheimer, *The Tragedy of Great Power Politics*, 138–67.
 - 16 Lin, *Competition in the Gray Zone*, 147.
 - 17 肖天亮 [Xiao Tianliang, ed.], *战略学 [The Science of Military Strategy]* (Beijing: National Defense University Press, 2020), 289.
 - 18 寿晓松 [Shou Xiaosong, ed.], *战略学 [The Science of Military Strategy]* (Beijing: National Defense University Press, 2020), 101.
 - 19 Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China* (Washington, DC: U.S. Department of Defense, 2022), <https://media.defense.gov/2022/Nov/29/2003122279/-1/-1/2022-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF>; Dave Aitel et al., *China's Cyber Operations: The Rising Threat to American Security* (New York, NY: Margin Research, 2022), <https://margin.re/content/files/2023/01/China-s-Cyber-Operations-Full-Report.pdf>.
 - 20 See, for example, 王照稳 付明华 [Wang Zhaowen and Fu Minghua], "信息化战争认知域作战探析" [An Exploration and Analysis of Cognitive Domain Operations in Informationized War], *解放军报* [Liberation Army News], July 28, 2015.
 - 21 Yamaguchi Shinji, Yatsuzuka Masaaki, and Momma Rira, *China's Quest for Control of the Cognitive Domain and Gray Zone Situations* (Tokyo: National Institute for Defense Studies, 2022), http://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2023_A03.pdf.
 - 22 Larry Diamond and Orville Schell, eds., *China's Influence and American Interests: Promoting Constructive Vigilance* (Stanford, CA: Hoover Institution Press, 2019), https://www.hoover.org/sites/default/files/research/docs/diamond-schell-chineseinfluence_oct2020rev.pdf.
 - 23 Timothy R. Heath, "China's Evolving Approach to Economic Diplomacy," National Bureau of Asian Research, *Asia Policy*, no. 22, July 2016, 163, <https://www.istor.org/stable/24905122>.
 - 24 戴正 洪邮生 [Dai Zheng and Hong Yousheng], "美国学界对 '灰色地带' 挑战的认知" [American Scholarly Views of the 'Gray Zone' Challenge], *国际展望 [Global Review]*, no. 4, 2019; 归泳涛 [Gui Yongtao], "'灰色地带' 之争: 美日对华博弈的新态势" ['Competing in the Gray-Zone': A New Situation in U.S.-China Engagement with China], *日本学刊 [Japanese Studies]*, no. 1, 2019; 沈志雄 [Shen Zhixiong], "'灰色地带' 与中美战略竞争" ['Gray Zone' and U.S.-China Strategic Competition], *世界知识 [World Affairs]*, no. 11, 2019; 冯武勇 刘秀玲 [Feng Wuyong and Liu Xiuling], "日本政府批准2014年版《防卫白皮书》评论" [Japanese Government Approves 2014 Edition of 'Defense White Paper' Commentary], *Xinhua News Agency*, August 5, 2014; 高兰 [Gao Lan], "日本'灰色地带事态'与中日安全困境" [Japan's 'Gray Zone Situation' and Sino-Japanese Security Dilemma], *日本学刊 [Japanese Studies]*, no. 2, 2016; 罗国强 田园馨 [Luo Guoqiang and Tian Yuanxin], "论防空识别区的性质—'灰色地带'的成因与特点" [On the Nature of Air Defense Identification Zone: Causes and Characteristics of the 'Gray Area'], *太平洋学报 [Pacific Journal]* 24, no. 5, 2016; "美媒称中美在战与和灰色地带上较量: 美先天不足" [U.S. Media Claim that U.S.-China Are Engaged in Gray Zone Competition: U.S. At a Disadvantage], *Cankao News*, May 20, 2016.
 - 25 戴正 洪邮生 [Dai Zheng and Hong Yousheng], "美国学界对 '灰色地带' 挑战的认知" [American Scholarly Views of the 'Gray Zone' Challenge], *国际展望 [Global Review]*, no. 4, 2019; and 王湘穗 [Wang Xiangsui], "混合战: 前所未有的综合" [Hybrid War: Unprecedented Integration], *解放军报 [PLA Daily]*, May 23, 2019. Also, see, for example, 吴明曦 [Wu Mingxi], *智能化战争 [Intelligent Wars]* (Beijing: National Defense Industry Press, December 2020), 500–16.
 - 26 肖天亮 [Xiao Tianliang, ed.], *战略学 [The Science of Military Strategy]* (Beijing: National Defense University Press, 2020), 289.
 - 27 See, for example, Peter A. Dutton, Isaac B. Kardon, and Conor M. Kennedy, *Qibouti: China's First Overseas Strategic Strongpoint* (Newport, RI: U.S. Naval War College, April 2020), China Maritime Report No. 6, <https://apps.dtic.mil/sti/pdfs/AD1099642.pdf>.
 - 28 See, for example, 杨颖 [Yang Ying], "和平时期军事力量运用, 目的在哪里?" [What is the Purpose of Using Military Force in Peacetime?], *China Military Network*, November 17, 2016, http://www.81.cn/jwzl/2016-11/17/content_7364178.htm. Also see, for example, Roderick Lee and Marcus Clay, "Don't Call It a Gray Zone: China's Use-of-Force Spectrum," *War on the Rocks*, May 9, 2022, <https://warontherocks.com/2022/05/dont-call-it-a-gray-zone-chinas-use-of-force-spectrum/>.
 - 29 Layton, *China's Enduring Grey-Zone Challenge*; and Timothy Thomas, *The Chinese Way of War: How Has it Changed?* (McLean, VA: MITRE, June 2020).
 - 30 王子晖 [Wang Zihui], "'斗争'! 习近平这篇讲话大有深意" ['Struggle'! Xi Jinping's Speech Was Very Meaningful], *新华 [Xinhua]*, September 4, 2019. Also see Zhou Xin and Sarah Zheng, "Xi Jinping Rallies China for Decades-long 'Struggle' to Rise in Global Order, Amid Escalating US Trade War," *South China Morning Post*, September 5, 2019, <https://www.scmp.com/economy/china-economy/article/3025725/xi-jinping-rallies-china-decades-long-struggle-rise-global>.
 - 31 "新修订的 '中国人民解放军政治工作条例' 颁行" [The Revised Version of PLA Political Work Regulations Promulgated], *中新网 [China News Service]*, December 15, 2003; and "中共中央关于颁布 '中国人民解放军政治工作条例' 的通知" [The Circular of the CCP Central Committee on Chinese People's Liberation Army Political Work Regulations], *中国共产党新闻网 [News of the Communist Party of China]*, December 15, 2003.

- 32 郭伦德 [Guo Lunde], “习近平引领统战工作进入新时代” [Xi Jinping Leads United Front Work into the New Era], China Tibet Net, December 12, 2017, https://web.archive.org/web/20190826053157/http://www.tibet.cn/cn/news/vc/201712/t20171222_5282108.html.
- 33 中国人民解放军军语 [PLA Dictionary of Military Terms] (Beijing: Military Science Press, 2011), 163. The basic definition also identifies six operations as part of MDOOTW: counterterrorism and stability maintenance operations; Humanitarian Assistance and Disaster Relief (HA/DR); operations to safeguard sovereignty and national interests; operations to safeguard safety and security; international peacekeeping; and international rescue and relief operations. See also 刘小力 [Liu Xiaoli] 军队非战争行动研究 [Research on Military Operations Other Than War] (Beijing: People's Armed Police Press, 2014), 5.
- 34 “新修订的‘中国人民解放军政治工作条例’颁行” [The Revised Version of PLA Political Work Regulations Promulgated], 中新网 [China News Service], December 15, 2003; and “中共中央关于颁布‘中国人民解放军政治工作条例’的通知” [The Circular of the CCP Central Committee on Chinese People's Liberation Army Political Work Regulations], 中国共产党新闻网 [News of the Communist Party of China], December 15, 2003.
- 35 See, for example, 姜玉坤 阎永峰 [Mei Yushen and Yan Yongfeng], “沈阳军区某集团军拉开‘三战’序幕” [A Certain Army of the Shenyang Military Region Pulls Back the Curtain on the ‘Three Warfares’], 中国青年报 [China Youth Daily], July 17, 2004; and 侯宝成 [Hou Baocheng], “政治工作为什么要加强对‘三战’的研究” [Why Political Work Should Step Up the Study of the ‘Three Warfares’].
- 36 Mao Tse-Tung, “On Correcting Mistaken Ideas in the Party,” in *Selected Works of Mao-Tse-Tung*, vol. I (Peking: Foreign Language Press, 1965), 106.
- 37 侯宝成 [Hou Baocheng], “政治工作为什么要加强对‘三战’的研究” [Why Political Work Should Step Up the Study of the ‘Three Warfares’].
- 38 王幸生著 [Wang Xingsheng, ed.], 军队政治工作学 [The Science of Military Political Work] (Beijing: Junshi Kexue 2011), 267.
- 39 Larry M. Wortzel, *The Chinese People's Liberation Army and Information Warfare* (Carlisle, PA: U.S. Army War College, Strategic Studies Institute, March 2014).
- 40 武怀堂 左军占 [Wu Huaitang and Zuo Junzhan, eds.], 心理战实用知识 [The Practical Knowledge of Psychological Warfare] (Beijing: Junshi Kexue 2006); 郝唯学 蒋杰 [Hao Weixue and Jiang Jie], “中国人民解放军心理战理论的历史发展及特点” [The History and Characteristics of PLA's Psychological Warfare Theory], 军事历史研究 [Military Historical Research], vol. 4, 2008; and 陈辉 [Chen Hui], “中国军队开展舆论战、心理战、法律战研究和训练” [China's Military Studies and Exercises Public Opinion Warfare, Psychological Warfare and Legal Warfare], 新华 [Xinhua], June 21, 2004. Also see, for example, Larry M. Wortzel, *The Chinese People's Liberation Army and Information Warfare* (Carlisle, PA: U.S. Army War College, Strategic Studies Institute, March 2014), <https://press.armywarcollege.edu/monographs/506/>.
- 41 Yu Guohua, “NDU Officer on Weaker Force Achieving Victory in Local War,” *China Military Science*, May 20, 1996. Quoted in Mark A. Stokes, “The Chinese Joint Aerospace Campaign: Strategy, Doctrine, and Force Modernization,” in James Mulvenon and David Finkelstein, eds., *China's Revolution in Doctrinal Affairs: Emerging Trends in the Operational Art of the Chinese People's Liberation Army* (Alexandria, VA: The CNA Corporation, December 2005), 273.
- 42 彭光谦 姚有志 [Peng Guangqian and Yao Youzhi, eds.], 战略学 [The Science of Military Strategy] (Beijing: Junshi kexue chubanshe, 2001), 79.
- 43 See, for example, 刘继贤 刘铮主编 [Liu Jixian and Liu Zheng, eds.], 新军事变革与军事法制建设 [The New Revolution in Military Affairs and Building a Military Legal System] (Beijing, China: PLA Press, 2005). See also 郑申侠 刘源主编 [Zheng Shenxia and Liu Yuan, eds.], 国防和军队建设贯彻落实科学发展观学习提要 [Study Materials for Completely Building the Military and National Defense] (Beijing, China: PLA Press, 2006), 192–194.
- 44 “习近平主持召开中央国家安全委员会第一次会议强调 坚持总体国家安全观 走中国特色国家安全道路 李克强张德江出席” [Xi Jinping: Adhere to the Overall National Security Concept and Follow the Path of National Security with Chinese Characteristics], 新华 [Xinhua], April 15, 2014, http://www.xinhuanet.com/politics/2014-04/15/c_1110253910.htm. Also see, for example, Timothy R. Heath, “The ‘Holistic Security Concept’: The Securitization of Policy and Increasing Risk of Militarized Crisis,” RAND, June 27, 2015, <https://www.rand.org/blog/2015/06/the-holistic-security-concept-the-securitization.html>.
- 45 For examples, see Lin, *Competition in the Gray Zone*.
- 46 Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China* (Washington, DC: Office of the Secretary of Defense, 2021), 1, <https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF>.
- 47 Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win* (Washington, DC: U.S. Department of Defense, 2019), https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/China_Military_Power_FINAL_5MB_20190103.pdf; and *ibid.*
- 48 战立鹏 [Zhan Lipeng], “毛泽东人民海军建设思想及启示” [Contemporary Lessons from Mao Zedong's Thought on Building the People's Navy], 军事历史 [Military History], no. 3, 2009, 20.
- 49 “全军实战化军事训练座谈会代表发言摘登” [All Military Actual Combat Military Training Forum Delegates Deliver a Speech], 解放军报 [PLA Daily], August 7, 2016; and “高津任战略支援部队司令员” [Gao Jin Becomes Strategic Support Force Commander], 新浪 [Sina], January 1, 2016.
- 50 See, for example, 周碧松 [Zhou Bisong], “战略边疆” [Strategic Frontiers], 军报新闻网 [Military Reporter Network], August 15, 2016.
- 51 Dave Aitel et al., *China's Cyber Operations: The Rising Threat to American Security* (New York, NY: Margin Research, 2022), <https://margin.re/content/files/2023/01/China-s-Cyber-Operations-Full-Report.pdf>; and Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China*.
- 52 Shinji, Masaaki, and Rira, *China's Quest for Control of the Cognitive Domain and Gray Zone Situations*; and Aitel, *China's Cyber Operations*.
- 53 Aitel, *China's Cyber Operations*.
- 54 See, for example, Andy Greenberg, “How China's Hacking Entered a Reckless New Phase,” *Wired*, July 19, 2021, <https://www.wired.com/story/china-hacking-reckless-new-phase/>.
- 55 Alex Joske, *Spies and Lies: How China's Greatest Covert Operations Fooled the World* (London: Hardie Grant, 2022); and Aitel, *China's Cyber Operations*.
- 56 Ken McCallum and Christopher Wray, “Joint Address by MIS and FBI Heads,” MIS, July 6, 2022, <https://www.mis.gov.uk/news/speech-by-mis-and-fbi>.
- 57 Aitel, *China's Cyber Operations*.
- 58 Defense Intelligence Agency, *China Military Power*; and Aitel, *China's Cyber Operations*.

- 59 Diamond and Schell, eds., *China's Influence and American Interests*; Anne-Marie Brady, *Magic Weapons: China's Political Influence Activities under Xi Jinping* [Washington: Wilson Center, September 2017], <https://www.wilsoncenter.org/article/magic-weapons-chinas-political-influence-activities-under-xi-jinping>; Jonas Parelló-Plesner and Belinda Li, *The Chinese Communist Party's Foreign Interference Operations: How the U.S. and Other Democracies Should Respond* [Washington, DC: Hudson Institute, June 2018], <https://www.hudson.org/foreign-policy/the-chinese-communist-party-s-foreign-interference-operations-how-the-u-s-and-other-democracies-should-respond>; and Alexander Bowe et al., *China's Overseas United Front Work: Background and Implications for the United States* [Washington, DC: U.S.-China Economic and Security Review Commission, August 24, 2018], https://www.uscc.gov/sites/default/files/Research/China%27s%20overseas%20United%20Front%20Work%20-%20Background%20and%20Implications%20for%20US_final_0.pdf.
- 60 Joske, *Spies and Lies*.
- 61 郭伦德 [Guo Lunde], “习近平引领统战工作进入新时代” [Xi Jinping Leads United Front Work into the New Era], [中国西藏网] China Tibet Network, December 12, 2017, https://web.archive.org/web/20190826053157/http://www.tibet.cn/cn/news/yc/201712/t20171222_5282108.html.
- 62 Shinji, Masaaki, and Rira, *China's Quest for Control of the Cognitive Domain and Gray Zone Situations*.
- 63 Lijian Zhao 赵立坚, Twitter post, March 12, 2020, 10:37 am, <https://twitter.com/zlj517/status/123811898828066823?lang=en>.
- 64 Jordan Greer, “The Daryl Morey Controversy, Explained: How a Tweet Created a Costly Rift between the NBA and China,” *Sporting News*, October 23, 2019, <https://www.sportingnews.com/us/nba/news/daryl-morey-tweet-controversy-nba-china-explained/togzszxh37filmpw17p9bqwi>.
- 65 Consulate-General of the People's Republic of China in Houston, “Chinese Diplomat Condemns Houston Rockets Manager for Erroneous Comments on Hong Kong,” *Xinhua News Agency*, October 6, 2019, http://www.xinhuanet.com/english/2019-10/07/c_138452633.htm.
- 66 “Briefing With Senior U.S. Government Officials on the Closure of the Chinese Consulate in Houston, Texas,” U.S. Department of State, July 24, 2020, <https://2017-2021.state.gov/briefing-with-senior-u-s-government-officials-on-the-closure-of-the-chinese-consulate-in-houston-texas/index.html>.
- 67 Xi Jinping, “Hold High the Great Banner of Socialism with Chinese Characteristics and Strive in Unity to Build a Modern Socialist Country in All Respects.” Emphasis added.
- 68 Sara Repucci and Amy Slipowitz, “Authoritarians on Offense,” *Journal of Democracy* 33, no. 2 (April 2022): 45–59, doi:10.1353/jod.2022.0017.
- 69 “Mid-Decade Challenges to National Competitiveness,” Special Competitive Studies Project, September 2022, <https://www.scspp.ai/wp-content/uploads/2022/09/SCSP-Mid-Decade-Challenges-to-National-Competitiveness.pdf>.

3. Intelligence Operations

- 1 张沅生 (Zhang Tuosheng), “中国国际军事安全危机行为研究” [Research on China's Behavior in International Military Security Crises], *世界经济与政治* [World Economics and Politics], trans. Interpret: China, Original work published April 14, 2011, <https://interpret.csis.org/translations/research-on-chinas-behavior-in-international-military-security-crises/>.
- 2 Ibid.

- 3 Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND 2018), 233, https://www.rand.org/pubs/research_reports/RR1772.html.
- 4 Angelo M. Codevilla, “Political Warfare,” in Carnes Lord and Frank R. Barnett, eds., *Political Warfare and Psychological Operations: Rethinking the U.S. Approach* (Washington, DC: National Defense University Press, 1989), 88, https://www.files.ethz.ch/isn/139664/1989-01_Political_Warfare_8-Chap.pdf.
- 5 Ralph D. Sawyer and Mei-chün Sawyer, eds., *The Seven Military Classics of Ancient China* (New York: Basic Books, 2007).
- 6 Ken McCallum and Christopher Wray, “Joint Address by MI5 and FBI Heads,” MI5, July 6, 2022, <https://www.mi5.gov.uk/news/speech-by-mi5-and-fbi>.
- 7 Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 5th ed (Los Angeles: Sage, 2012), 103.
- 8 “PRC National Intelligence Law (As Amended in 2018),” China Law Translate, <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/>.
- 9 Peter Mattis and Matthew Brazil, *Chinese Communist Espionage: An Intelligence Primer* (Annapolis, MD: Naval Institute Press, 2019).
- 10 Ibid.
- 11 Transcript of Proceedings before the Honorable Timothy S. Black, Judge, United States v. Yanjun Xu, No. 1:18-cr-0043 (S.D. Ohio. 2021), <https://storage.courtlistener.com/recap/gov.uscourts.ohsd.212371/gov.uscourts.ohsd.212371.180.0.pdf>.
- 12 Ibid.
- 13 Nicholas Eftimiades, *Chinese Intelligence Operations* (Annapolis, MD: Naval Institute Press, 1994).
- 14 “Director Wray Addresses Threats Posed to the U.S. by China,” Federal Bureau of Investigation, February 1, 2022, <https://www.fbi.gov/news/stories/director-wray-addresses-threats-posed-to-the-us-by-china-020122>.
- 15 United States v. Qiming Lin, No. 1:22-mj-00251-MMH (E.D.N.Y. 2022), <https://www.justice.gov/opa/press-release/file/1484296/download>.
- 16 “IIO Overseas,” safeguarddefenders.com/en/iio-overseas; and “China heeft illegale politiebureaus in Nederland: aanwijzingen voor intimidatie” [China has illegal police stations in the Netherlands: evidence of intimidation], RTL Nieuws, October 25, 2022, <https://www.rtlnieuws.nl/onderzoek/artikel/5342214/china-illegale-politiebureaus-nederland-dissidenten-onderzoek>.
- 17 Holger Roonemaa and Michael Weiss, “Top NATO Scientist With Security Clearance Busted Spying for China,” *The Daily Beast*, March 19, 2021, <https://www.thedailybeast.com/top-nato-scientist-with-security-clearance-busted-spying-for-china>.
- 18 Eftimiades, *Chinese Intelligence Operations*.
- 19 “U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage,” U.S. Department of Justice, May 19, 2014, <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>; and “APT1: Exposing One of China's Cyber Espionage Units,” Mandiant, accessed September 16, 2022, <https://www.mandiant.com/resources/reports/apt1-exposing-one-chinas-cyber-espionage-units>.
- 20 John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era* (Washington, DC: NDU Press,

- 2018), https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.
- 21 In previous court filings, the U.S. Department of Justice has defined Chinese intelligence cut-outs and co-optees as “a mutually trusted person or mechanism used to create a compartment between members of an operation to enable them to pass material and/or messages securely. A cut-out or co-optee can operate under a variety of covers, posing as diplomats, journalists, academics, or business people both at home and abroad. These individuals are tasked with spotting, assessing, targeting, collecting, and running sources that have access to classified, open-source, proprietary, or sensitive information that the government of the PRC can utilize for economic, political, or military decision-making or advantage.” See Indictment, United States v. Candace Marie Claiborne, No. 1:17-cr-00069-RDM (D.D.C. 2017), https://storage.courtlistener.com/recap/gov.uscourts.dcd.185733/gov.uscourts.dcd.185733.8.0_1.pdf.
 - 22 In October 2022, the White House issued new guidelines to govern U.S. signals intelligence activities, which extended existing prohibitions against using U.S. intelligence capabilities to collect information for commercial gain, specifically: “It is not a legitimate objective to collect foreign private commercial information or trade secrets to afford a competitive advantage to United States companies and United States business sectors commercially. The collection of such information is authorized only to protect the national security of the United States or of its allies or partners.” See “Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities,” The White House, October 7, 2022, <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/>.
 - 23 Zhongwen Huo and Zongxiao Wang, *Sources and Techniques of Obtaining National Defense Science and Technology Intelligence* (Guofang Keji Qingbaoyuan Ji Huoqu Jishu) (Beijing: Kexue Jishu Wenxuan Publishing Co., 1991), <https://irp.fas.org/world/china/docs/sources.html>.
 - 24 Ibid.
 - 25 Ibid.
 - 26 For more detail on the agent acquisition cycle, see Randy Burkett, “An Alternative Framework for Agent Recruitment: From MICE to RASCLS,” *Studies in Intelligence* 57, no. 1 (Extracts, March 2013) <https://www.cia.gov/static/3e909813c3f24f6a6481524038bcace/Alt-Framework-Agent-Recruitment.pdf>; Lowenthal, *Intelligence*, 103; and Donald A. Petkus “Ethics of Human Intelligence Operations: Of MICE and Men,” *International Journal of Intelligence Ethics* 1, no. 1 (Spring 2010), <https://journals.flvc.org/ijie/article/view/83436/petkus>.
 - 27 Roger Faligot and Natasha Lehrer, *Chinese Spies: From Chairman Mao to Xi Jinping*, updated English edition (London: Hurst & Company, 2019); and Mattis and Brazil, *Chinese Communist Espionage*.
 - 28 Alex Joske, *Spies and Lies: How China's Greatest Covert Operations Fooled the World* (London: Hardie Grant, 2022).
 - 29 See Indictment, United States v. Candace Marie Claiborne.
 - 30 Statement of Offense, United States v. Jun Wei Yeo, No. 1:20-cr-00087-TSC (D.D.C. 2020), <https://storage.courtlistener.com/recap/gov.uscourts.dcd.219179/gov.uscourts.dcd.219179.9.0.pdf>.
 - 31 Another earlier example is the case of Tai Shen Kuo. Kuo, a Taiwanese-American businessman, lived in the United States for decades before he was imprisoned for his activities on behalf of Chinese intelligence, which included recruiting and handling two Americans who provided him with classified U.S. defense information. Kuo established two front companies purportedly designed to secure U.S. defense contracts related to military sales to Taiwan, which he used as a platform to cultivate relationships with cleared current and former U.S. government employees. Kuo presented himself as pro-Taiwan, appealing to his potential recruits as someone who represented an ostensible U.S. ally, even though Kuo was in regular contact with a China-based intelligence official. This is a more traditional approach to the “false flag” HUMINT operation, a technique where intelligence officers present themselves as representatives of a different country or organization than the one they truly represent. See Statement of Facts, United States v. Tai Shen Kuo, No. 1:08-cr-00179-LMB (E.D. Va. 2008), <https://storage.courtlistener.com/recap/gov.uscourts.vaed.229573/gov.uscourts.vaed.229573.45.0.pdf>. For additional insight into the anatomy and ethics of false flag HUMINT operations, see James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, (Washington, DC: Potomac Books, 2006), 52–57.
 - 32 Proxies also work on behalf of the MSS within China. U.S. Department of State employee Candace Claiborne was initially evaluated by an individual who presented himself as a Shanghai-based spa owner and restaurateur but who was actually operating as a cut-out for the MSS's Shanghai State Security Bureau (SSSB). See Indictment, United States v. Candace Marie Claiborne.
 - 33 “German Spy Agency Warns of Chinese LinkedIn Espionage,” BBC News, December 10, 2017, <https://www.bbc.com/news/world-europe-42304297>.
 - 34 McCallum and Wray, “Joint Address by MIS and FBI Heads.”
 - 35 “German Intelligence Unmasks Alleged Covert Chinese Social Media Profiles,” Reuters, December 10, 2017, <https://www.reuters.com/article/us-germany-security-china-idUSKBN1E40CA>.
 - 36 Two American citizens convicted of various charges related to their relationships with Chinese intelligence officers—Kevin Mallory and Shapour Moinian—were initially approached by Chinese intelligence on LinkedIn after they had separated from government service. See Memorandum Opinion, United States v. Kevin Patrick Mallory, No. 1:17-cr-154 (E.D. Va. 2018), <https://storage.courtlistener.com/recap/gov.uscourts.vaed.368226/gov.uscourts.vaed.368226.201.0.pdf>; and Compliant for Violation of: Title 18, U.S.C. Sec 1001 - False Statements, United States v. Shapour Moinian, No. 3:21-mj-03884-AGS (S.D. Cal. 2021), <https://storage.courtlistener.com/recap/gov.uscourts.casd.718325/gov.uscourts.casd.718325.1.0.pdf>.
 - 37 Statement of Offense, United States vs. Jun Wei Yeo.
 - 38 Ibid.
 - 39 See Criminal Indictment, United States v. Wu Zhiyong et al., No. 1:20-cr-00046-UNA (N.D. GA. 2020), <https://storage.courtlistener.com/recap/gov.uscourts.qand.273226/gov.uscourts.qand.273226.1.0.pdf>; “Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People,” U.S. Department of Justice, May 9, 2019, <https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including>; and News Service, “Man Accused of Using OPM Hack Malware,” *Washington Post*, August 25, 2017, https://www.washingtonpost.com/national/chinese-man-charged-with-using-malware-linked-to-opm-hack/2017/08/25/a0680be8-8486-11e7-b359-15a3617c767b_story.html.
 - 40 For analysis of how China may use this data, see, for example, Sina Beaghley, Joshua Mendelsohn, and David

Stebbins, "What Is the Adversary Likely to Do with the Clearance Records for 20 Million Americans?," RAND, January 20, 2017, <https://www.rand.org/blog/2017/01/what-is-the-adversary-likely-to-do-with-the-clearance.html>.

- 41 Burkett, "An Alternative Framework for Agent Recruitment."
- 42 Statement of Offense, United States vs. Jun Wei Yeo.
- 43 Katherine Herbig, *Changes in Espionage by Americans: 1947-2007* (Washington, DC: U.S. Department of Defense, March 2008), <https://apps.dtic.mil/sti/pdfs/ADA479738.pdf>.
- 44 Memorandum Opinion and Affidavit in Support of an Application for a Criminal Complaint and Arrest Warrant, United States v. Kevin Patrick Mallory, No. 1:17-cr-154 (E.D. Va. 2017), <https://storage.courtlistener.com/recap/gov.uscourts.vaed.368226/gov.uscourts.vaed.368226.201.0.pdf>.
- 45 Burkett, "An Alternative Framework for Agent Recruitment."
- 46 McCallum and Wray, "Joint Address by MI5 and FBI Heads."
- 47 Government's Sentencing Memorandum, United States v. Kun Shan Chun, No. 1:16-cr-00518-VM (S.D. NY. 2017), <https://storage.courtlistener.com/recap/gov.uscourts.nysd.461408/gov.uscourts.nysd.461408.13.0.pdf>.
- 48 United States' Memorandum in Opposition to Defendant's Motion to Dismiss Counts 1 and 2, United States v. Yanjun Xu, No. 1:18-cr-00043-TDB (S.D. Ohio 2019), <https://storage.courtlistener.com/recap/gov.uscourts.ohsd.212371/gov.uscourts.ohsd.212371.68.0.pdf>.
- 49 Transcript of Proceedings Before the Honorable Timothy S. Black, Judge, United States vs. Yanjun Xu.
- 50 Ibid.
- 51 Ibid.
- 52 Ibid.
- 53 The tradecraft in the Xu case, particularly the ways in which Xu communicated with his sources and the cover that he used to justify the exchange of information and money, is mirrored in other economic espionage cases. In the case of Hao Zhang, a scientist who provided trade secrets to the Chinese Academy of Sciences (CAS) Nanjing Institute of Soil Sciences (NISS) as part of an application for a prestigious position and entry into the Hundred Talents program, a similar process of information refinement appears to have taken place over the course of several years. Unfortunately, unlike the Xu case, the direct role of the MSS in that investigation is unknown. See Sealed Indictment, United States v. Yanjun Xu, No. 1:18-cr-00043-TSB (S.D. Ohio 2018), <https://storage.courtlistener.com/recap/gov.uscourts.ohsd.212371/gov.uscourts.ohsd.212371.1.0.pdf>.
- 54 U.S. Attorney's Office, Eastern District of New York, "Federal Jury Convicts Three Defendants of Interstate Stalking of Chinese Nationals in the U.S. and Two of Those Defendants for Acting or Conspiring to Act on Behalf of the People's Republic of China," June 20, 2023, <https://www.justice.gov/usao-edny/pr/federal-jury-convicts-three-defendants-interstate-stalking-chinese-nationals-us-and>.
- 55 "Two Arrested for Operating Illegal Overseas Police Station of the Chinese Government," U.S. Department of Justice, April 17, 2023, <https://www.justice.gov/opa/pr/two-arrested-operating-illegal-overseas-police-station-chinese-government>.
- 56 William K. Rashbaum and Karen Zraick, "FBI Arrests Two on Charges Tied to Chinese Police Outpost in New York," *New York Times*, April 18, 2023, <https://www.nytimes.com/2023/04/17/nyregion/fbi-chinese-police-outpost-nyc.html>.
- 57 Quoted in Megha Rajagopalan and William K. Rashbaum, "With F.B.I. Search, U.S. Escalates Global Fight Over Chinese Police

Outposts," *New York Times*, January 12, 2023, <https://www.nytimes.com/2023/01/12/world/europe/china-outpost-new-york.html>.

- 58 "40 Officers of China's National Police Charged in Transnational Repression Schemes Targeting U.S. Residents," U.S. Department of Justice, April 17, 2023, <https://www.justice.gov/opa/pr/40-officers-china-s-national-police-charged-transnational-repression-schemes-targeting-us>.
- 59 See, for example, "34 Officers of People's Republic of China National Police Charged with Perpetrating Transnational Repression Scheme Targeting U.S. Residents," U.S. Department of Justice, Eastern District of New York, April 17, 2023, <https://www.justice.gov/usao-edny/pr/34-officers-peoples-republic-china-national-police-charged-perpetrating-transnational>.
- 60 "U.S. Entertainer Convicted of Engaging in Foreign Influence Campaign," U.S. Department of Justice, April 26, 2023, <https://www.justice.gov/opa/pr/us-entertainer-convicted-engaging-foreign-influence-campaign>.
- 61 Bethany Allen-Ebrahimian and Alison Snyder, "Fake Bomb Threats Used to Harass China Critics," *Axios*, April 2, 2023, <https://www.axios.com/2023/03/29/chinese-activists-false-bomb-threats>.
- 62 United States of America v. Sun Hoi Ying, Sealed Complaint, 22 MAG 1711, U.S. Attorney's Office, Southern District of New York, February 18, 2022, 5, <https://www.justice.gov/opa/press-release/file/1488681/download>.
- 63 U.S. Attorney's Office, Southern District of New York, "Chinese National Charged With Acting As An Unregistered Agent Of The Chinese Government In The United States," March 30, 2022, <https://www.justice.gov/usao-sdny/pr/chinese-national-charged-acting-unregistered-agent-chinese-government-united-states>.
- 64 Rajagopalan and Rashbaum, "With F.B.I. Search, U.S. Escalates Global Fight Over Chinese Police Outposts."
- 65 "Patrol and Persuade," *Safeguard Defenders*, December 13, 2022, <https://safeguarddefenders.com/en/patrol-and-persuade>.
- 66 Compliant and Affidavit in Support of Arrest Warrants, United States v. Lu Jianwang and Chen Jinping, No. 23-MJ-265 (E.D.N.Y. 2023), <https://www.justice.gov/d9/2023-04/police-station--23-mj-265-amended-complaint-signed.pdf>.
- 67 Strider Technologies Inc., *The Los Alamos Club* (Salt Lake City, UT: Strider Technologies Inc, 2022), <https://www.striderintel.com/resources/the-los-alamos-club/>.
- 68 Cat Cadell and Ellen Nakashima, "American Technology Boosts China's Hypersonic Missile Program," *Washington Post*, October 19, 2022, <https://www.washingtonpost.com/national-security/2022/10/17/china-hypersonic-missiles-american-technology/>.
- 69 "User Clip: Gen. Alexander, 'Greatest Transfer,' AEI," C-SPAN, December 9, 2021, <https://www.c-span.org/video/?c4990859/user-clip-gen-alexander-greatest-transfer-aei>.
- 70 James Lewis, "How Much Have the Chinese Actually Taken?," *CSIS, Commentary*, March 22, 2018, <https://www.csis.org/analysis/how-much-have-chinese-actually-taken>.
- 71 Government Accountability Office, *Military Airlift: Cost and Complexity of the C-17 Aircraft Research and Development Program* (Washington, DC: Government Accountability Office March 1991), <https://www.gao.gov/assets/nsiad-91-5.pdf>; Congressional Research Service, *Air Force F-22 Fighter Program*, CRS Report No. RL31673 (Washington, DC: July 2013), https://www.everycrsreport.com/files/20130711_

[RL31673_c70b986e6de321f9f00ccb5173d56d3fc781d1a.pdf](#); and John R. Hoehn, *F-35 Joint Strike Fighter (JSF) Program*, CRS Report no. RL30563 (Washington, DC: Congressional Research Service, May 2022), <https://crsreports.congress.gov/product/pdf/RL/RL30563>.

- 72 “Chinese National Sentenced for Stealing Trade Secrets Worth \$1 Billion,” U.S. Department of Justice, February 27, 2020, <https://www.justice.gov/opa/pr/chinese-national-sentenced-stealing-trade-secrets-worth-1-billion>.
- 73 “Jury Convicts Chinese Intelligence Officer of Espionage Crimes, Attempting to Steal Trade Secrets,” U.S. Department of Justice, November 5, 2021, <https://www.justice.gov/opa/pr/jury-convicts-chinese-intelligence-officer-espionage-crimes-attempting-steal-trade-secrets>; and “GE90 Engine Surpasses 100 Million Hours,” GE Aerospace, July 4, 2020, <https://www.geaerospace.com/press-release/ge90-engine-family/ge90-engine-surpasses-100-million-hours>.
- 74 David E. Pozen, “The Mosaic Theory, National Security, and the Freedom of Information Act,” Columbia Law School, 2005, https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1527&context=faculty_scholarship.
- 75 Huo and Wang, *Sources and Techniques of Obtaining National Defense Science and Technology Intelligence*.
- 76 “OPM Announces Steps to Protect Federal Workers and Others from Cyber Threats,” Office of Personnel Management, July 9, 2015, <https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/>.
- 77 Stephen Engelberg, “Ex-C.I.A. Aid Convicted in Spy Case,” *New York Times*, February 8, 1986, <https://www.nytimes.com/1986/02/08/us/ex-cia-aid-convicted-in-spy-case.html>.
- 78 Indictment, United States v. Alexander Yuk Ching Ma, No. 1:20-cr-00083-DKW (D. Haw. 2020), <https://storage.courtlistener.com/recap/gov.uscourts.hid.151376/gov.uscourts.hid.151376.17.0.pdf>.
- 79 Indictment, United States v. Jerry Chun Shing Lee, No. 1:18-cr-00089 (E.D. VA. 2018), <https://storage.courtlistener.com/recap/gov.uscourts.vaed.383164/gov.uscourts.vaed.383164.27.0.1.pdf>.
- 80 Warren P. Strobel and Gordon Lubold, “Cuba to Host Secret Chinese Spy Base Focusing on U.S.,” *Wall Street Journal*, June 8, 2023, <https://www.wsj.com/articles/cuba-to-host-secret-chinese-spy-base-focusing-on-u-s-b2fed0e0>.

4. Cyber Operations

- 1 “China’s Military Strategy (2015),” State Council Information Office of the People’s Republic of China, May 15, 2015, http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm.
- 2 “中国的军事战略” [China’s Military Strategy], 中华人民共和国国务院新闻办公室 [State Council Information Office of the People’s Republic of China], May 15, 2015, https://www.gov.cn/zhengce/2015-05/26/content_2868988.htm.
- 3 Dina Temple-Raston, “China’s Microsoft Hack May Have Had a Bigger Purpose Than Just Spying,” NPR, August 26, 2021, <https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying>.
- 4 Ibid.
- 5 Andy Greenberg, “Chinese Hacking Spree Hit an ‘Astronomical’ Number of Victims,” *Wired*, March 5, 2021, <https://www.wired.com/story/china-microsoft-exchange-server-hack-victims/>.

- 6 Ibid.
- 7 Ibid.
- 8 See, for example, Benjamin Jensen, “The Cyber Character of Political Warfare,” *Brown Journal of World Affairs* Vol. 24, no. 1 (Fall/Winter 2017): 159–72, <https://www.jstor.org/stable/27119085>.
- 9 Eric Geller, “Chinese Nationals Charged for Anthem Hack, ‘One of the Worst Data Breaches in History,’” Politico, May 9, 2019, <https://www.politico.com/story/2019/05/09/chinese-hackers-anthem-data-breach-1421341>; and Sealed Indictment, United States v. Fujie Wang and John Doe, No. 1:19-cr-000153-JRS-MJD (S.D. Ind. 2019), <https://www.justice.gov/opa/press-release/file/1161466/download>.
- 10 Temple-Raston, “China’s Microsoft Hack May Have Had A Bigger Purpose Than Just Spying”; and Taylor Telford and Craig Timberg, “Marriott Discloses Massive Data Breach Affecting up to 500 Million Guests,” *Washington Post*, December 1, 2018, <https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-quests/>.
- 11 “Evolution of China’s Cyber Threat,” *Small Wars Journal*, September 23, 2021, <https://smallwarsjournal.com/jrnl/art/evolution-chinas-cyber-threat>; and “Chinese Definitions of Information Warfare,” Swiss Institute for Global Affairs, July 5, 2022, <https://www.globalaffairs.ch/2022/06/08/chinese-definitions-of-information-warfare/>.
- 12 “中国的军事战略” [China’s Military Strategy], 中华人民共和国国务院新闻办公室 [State Council Information Office of the People’s Republic of China], May 15, 2015, https://www.gov.cn/zhengce/2015-05/26/content_2868988.htm.
- 13 “China’s Military Strategy (2015),” State Council Information Office of the People’s Republic of China, May 15, 2015, http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm.
- 14 “Hackers Attack U.S. Government Web Sites in Protest of Chinese Embassy Bombing,” CNN, May 10, 1999, <http://www.cnn.com/TECH/computing/9905/10/hack.attack/>.
- 15 William Howlett IV, “The Rise of China’s Hacking Culture: Defining Chinese Hackers,” CSUSB ScholarWorks, Electronic Theses, Projects, and Dissertations, June 2016, <https://scholarworks.lib.csusb.edu/etd/383>.
- 16 “Red Line Drawn: China Recalculates Its Use of Cyber Espionage,” Mandiant, June 2016, <https://www.mandiant.com/resources/reports/red-line-drawn-china-recalculates-its-use-cyber-espionage/>.
- 17 Dorothy Denning, “How the Chinese Cyberthreat Has Evolved,” RealClearDefense, October 6, 2017, https://www.realcleardefense.com/articles/2017/10/06/how_the_chinese_cyberthreat_has_evolved_112442.html.
- 18 “APT1: Exposing One of China’s Cyber Espionage Units,” Mandiant, September 2021, <https://www.mandiant.com/resources/reports/apt1-exposing-one-chinas-cyber-espionage-units>.
- 19 “Central Network Security and Informatization Leading Group Established,” Xinhua News Agency, July 12, 2014, https://web.archive.org/web/20140712220934/http://news.xinhuanet.com/info/2014-02/28/c_133148759.htm.
- 20 Ibid.
- 21 Teresa Welsh, “Obama, Xi Reach Agreement to End Cyberattacks,” U.S. News, September 25, 2015, <https://www.usnews.com/news/articles/2015/09/25/president-obama-chinese-president-xi-jinping-announce-agreement-to-stop-hacking>.

- 22 Adam Segal, "The U.S.-China Cyber Espionage Deal One Year Later," Council on Foreign Relations, September 28, 2016, <https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later>.
- 23 "China's Military Strategy (2015)," State Council Information Office of the People's Republic of China; and "Evolution of China's Cyber Threat," *Small Wars Journal*.
- 24 "Evolution of China's Cyber Threat," *Small Wars Journal*.
- 25 John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era* (Washington, DC: NDU Press, 2018), https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.
- 26 Suyash Desai, "PLA SSF: Why China Will Be Ahead of Everyone in Future Cyber, Space or Information Warfare," *The Print*, December 31, 2019, <https://theprint.in/opinion/pla-ssf-why-china-will-be-ahead-of-everyone-in-future-cyber-space-or-information-warfare/342772/>.
- 27 Costello and McReynolds, *China's Strategic Support Force*.
- 28 Insikt Group, "Threat Activity Group RedFoxtrot Linked to China's PLA Unit 69010; Targets Bordering Asian Countries," Recorded Future, June 16, 2021, <https://www.recordedfuture.com/redfoxtrot-china-pla-targets-bordering-asian-countries>.
- 29 Nalani Fraser et al., "APT41: A Dual Espionage and Cyber Crime Operation," Mandiant, August 7, 2019, <https://www.mandiant.com/resources/blog/apt41-dual-espionage-and-cyber-crime-operation>.
- 30 Dorothy Denning, "Cyberwar: How Chinese Hackers Became a Major Threat to the U.S.," *Newsweek*, October 5, 2017, <https://www.newsweek.com/chinese-hackers-cyberwar-us-cybersecurity-threat-678378>.
- 31 Denning, "How the Chinese Cyberthreat Has Evolved."
- 32 Kannan and Bhalla, "Inside China's Cyber War Room."
- 33 "Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity," Cybersecurity and Infrastructure Security Agency, October 24, 2020, <https://www.cisa.gov/uscert/ncas/alerts/aa20-258a>; and "Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research," U.S. Department of Justice, July 21, 2020, <https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion>. In 2015, Presidents Xi and Obama agreed at a summit to stem cyber theft of IP, particularly for commercial advantage. However, Xi's reorganization of his cyber capabilities was already a fait accompli, and their focus was shifting, which made such a promise easier to make. Further, Chinese hacks in 2017 and 2018 directly contravened the agreement.
- 34 Jr Ng, "China Broadens Cyber Options," *Asian Military Review*, January 15, 2020, <https://www.asianmilitaryreview.com/2020/01/china-broadens-cyber-options/>.
- 35 "Evolution of China's Cyber Threat," *Small Wars Journal*.
- 36 U.S.-China Economic and Security Review Commission, *2022 Annual Report to Congress* (Washington, DC: November 2022), 419, https://www.uscc.gov/sites/default/files/2022-11/2022_Annual_Report_to_Congress.pdf.
- 37 "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," The White House, July 19, 2021, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/>.
- 38 Rogier Creemer, *China's Cyber Governance Institutions* (Leiden, Netherlands: Leiden Asia Centre, January 2021), <https://leidenasiacentre.nl/wp-content/uploads/2021/01/Chinas-Cyber-Governance-Institutions-Layout-geconverteerd-1.pdf>.
- 39 "Who Is Gothic Panda and How Can You Protect Yourself?," Team Password, September 7, 2021, <https://teampassword.com/blog/who-is-gothic-panda-and-how-can-you-protect-yourself>.
- 40 "APT3: A Nation-State Sponsored Adversary Responsible For Multiple High Profile Campaigns," Cyware Labs, May 28, 2019, <https://cyware.com/blog/apt3-a-nation-state-sponsored-adversary-responsible-for-multiple-high-profile-campaigns-f58c>.
- 41 Ionut Ilascu, "Historic APT10 Cyber Espionage Group Breached Systems in Over 12 Countries," Bleeping Computer, December 21, 2018, <https://www.bleepingcomputer.com/news/security/historic-apt10-cyber-espionage-group-breached-systems-in-over-12-countries/>.
- 42 Creemer, *China's Cyber Governance Institutions*.
- 43 "Measures for Cybersecurity Reviews," China Cybersecurity Review Technology and Certification Center, trans. Center for Security and Emerging Technology, January 25, 2021, https://cset.georgetown.edu/wp-content/uploads/t0258_cyber_review_EN.pdf.
- 44 Ng, "China Broadens Cyber Options."
- 45 "Cyberspace Administration of China (CAC) (国家互联网信息办公室)," Thomson Reuters Practical Law, accessed May 10, 2023, <https://uk.practicallaw.thomsonreuters.com/8-618-2325>.
- 46 Dakota Cary, *China's National Cybersecurity Center, A Base for Military-Civil Fusion in the Cyber Domain*, (Washington, DC: Center for Security and Emerging Technology, July 2021), <https://cset.georgetown.edu/publication/chinas-national-cybersecurity-center>.
- 47 Ng, "China Broadens Cyber Options."
- 48 Ibid.
- 49 Mara Hvistendahl, "China's Hacker Army," *Foreign Policy*, March 3, 2010, <https://foreignpolicy.com/2010/03/03/chinas-hacker-army/>.
- 50 Ng, "China Broadens Cyber Options."
- 51 "China's Military Strategy (2015)," The State Council Information Office of the People's Republic of China.
- 52 B.K. Williams, "Evaluating China's Road to Cyber Super Power," Lawrence Livermore National Laboratory, November 15, 2021, doi:10.2172/1830481; and U.S.-China Economic and Security Review Commission, *2022 Annual Report to Congress*.
- 53 Insikt Group, "Threat Activity Group RedFoxtrot Linked to China's PLA Unit 69010."
- 54 "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research," U.S. Department of Justice, July 19, 2021, <https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion>.
- 55 Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," Northrop Grumman, October 9, 2009, <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf>.

- 56 Ibid.
- 57 U.S.-China Economic and Security Review Commission, *2022 Annual Report to Congress*.
- 58 Creemer, *China's Cyber Governance Institutions*.
- 59 Michael Isikoff, "Chinese hacked Obama, McCain campaigns, took internal documents, officials say," NBC News, June 7, 2013, <https://www.nbcnews.com/id/wbna52133016>.
- 60 Ibid.
- 61 "SASC Investigation Finds Chinese Intrusions into Key Defense Contractors," U.S. Senate Committee on Armed Services, September 17, 2014, <https://www.armed-services.senate.gov/press-releases/sasc-investigation-finds-chinese-intrusions-into-key-defense-contractors>.
- 62 Mike Mount, "Hackers stole data on Pentagon's newest fighter jet," CNN, April 21, 2009, <https://www.cnn.com/2009/US/04/21/pentagon.hacked/>.
- 63 Ng, "China Broadens Cyber Options."
- 64 "Evolution of China's Cyber Threat," *Small Wars Journal*.
- 65 Fraser, "APT41."
- 66 Ellen Nakashima, "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say," *Washington Post*, December 1, 2021, <https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/>; and Jordan Valinsky, "Marriott reveals data breach of 500 million Starwood guests," CNN, November 30, 2018, <https://www.cnn.com/2018/11/30/tech/marriott-hotels-hacked/index.html>.
- 67 Ke Hongfa, Zhu Jilu, and Zhao Rong, "Promote the construction of core support capabilities in cyberspace," *Guofang Keji*, 2017, 50-4.
- 68 Ibid., 50-4.
- 69 Ibid., 50-4.
- 70 Ibid., 50-4.
- 71 Sergiu Gatlan, "US: Chinese govt hackers breached telcos to snoop on network traffic," *Bleeping Computer*, June 7, 2022, <https://www.bleepingcomputer.com/news/security/us-chinese-govt-hackers-breached-telcos-to-snoop-on-network-traffic/>.
- 72 "Evolution of China's Cyber Threat," *Small Wars Journal*.
- 73 Ravie Lakshmanan, "Chinese Hackers Target Middle East Telecoms in Latest Cyber Attacks," *The Hacker News*, December 6, 2022, <https://thehackernews.com/2022/12/chinese-hackers-target-middle-east.html>.
- 74 Ravie Lakshmanan, "New Cyber Espionage Group Targeting Ministries of Foreign Affairs," *The Hacker News*, June 11, 2021, <https://thehackernews.com/2021/06/new-cyber-espionage-group-targeting.html>; and David Hollingworth, "Chinese Hackers Update Turian Backdoor to Access Iranian Networks," *Cybersecurity Connect*, January 19, 2023, <https://www.cybersecurityconnect.com.au/technology/8620-chinese-hackers-update-turian-backdoor-to-access-iranian-network>.
- 75 "People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices," National Security Agency, Cybersecurity and Infrastructure Security Agency, and Federal Bureau of Investigation, June 2022, https://media.defense.gov/2022/Jun/07/2003013376/-1/-1/0/CSA_PRC_SPONSORED_CYBER_ACTORS_EXPLOIT_NETWORK_PROVIDERS_DEVICES_TLPWHITE.PDF.
- 76 Patrick Howell O'Neil, "Chinese Hackers Exploited Years-Old Software Flaws to Break into Telecom Giants," *MIT Technology Review*, June 8, 2022, <https://www.technologyreview.com/2022/06/08/1053375/chinese-hackers-exploited-years-old-software-flaws-to-break-into-telecom-giants/>.
- 77 Charles Riley, "Insurance giant Anthem Hit by massive data breach," CNN, February 6, 2015, <https://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/index.html>.
- 78 Kate O'Flaherty, "All the ways TikTok tracks you and how to stop it," *Wired*, October 23, 2021, <https://www.wired.co.uk/article/tiktok-data-privacy>.
- 79 Colin Demarest, "What TikTok withholds is as concerning as what it posts, Nakasone says," *C4ISRnet*, March 8, 2023, <https://www.c4isrnet.com/battlefield-tech/it-networks/2023/03/08/what-tiktok-withholds-is-as-concerning-as-what-it-posts-nakasone-says/>.
- 80 Denning, "How the Chinese Cyberthreat Has Evolved." Patriotic hackers were a relatively new phenomenon for China, emerging on the scene the year before in response to violence against ethnic Chinese in Indonesia, and they continued something resembling vigilante justice against perceived slights to China.
- 81 "Evolution of China's Cyber Threat," *Small Wars Journal*.
- 82 "The Most Famous Chinese Cyberattacks," *The Week*, April 30, 2021, <https://www.theweek.co.uk/news/world-news/china/952661/the-most-famous-cyber-attacks-conducted-by-china>.
- 83 Katie Robertson, "News Corp Says Journalists' Emails Were Hacked in an Attack Linked to China," *New York Times*, February 4, 2022, <https://www.nytimes.com/2022/02/04/business/media/news-corp-email-hack.html>.
- 84 "Log4j Vulnerability - What Everyone Needs to Know," National Cyber Security Centre, December 14, 2021, <https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know>; and Rufus Brown et al., "Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments," *Mandiant*, March 8, 2022, <https://www.mandiant.com/resources/blog/apt41-us-state-governments>.
- 85 Joseph Marks, "Chinese Hackers Breached Six State Governments, Researchers Say," *Washington Post*, March 8, 2022, <https://www.washingtonpost.com/politics/2022/03/08/chinese-hackers-breached-six-state-governments-researchers-say/>.
- 86 Scott Tong, "Theft of Farming Secrets Is Backdrop for U.S.-China Trade Deal," *Marketplace*, January 15, 2020, <https://www.marketplace.org/2020/01/15/theft-of-farming-secrets-is-backdrop-for-u-s-china-trade-deal/>; and Chris Bennett, "While America Slept, China Stole the Farm," *AgWeb*, June 8, 2021, <https://www.agweb.com/news/business/technology/while-america-slept-china-stole-farm>.
- 87 Josh Dawsey, Ellen Nakashima, and Tim Starks, "Chinese Hackers Are Scanning State Political Party Headquarters, FBI Says," *Washington Post*, October 17, 2022, <https://www.washingtonpost.com/politics/2022/10/17/chinese-hackers-are-scanning-state-political-party-headquarters-fbi-says/>.
- 88 Hongfa, Jilu, and Rong, "Promote the Construction of Core Support Capabilities in Cyberspace," 50-54.
- 89 "Chinese Gas Pipeline Intrusion Campaign," *Cybersecurity and Infrastructure Security Agency and the Federal Bureau of Investigation*, July 21, 2021, https://www.cisa.gov/sites/default/files/publications/AA21-201A_Chinese_Gas_Pipeline_Intrusion_Campaign_2011_to_2013%20%28%29.pdf.
- 90 Christian Vasquez and Blake Sobczak, "China Hacking Threat Prompts Rare U.S. Pipeline Warning," *E&E News*, July 21, 2021,

<https://www.eenews.net/articles/china-hacking-threat-prompts-rare-u-s-pipeline-warning/>.

- 91 Alan Suderman, "Critical Entities Targeted in Suspected Chinese Cyber Spying," AP News, June 15, 2021, <https://apnews.com/article/government-and-politics-hacking-technology-business-7350235e07d46ba5afc1238b553ea4b9>.
- 92 Vasquez and Sobczak, "China Hacking Threat Prompts Rare U.S. Pipeline Warning," E&E News, and Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (McLean, VA: ODNI, April 2021), <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021>.
- 93 Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (McLean, VA: ODNI, March 2022), <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/item/2279-2022-annual-threat-assessment-of-the-u-s-intelligence-community>.
- 94 Denning, "How the Chinese Cyberthreat Has Evolved."
- 95 Pierre Thomas and Olivia Katrandjian, "Chinese Hack Into US Chamber of Commerce, Authorities Say," ABC News, December 21, 2011, <https://abcnews.go.com/International/chinese-hack-us-chamber-commerce-authorities/story?id=15207642>.
- 96 "User Clip: Gen. Alexander, 'Greatest Transfer,' AEI," C-SPAN, December 9, 2021, <https://www.c-span.org/video/?c4990859/user-clip-gen-alexander-greatest-transfer-aei>.
- 97 Lewis, "How Much Have the Chinese Actually Taken?"
- 98 Fraser, "APT41."
- 99 Denning, "How the Chinese Cyberthreat Has Evolved."
- 100 Lily Hay Newman, "Indictment Alleges Who Hacked Anthem, but Not Why," *Wired*, May 10, 2019, <https://www.wired.com/story/anthem-hack-indictment-china/>.
- 101 Ibid. Note that Rosenstein did not say that all of the economic espionage took place as a result of cyber operations, but the thrust of his press conference was about Chinese cybercrime and an apparent reneging on the 2015 pledge to reduce cybercrime.
- 102 Fraser, "APT41."
- 103 Andy Greenberg, "A Pro-China Disinfo Campaign Is Targeting US Elections—Badly," *Wired*, October 26, 2022, <https://www.wired.com/story/us-midterm-election-disinformation-dragonbridge/>; and *U.S. vs Wong Ong Hua and Lian Yang Ching*, 1:20-cr-00166, U.S. District Court for the District of Columbia, August 18, 2020, <https://www.justice.gov/opa/press-release/file/1317211/download>.
- 104 "APT1," Mandiant.
- 105 Lu Chuanying, *A Chinese Perspective on Public Cyber Attribution* (Washington, DC: Carnegie Endowment for International Peace, March 2022), <https://carnegieendowment.org/2022/03/28/chinese-perspective-on-public-cyber-attribution-pub-86699>.
- 106 "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," U.S. Department of Justice, December 20, 2018, <https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion>.
- 107 "Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial

Aviation and Technological Data for Years," U.S. Department of Justice, October 30, 2018, <https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal>.

- 108 Adam Segal, "Three Thoughts on Cyber and the Defense Department's Report on the Chinese Military," Council on Foreign Relations, May 7, 2013, <https://www.cfr.org/blog/three-thoughts-cyber-and-defense-departments-report-chinese-military>.
- 109 Andrea Peterson, "Suspected Chinese state-linked threat actors infiltrated major Afghan telecom provider," *The Record*, September 27, 2021, <https://therecord.media/suspected-chinese-state-linked-threat-actors-infiltrated-major-afghan-telecom-provider/>.
- 110 Ma Qian, "Slandering China won't make cyberspace more secure," Xinhua News Agency, July 20, 2021, http://www.xinhuanet.com/english/2021-07/20/c_1310073113.htm.
- 111 "China Overtakes Russia as World's Biggest State Hacker," *The Week UK*, October 9, 2018, <https://www.theweek.co.uk/96999/china-overtakes-russia-as-world-s-biggest-state-hacker>.
- 112 Ibid.
- 113 "Assessing China's Digital Silk Road Initiative," Council on Foreign Relations, n.d., <https://www.cfr.org/china-digital-silk-road>.

5. Information and Disinformation Operations

- 1 Xi Jinping, "Hold High the Great Banner of Socialism with Chinese Characteristics and Strive in Unity to Build a Modern Socialist Country in All Respects: Report to the 20th National Congress of the Communist Party of China," CGTN, October 16, 2022, <https://news.cgtn.com/news/files/Full-text-of-the-report-to-the-20th-National-Congress-of-the-Communist-Party-of-China.pdf>.
- 2 习近平 [Xi Jinping], "高举中国特色社会主义伟大旗帜为全面建设社会主义现代化国家而团结奋斗——在中国共产党第二十次全国代表大会上的报告" [Hold High the Great Banner of Socialism with Chinese Characteristics and Strive in Unity to Build a Modern Socialist Country in All Respects: Report to the 20th National Congress of the Communist Party of China], 新华社 [Xinhua News Agency], October 25, 2022, https://www.gov.cn/xinwen/2022-10/25/content_5721685.htm.
- 3 Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020), 10–11.
- 4 "Full Text of the Report to the 20th National Congress of the Communist Party of China," Ministry of Foreign Affairs of the People's Republic of China, October 25, 2022, https://www.fmprc.gov.cn/eng/zxxx_662805/202210/t20221025_10791908.html.
- 5 David Bandurski, "Public Diplomacy," China Media Project, October 12, 2021, <https://chinamediaproject.org/the-ccp-dictionary/public-diplomacy/>.
- 6 Ibid.
- 7 "Address by H.E. Xi Jinping President of the People's Republic of China At the Conference of the 70th Anniversary of CCPIIT and Global Trade and Investment Promotion Summit," Ministry of Foreign Affairs of the People's Republic of China, May 18, 2022, https://www.fmprc.gov.cn/eng/zxxx_662805/202205/t20220518_10688542.html.
- 8 "Strengthening Cooperation Among Political Parties to Jointly Pursue the People's Wellbeing – Keynote Address by Xi Jinping at the CCP and World Political Parties Summit," CSIS, *Interpret*

China, July 6, 2021, <https://interpret.csis.org/translations/strengthening-cooperation-among-political-parties-to-jointly-pursue-the-peoples-wellbeing-keynote-address-by-xi-jinping-at-the-ccp-and-world-political-parties-summit/>.

- 9 In addition to the frequency of the term, it also appears in a diverse array of context. See, for example, H.E. Wang Yi, "Working as Cooperation Partners for True Multilateralism," Ministry of Foreign Affairs of the People's Republic of China, July 8, 2022, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zvjh_665391/202207/t20220710_10718093.html.
- 10 The research team conducted an English-language textual analysis of the official remarks posted to "Speeches," Ministry of Foreign Affairs of the People's Republic of China, accessed December 28, 2022, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zvjh_665391/.
- 11 "President Xi Jinping's Message to The Davos Agenda in Full," World Economic Forum, January 17, 2022, <https://www.weforum.org/agenda/2022/01/address-chinese-president-xi-jinping-2022-world-economic-forum-virtual-session/>; "Xi Jinping Attends the Opening Ceremony of the Eighth Ministerial Conference of the Forum on China-Africa Cooperation and Delivers a Keynote Speech," Ministry of Foreign Affairs of the People's Republic of China, November 29, 2021, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zjzq_663340/fzs_663828/dqzzywt_664274/202112/t20211207_10463463.html; "Jointly Upholding True Multilateralism and Starting a New Journey of Maritime Governance," Ministry of Foreign Affairs of the People's Republic of China, September 2, 2022, https://www.fmprc.gov.cn/eng/zxxx_662805/202209/t20220902_10760374.html; Global Times, Twitter post, October 27, 2022, 9:40 p.m., <https://twitter.com/globaltimesnews/status/1585491565383802880>; "Working as Cooperation Partners for True Multilateralism," Ministry of Foreign Affairs of the People's Republic of China, July 8, 2022, https://www.fmprc.gov.cn/eng/wjb_663304/wjbz_663308/2461_663310/202207/t20220710_10718093.html; and "Rising to Challenges Together for a Shared Future," Ministry of Foreign Affairs of the People's Republic of China, February 19, 2022, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/wjbz_663308/2461_663310/202202/t20220219_10643721.html.
- 12 "Address by H.E. Xi Jinping President of the People's Republic of China At the Conference of the 70th Anniversary of CCPIT and Global Trade and Investment Promotion Summit."
- 13 H.E. Wang Yi, "Upholding Equity and Justice to Promote Sound Development of the Global Human Rights Cause," (speech, Ministry of Foreign Affairs of the People's Republic of China, February 28, 2022), https://www.fmprc.gov.cn/mfa_eng/wjb_663304/wjbz_663308/2461_663310/202202/t20220228_10646322.html.
- 14 "Lijian Zhao 赵立坚," Twitter, accessed December 28, 2022, <https://twitter.com/zlj517>.
- 15 Lijian Zhao 赵立坚, Twitter post, July 13, 2022, 7:56 a.m., <https://twitter.com/zlj517/status/1547233519134420992>; Lijian Zhao 赵立坚, Twitter post, July 17, 2022, 11:57 p.m., <https://twitter.com/zlj517/status/1548562601755680768>; and Lijian Zhao 赵立坚, Twitter post, June 4, 2022, 5:21 a.m., <https://twitter.com/zlj517/status/1533061317258805248>.
- 16 "Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on April 29, 2022," Ministry of Foreign Affairs of the People's Republic of China, April 29, 2022, https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202204/t20220429_10680765.html.
- 17 In 2022, three of Zhao's tweets hit a certain threshold of more than 40,000 retweets and 10,000 likes. Two used images depicting damage caused in historic conflicts involving the U.S. military. The third was a redrawn world map showing an "international community" comprised only of the United States, Canada, Europe, Australia, New Zealand, and Japan. See Lijian Zhao 赵立坚, Twitter post, August 16, 2022, 6:19 a.m., <https://twitter.com/zlj517/status/1559530185686675457>; Lijian Zhao 赵立坚, Twitter post, September 26, 2022, 6:37 a.m., <https://twitter.com/zlj517/status/1574392669383426048>; and Lijian Zhao 赵立坚, Twitter post, March 17, 2022, 4:22 p.m., <https://twitter.com/zlj517/status/1504599052868255744>.
- 18 Timothy Nerozzi, "Chinese Embassy in France Releases Anti-American Song: US Is 'Human Rights Cop,'" Fox News, December 14, 2021, <https://www.foxnews.com/world/chinese-embassy-france-releases-anti-american-song>.
- 19 "Deer Show | American Democracy? Or Ameri-cracy?!", YouTube video, posted by New China TV, December 10, 2021, 3:18, <https://www.youtube.com/watch?v=kmmU688ifD8>.
- 20 Nerozzi, "Chinese Embassy in France Releases Anti-American Song."
- 21 David Shepardson, "Senators Seek Update on U.S. Security Review of TikTok," Reuters, June 24, 2022, sec. Technology, <https://www.reuters.com/technology/senators-seek-update-us-security-review-tiktok-2022-06-24/>; and Drew Harwell and Tony Romm, "TikTok's Beijing Roots Fuel Censorship Suspicion as It Builds a Huge U.S. Audience," *Washington Post*, September 17, 2019, <https://www.washingtonpost.com/technology/2019/09/15/tiktoks-beijing-roots-fuel-censorship-suspicion-it-builds-huge-us-audience/>.
- 22 Heather Wishart-Smith, "What You Should Know about the TikTok National Security Debate," *Forbes*, November 1, 2022, <https://www.forbes.com/sites/heatherwishartsmith/2022/11/01/what-you-should-know-about-the-tiktok-national-security-debate/>.
- 23 Alex Hern, "Revealed: How TikTok Censors Videos That Do Not Please Beijing," *The Guardian*, September 25, 2019, <https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing>.
- 24 Sarah Cook, "Beijing's Global Megaphone," Freedom House, 2020, <https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone>.
- 25 Harwell and Romm, "TikTok's Beijing Roots Fuel Censorship Suspicion as It Builds a Huge U.S. Audience."
- 26 Daniel Flatley and Emily Birnbaum, "TikTok Security Deal's Prospects Are Clouded by FBI's Doubts, State Bans," *Bloomberg*, December 13, 2022, <https://www.bloomberg.com/news/articles/2022-12-13/tiktok-security-deal-in-cfius-panel-is-clouded-by-fbi-s-doubts-state-bans>.
- 27 Zak Doffman, "Is TikTok Seriously Dangerous—Do You Need To Delete It?," *Forbes*, July 11, 2020, <https://www.forbes.com/sites/zakdoffman/2020/07/11/tiktok-seriously-dangerous-warning-delete-app-trump-ban/>.
- 28 Emily Baker-White, "TikTok Parent ByteDance Planned to Use TikTok To Monitor The Physical Location of Specific American Citizens," *Forbes*, October 20, 2022, <https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/>.
- 29 Wishart-Smith, "What You Should Know about the TikTok National Security Debate."
- 30 Cook, "Beijing's Global Megaphone."
- 31 Ibid.
- 32 Peter Mattis, "China's 'Three Warfares' in Perspective," War

- on the Rocks, January 30, 2018, <https://warontherocks.com/2018/01/chinas-three-warfares-perspective/>.
- 33 Seth D. Kaplan, "How China's Propaganda Influences the West," *Wall Street Journal*, August 21, 2022, <https://www.wsj.com/articles/how-chinas-propaganda-influences-the-west-state-media-cable-censorship-wechat-social-media-hong-kong-election-russia-ukraine-newspaper-11661108182>.
 - 34 Cook, "Beijing's Global Megaphone."
 - 35 Jonathan Kaiman, "'China Has Conquered Kenya': Inside Beijing's New Strategy to Win African Hearts and Minds," *Los Angeles Times*, August 7, 2017, <https://www.latimes.com/world/asia/la-fg-china-africa-kenya-20170807-htmlstory.html>.
 - 36 Ibid.
 - 37 "TNN Will Air Xinhua News Reports Locally," *Bangkok Post*, January 2, 2014, <https://www.bangkokpost.com/business/387572/tnn-will-air-xinhua-news-reports-locally>.
 - 38 "ZTE and Pakistan Sign Digital Terrestrial Television Agreement," ZTE, May 15, 2017, <https://www.zte.com.cn/global/about/news/0515ma>.
 - 39 Cook, "Beijing's Global Megaphone."
 - 40 Ibid.
 - 41 Ibid.
 - 42 Brian Flood, "Washington Post Publishes Special Advertising Section Pushing 'Propaganda' for Communist China," Fox News, August 29, 2019, <https://www.foxnews.com/media/washington-post-china-propaganda-advertising-section>.
 - 43 Amanda Meade, "Nine Entertainment Newspapers Quit Carrying China Watch Supplement," *The Guardian*, December 8, 2020, sec. Media, <https://www.theguardian.com/media/2020/dec/09/nine-entertainment-newspapers-quit-carrying-china-watch-supplement>.
 - 44 Cook, "Beijing's Global Megaphone."
 - 45 Emily Feng, "China and the World: How Beijing Spreads the Message," *Financial Times*, July 12, 2018, <https://www.ft.com/content/f5d00a86-3296-11e8-b5bf-23cb17fd1498>.
 - 46 Cook, "Beijing's Global Megaphone."
 - 47 Ibid.
 - 48 Ben Cohen, Georgia Wells, and Tom McGinty, "How One Tweet Turned Pro-China Trolls against the NBA," *Wall Street Journal*, October 16, 2019, <https://www.wsj.com/articles/how-one-tweet-turned-pro-china-trolls-against-the-nba-11571238943>.
 - 49 Cohen, Wells, and McGinty, "How One Tweet Turned Pro-China Trolls against the NBA."
 - 50 Ibid.
 - 51 James T. Areddy and Ben Cohen, "The Houston Rockets Were China's Team. Then a Hong Kong Tweet Happened," *Wall Street Journal*, October 11, 2019, <https://www.wsj.com/articles/the-houston-rockets-were-chinas-team-then-a-hong-kong-tweet-happened-11570802945>.
 - 52 "Daryl Morey Backtracks after Hong Kong Tweet Causes Chinese Backlash," BBC News, October 7, 2019, <https://www.bbc.com/news/business-49956385>.
 - 53 Cohen, "The Houston Rockets Were China's Team. Then a Hong Kong Tweet Happened."
 - 54 "Rockets GM Daryl Morey Creates China-NBA Tension with Tweet," *Los Angeles Times*, October 7, 2019, <https://www.latimes.com/sports/story/2019-10-06/rockets-morey-china-hong-kong-tweet>.
 - 55 Ben Rohrbach, "Enes Kanter and the Tangled Web of the NBA, Nike, Their Biggest Stars and China," Yahoo Sports, November 24, 2021, <https://sports.yahoo.com/enes-kanter-and-tangled-web-of-nba-nike-lebron-james-china-230916548.html>.
 - 56 "Daryl Morey Backtracks after Hong Kong Tweet Causes Chinese Backlash," BBC News.
 - 57 Rohrbach, "Enes Kanter and the Tangled Web of the NBA, Nike, Their Biggest Stars and China."
 - 58 "Daryl Morey Backtracks after Hong Kong Tweet Causes Chinese Backlash," BBC News.
 - 59 "China's CCTV Shows NBA Game, Ending 18-Month Blackout," Reuters, March 30, 2022, <https://www.reuters.com/lifestyle/sports/chinas-cctv-shows-nba-game-ending-18-month-blackout-2022-03-30/>.
 - 60 "Rockets GM Daryl Morey Creates China-NBA Tension with Tweet," *Los Angeles Times*.
 - 61 Mark Fainaru-Wada and Steve Fainaru, "Study: NBA Owners Have \$10 Billion in China," ESPN, May 19, 2022, https://www.espn.com/nba/story/_/id/33938932/nba-owners-mum-china-relationship-more-10-billion-invested-there. The sanctioned entity is China State Shipbuilding Corp (CSSC). ESPN reported that Heat owner Micky Arison, who also owns Carnival Corp., the world's largest cruise operator, launched a joint venture in 2018 with the CSSC to establish a China-based cruise line. The CSSC is a state-owned enterprise with close ties to the PLA and builds aircraft carriers for the PLAN.
 - 62 Fainaru-Wada and Fainaru, "Study: NBA Owners Have \$10 Billion in China."
 - 63 Rohrbach, "Enes Kanter and the Tangled Web of the NBA, Nike, Their Biggest Stars and China."
 - 64 Marc A. Thiessen, "Enes Freedom Was Cut for Exposing How U.S. Corporations Became Foreign Agents of Communist China," *Washington Post*, February 15, 2022, <https://www.washingtonpost.com/opinions/2022/02/15/enes-kanter-freedom-nba-china-rockets/>.
 - 65 Chen Weihua (陈卫华), Twitter post, February 10, 2022, 2:17 p.m., <https://twitter.com/chenweihua/status/1491899102723989512>.
 - 66 PEN America, *Made in Hollywood, Censored by Beijing: The U.S. Film Industry and Chinese Government Influence* (New York: PEN America, 2020), https://pen.org/wp-content/uploads/2020/09/Made_in_Hollywood_Censored_by_Beijing_Report_FINAL.pdf.
 - 67 Jane Hu, "When Hollywood Met China," *The New Yorker*, September 12, 2022, <https://www.newyorker.com/books/under-review/when-hollywood-met-china>.
 - 68 Terry Gross, "Hollywood Relies on China to Stay Afloat. What Does That Mean for Movies?," NPR, February 21, 2022, <https://www.npr.org/2022/02/21/1081435029/china-hollywood-movies-censorship-erich-schwartzel>.
 - 69 Ibid.
 - 70 Ibid.
 - 71 PEN America, *Made in Hollywood, Censored by Beijing*.
 - 72 Shirley Li, "How Hollywood Sold Out to China," *The Atlantic*, September 10, 2021, <https://www.theatlantic.com/culture/archive/2021/09/how-hollywood-sold-out-to-china/620021/>.
 - 73 Pamela McClintock, "U.S. Lost 2,000-Plus Movie Theater Screens Amid Pandemic," *Hollywood Reporter*, March 9, 2023, <https://www.hollywoodreporter.com/movies/movie-news/movie-theater-screen-losses-ticket-prices-1235346523/>; and

Lai Lin Thomala, "Number of Cinema Screens in China from 2009 to 2021," Statista, April 29, 2022, <https://www.statista.com/statistics/279111/number-of-cinema-screens-in-china/>.

- 74 Martha Bayles, "Hollywood's Great Leap Backward on Free Expression," *The Atlantic*, September 15, 2019, <https://www.theatlantic.com/ideas/archive/2019/09/hollywoods-great-leap-backward-free-expression/598045/>.
- 75 PEN America, *Made in Hollywood, Censored by Beijing*.
- 76 Ibid.
- 77 Li, "How Hollywood Sold Out to China."
- 78 Gross, "Hollywood Relies on China to Stay Afloat. What Does That Mean for Movies?"
- 79 Jin Yu Young, Amy Chang Chien, and Azi Paybarah, "'Shang-Chi' Wins a Warm Asia Greeting. Then There's China," *New York Times*, September 24, 2021, <https://www.nytimes.com/2021/09/17/business/shang-chi-china-marvel.html>.
- 80 PEN America, *Made in Hollywood, Censored by Beijing*.
- 81 Ibid.
- 82 Li, "How Hollywood Sold Out to China."
- 83 Bayles, "Hollywood's Great Leap Backward on Free Expression."
- 84 Ibid.
- 85 Lai Lin Thomala, "Box Office Revenue of the Most Successful Movies of All Time in China as of June 7, 2023," Statista, accessed February 2023, <https://www.statista.com/statistics/260007/box-office-revenue-of-the-most-successful-movies-of-all-time-in-china/>; and Patrick Brzeski, "China Box Office: 'Battle of Lake Changjin 2' Roars Past \$100M on First Day of Chinese New Year," *Hollywood Reporter*, February 1, 2022, <https://www.hollywoodreporter.com/movies/movie-news/battle-of-lake-changjin-2-box-office-1235084938/>.
- 86 Daniel Victor, "John Cena Apologizes to China for Calling Taiwan a Country," *New York Times*, May 25, 2021, <https://www.nytimes.com/2021/05/25/world/asia/john-cena-taiwan-apology.html>.
- 87 Li, "How Hollywood Sold Out to China."
- 88 Vincent Ni, "John Cena 'Very Sorry' for Saying Taiwan Is a Country," *The Guardian*, May 25, 2021, <https://www.theguardian.com/world/2021/may/26/john-cena-very-sorry-for-saying-taiwan-is-a-country>.
- 89 Ni, "John Cena 'Very Sorry' for Saying Taiwan Is a Country."
- 90 Li, "How Hollywood Sold Out to China."
- 91 Memorandum Opinion and Order, United States v. Gregory B. Craig, No. 1:19-cr-00125-ABJ (D.D.C. 2019), https://storage.courtlistener.com/recap/gov.uscourts.dcd.206162/gov.uscourts.dcd.206162.85.0_1.pdf.
- 92 Central Intelligence Agency, *Communism: The United Front in Communist China* (McClean, VA: Central Intelligence Agency, May 1957), <https://www.cia.gov/readingroom/docs/CIA-RDP78-00915R000600210003-9.pdf>.
- 93 The FARA and LDA databases often include text disparities across both foreign principals and clients and registrants, which requires significant manual data cleansing to standardize lists of both foreign clients and their agents. Only the FARA database assigns tracking numbers, but these are only assigned to foreign agents, not foreign principals. As such, in the LDA database, for example, a foreign client may be listed in five or more unique ways depending on the level of detail that is included when listing the entity. Extraneous commas, inconsistent use

of an entity's form of incorporation (e.g., LLC, PLC, and Inc.), abbreviations, and other non-standard text render it difficult to normalize and assess statistical figures. Further, in the FARA database, registrations for the Fujian Jinhua Integrated Circuit Company appear under five unique variations. As such, the numbers cited in this section may slightly differ from other analyses.

- 94 It is important to note that the LDA's reporting requirements are far less detailed than those required under FARA. For example, under FARA, foreign agents are obligated to submit copies of all materials they prepare on behalf of the foreign principal and copies of many of the communications activities on behalf of the foreign principal. LDA reporting requirements, on the other hand, only require short, general descriptions of the lobbying issue areas that were undertaken on the foreign client's behalf, such as "Lobbying related to clients (sic) role in the computer industry and US manufacturing presence" or "Telecommunications and trade issues."
- 95 Kiran Stacey, "Huawei turns to US group in public relations battle," *Financial Times*, March 25, 2019, <https://www.ft.com/content/7f32addc-4f34-11e9-b401-8d9ef1626294>.
- 96 "Exhibit A to Registration Statement," U.S. Department of Justice, December 10, 2021, <https://efile.fara.gov/docs/7057-Exhibit-AB-20211210-1.pdf>.
- 97 Lachlan Markay, "How China Used Influencers to Promote the Beijing Olympics," *Axios*, April 8, 2022, <https://www.axios.com/2022/04/08/inside-chinas-olympic-influencer-campaign>.
- 98 Lingling Wei, "China Ratchets Up Pressure on Foreign Companies," *Wall Street Journal*, April 28, 2023, <https://www.wsj.com/articles/china-ratchets-up-pressure-on-foreign-companies-524b958e>.
- 99 Mike Gallagher, "The Select Committee on the Chinese Communist Party: Rep. Gallagher statement on CCP Raid of Bain, Mintz, and Expansion of Counter-Espionage Law," *WIS Politics*, April 27, 2023, <https://www.wispolitics.com/2023/the-select-committee-on-the-chinese-communist-party-rep-gallagher-statement-on-ccp-raid-of-bain-mintz-and-expansion-of-counter-espionage-law>.
- 100 Laura Silver, Christine Huang, and Laura Clancy, "How Global Public Opinion of China Has Shifted in the Xi Era," *Pew Research Center*, September 28, 2022, <https://www.pewresearch.org/global/2022/09/28/how-global-public-opinion-of-china-has-shifted-in-the-xi-era/>.
- 101 Silver, Huang, and Clancy, "How Global Public Opinion of China Has Shifted in the Xi Era."

6. The United Front

- 1 Alex Joske, *The Party Speaks for You* (Canberra, Australia: Australian Strategic Policy Institute, 2020), 6, <https://www.aspi.org.au/report/party-speaks-you>.
- 2 习近平 [Xi Jinping], "习近平在欧美同学会成立100周年庆祝大会上的讲话" [Speech by Xi Jinping at the Celebration Ceremony of the 100th Anniversary of the European and American Scholars Association], 人民网 [People's Daily Online], October 13, 2013, https://cpc-people-com-cn.translate.goog/n/2013/1022/c64094-23281641.html?_x_tr_sch=http&_x_tr_sl=zh-CN&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc.
- 3 Larry Diamond, "Democracy's Arc: From Resurgent to Imperiled," *Journal of Democracy* 33, no. 1 (January 2022): 172, <https://www.journalofdemocracy.org/articles/democracys-arc-from-resurgent-to-imperiled/>.
- 4 "习近平同党外人士座谈并共迎新春时强" [Xi Jinping Holds Discussions with Non-Party Personages and Welcomes the

- Spring Festival Together], 人民日报 [People's Daily], January 17, 2023, http://paper.people.com.cn/rmrb/html/2023-01/17/nw.D110000renmrb.20230117_1-01.htm?utm_source=stack&utm_medium=email.
- 5 毛泽东 (Mao Zedong), “共产党人发刊词” [‘Communist’ opening words], Chinese Marxism Library, October 4, 1939, <https://www.marxists.org/chinese/maozedong/marxist.org-chinese-mao-19391004.htm>.
 - 6 Central Intelligence Agency, *Communism: The United Front in Communist China* (McClean, VA: CIA, May 1957), <https://www.cia.gov/readingroom/document/cia-rdp78-00915r000600210003-9>.
 - 7 习近平 [Xi Jinping], “习近平: ‘大侨务’观念的确立” [Xi Jinping: The Establishment of the Concept of ‘Great Overseas Chinese Affairs’], 爱思想 [Aisixiang], May 30, 2017, <http://www.aisixiang.com/data/93625.html>.
 - 8 “专设统战工作领导小组 中央‘大统战’思维升级” [Set up a leading group for United Front work to upgrade the thinking of the Central Committee’s ‘Great United Front’], 中国共产党新闻网—人民网 [Communist Party of China CPC—People’s Daily Online], July 31, 2015, <https://cpc.people.com.cn/xuexi/n/2015/0731/c385474-27391395.html>. Alex Joske has put forth a helpful set of terminology to differentiate the various components of united front work, which includes both the formal United Front Work Department (UFWD)—the CCP Central Committee department that coordinates united front work—and the “united front system,” which is the broad range of agencies, organizations, and individuals carrying out united front work. See Alex Joske, *The Party Speaks for You* (Canberra, Australia: Australian Strategic Policy Institute, 2020), 6, <https://www.aspi.org.au/report/party-speaks-you>.
 - 9 “专设统战工作领导小组 中央‘大统战’思维升级” [Set up a leading group for United Front work to upgrade the thinking of the Central Committee’s ‘Great United Front’].
 - 10 “习近平: 巩固发展最广泛的爱国统一战线” [Xi Jinping: Consolidate and Develop the Broadest Patriotic United Front] 新华社 [Xinhua News Agency], May 5, 2015, <http://www.xinhuanet.com/politics/2015-05/20/c.1115351358.htm>.
 - 11 “中共中央印发‘中国共产党统一战线工作条例’” [The Central Committee of the Communist Party of China issued the ‘Regulations on the Work of the United Front of the Communist Party of China’], 新华社 [Xinhua News Agency], January 1, 2021, http://www.gov.cn/zhengce/2021-01/05/content_5577289.htm.
 - 12 Alex Joske, “Reorganizing the United Front Work Department: New Structures for a New Era of Diaspora and Religious Affairs Work,” Jamestown Foundation, May 9, 2019, <https://jamestown.org/program/reorganizing-the-united-front-work-department-new-structures-for-a-new-era-of-diaspora-and-religious-affairs-work/>.
 - 13 薛钰 [Xue Yu], “周恩来与党的隐蔽战线—试谈民主革命时期周恩来对我党情报保卫工作的贡献” [Zhou Enlai and the Party’s Hidden Front—Talking about Zhou Enlai’s Contribution to Our Party’s Intelligence Protection Work during the Democratic Revolution], 人民日报 [People’s Daily], March 9, 2018, <https://web.archive.org/web/20180309073811/http://www.people.com.cn/GB/shizheng/8198/9405/34150/2544000.html>.
 - 14 刘仰 [Liu Yang], “怕孔子学院?美国的自信去哪了” [Afraid of Confucius Institute? Where is American Self-Confidence], 人民日报 [People’s Daily], June 20, 2014, <http://world.people.com.cn/n/2014/0620/c1002-25178548.html>.
 - 15 “Petition to the Committee of the Council,” Inside Higher Ed, 2014, [https://www.insidehighered.com/sites/default/files/files/Chicago%20Petition%20re%20Confucius%20Institute%20\(2\).docx](https://www.insidehighered.com/sites/default/files/files/Chicago%20Petition%20re%20Confucius%20Institute%20(2).docx).
 - 16 Marshall Sahlins, “China U.,” *The Nation*, October 20, 2013, <https://www.thenation.com/article/archive/china-u/>; and Elizabeth Redden, “Censorship at China Studies Meeting,” Inside Higher Ed, August 6, 2014, <https://www.insidehighered.com/news/2014/08/06/accounts-confucius-institute-ordered-censorship-chinese-studies-conference>.
 - 17 “Petition to the Committee of the Council,” Inside Higher Ed.
 - 18 Sahlins, “China U.”
 - 19 Author interview with Mark Kelton, June 2, 2020.
 - 20 James M. Olson, *To Catch a Spy: The Art of Counterintelligence* (Washington, DC: Georgetown University Press, 2019), 7.
 - 21 “Confucius Teaches Cultures,” *China Daily*, June 25, 2014, https://www.chinadaily.com.cn/opinion/2014-06/25/content_17613251.htm; and Elizabeth Redden, “Debate Renews over Confucius Institutes,” Inside Higher Ed, July 24, 2014, <https://www.insidehighered.com/news/2014/07/24/debate-renews-over-confucius-institutes>.
 - 22 “How Many Confucius Institutes Are in the United States?,” National Association of Scholars, March 22, 2023, https://www.nas.org/blogs/article/how_many_confucius_institutes_are_in_the_united_states.
 - 23 Reed Rubinstein, “Letter to Sen. Rob Portman,” U.S. Department of Education, January 5, 2021, <https://www2.ed.gov/policy/highered/leg/portman-jan8-2021.pdf>.
 - 24 “China’s Impact on the U.S. Education System,” Hearing Before the U.S. Senate Permanent Subcommittee on Investigations of the Committee on Homeland Security and Governmental Affairs, February 28, 2019, <https://www.govinfo.gov/content/pkg/CHRG-116shrg36158/html/CHRG-116shrg36158.htm>.
 - 25 Stony Brook University observed a drop from 2,494 non-resident alien students from China enrolled in Fall 2017 to 1,550 in Fall 2022. At an estimated tuition of \$25,000 per student, this is a more than \$23.6 million loss in revenue for the university. In the same period, the University of Nebraska at Lincoln observed a nearly 75 percent reduction in Chinese student enrollments, from 1,203 to 303, representing a loss of approximately \$22.5 million in annual revenue.
 - 26 Joyce Lau, “Dalai Lama to Speak at University of Sydney,” *New York Times*, April 29, 2013, <https://www.nytimes.com/2013/04/29/world/asia/29iht-educbriefs29.html>.
 - 27 Quoted in Joske, *The Party Speaks for You*.
 - 28 “National Security Risks Affecting the Australian Higher Education and Research Sector,” Australian Parliamentary Joint Committee on Intelligence and Security, March 19, 2021, Australia, https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/commint/3ca6fe4f-b221-48f6-812e-ccfd3cd59d55/&sid=0000; and Sebastian Rotella, “Even on U.S. Campuses, China Cracks Down on Students Who Speak Out,” ProPublica, November 30, 2021, <https://www.propublica.org/article/even-on-us-campuses-china-cracks-down-on-students-who-speak-out>.
 - 29 Emma Whitford, “Political Art Roils George Washington Campus,” Inside Higher Ed, February 7, 2022, <https://www.insidehighered.com/news/2022/02/08/gwu-president-criticized-response-political-art>.
 - 30 Josh Rogin, “Another University Learns the Hard Way about Chinese Censorship on Campus,” *Washington Post*, February 9, 2022, <https://www.washingtonpost.com/opinions/2022/02/09/another-university-learns-hard-way-about-chinese-censorship-campus/>.

- 31 Paul Charon and Jean-Baptiste Jeangène Vilmer, *Les Opérations d'influence Chinoises* [Chinese Influence Operations] (Paris: Institute for Strategic Research, October 2021), 281, <https://www.irsem.fr/rapport.html>.
- 32 Charon and Vilmer, *Chinese Influence Operations*; and Josh Horwitz, "Chinese Students in the US Are Using 'Inclusion' and 'Diversity' to Oppose a Dalai Lama Graduation Speech," Quartz, February 15, 2017, <https://qz.com/908922/chinese-students-at-ucsd-are-evoking-diversity-to-justify-their-opposition-to-the-dalai-lamas-graduation-speech/>.
- 33 "Who We Are," China-United States Exchange Foundation, n.d., <https://www.cusef.org.hk/en/who-we-are/about-us>.
- 34 "Supplemental Statement," U.S. Department of Justice, March 31, 2022, <https://efile.fara.gov/docs/6584-Supplemental-Statement-20220331-7.pdf>.
- 35 Alexander Bowe, "China's Overseas United Front Work," U.S.-China Economic and Security Review Commission, August 24, 2018, https://www.uscc.gov/sites/default/files/Research/China%27s%20Overseas%20United%20Front%20Work%20-%20Background%20and%20Implications%20for%20US_final_0.pdf; and Bethany Allen-Ebrahimian, "This Beijing-Linked Billionaire Is Funding Policy Research at Washington's Most Influential Institutions," *Foreign Policy*, November 28, 2017, <https://foreignpolicy.com/2017/11/28/this-beijing-linked-billionaire-is-funding-policy-research-at-washingtons-most-influential-institutions-china-dc/>.
- 36 "Exhibit B to Registration Statement," U.S. Department of Justice, January 15, 2019, <https://efile.fara.gov/docs/6328-Exhibit-AB-20190115-8.pdf>.
- 37 "About CPIFA," Chinese People's Institute of Foreign Affairs, n.d., <http://www.cpifa.org/en/class/view?id=7>.
- 38 "Protecting Government and Business Leaders at the U.S. State and Local Level from People's Republic of China (PRC) Influence Operations," National Counterintelligence and Security Center, July 2022, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/PRC_Subnational_Influence-06-July-2022.pdf.
- 39 Quentin McDermott, "Sam Dastyari Defended China's Policy in South China Sea in Defiance of Labor Policy, Secret Recording Reveals," ABC News, November 29, 2017, <https://www.abc.net.au/news/2017-11-29/sam-dastyari-secret-south-china-sea-recordings/9198044>.
- 40 Ibid.
- 41 Ibid; and 习近平 [Xi Jinping], "习近平同志在中共中央政治局第八次集体学习时的讲话" [Comrade Xi Jinping's Remarks to the Eighth Collective Study Session of the CCP Politburo], 太平洋学报 [Pacific Journal], trans. Interpret: China, original work published July 30, 2013, <https://interpret.csis.org/translations/comrade-xi-jinpings-remarks-to-the-eighth-collective-study-session-of-the-ccp-politburo/>.
- 42 Peter Hartcher, "Sam Dastyari: Riding the Red Dragon Express Not a Good Look," Sydney Morning Herald, September 3, 2016, <https://www.smh.com.au/opinion/sam-dastyari-riding-the-red-dragon-express-not-a-good-look-20160902-gr7tcv.html>; and James Massola, "Chinese Donor the Yuhu Group Steps in to Help Sam Dastyari," *Sydney Morning Herald*, March 27, 2015, <https://www.smh.com.au/politics/federal/chinese-donor-the-yuhu-group-steps-in-to-help-sam-dastyari-20150327-lm9be2.html>.
- 43 Nick McKenzie, James Massola, and Richard Baker, "Labor Senator Sam Dastyari Warned Wealthy Chinese Donor Huang Xiangmo His Phone Was Bugged," *Sydney Morning Herald*, November 29, 2017, <https://www.smh.com.au/politics/federal/labor-senator-sam-dastyari-warned-wealthy-chinese-donor-huang-xiangmo-his-phone-was-bugged-20171128-qzu14c.html>.
- 44 Yan Zhuang, "A Test Case for Australia's Broad New Law against Foreign Meddling," *New York Times*, July 28, 2022, <https://www.nytimes.com/2022/07/28/world/australia/di-san-h-duong-chinese-australia.html>.
- 45 Ken McCallum and Christopher Wray, "Joint Address by MI5 and FBI Heads," MI5, July 6, 2022, <https://www.mi5.gov.uk/news/speech-by-mi5-and-fbi>.
- 46 Gerry Shih, "Solomon Islands Recognizes Beijing as Diplomatic Stranglehold Tightens around Taiwan," *Washington Post*, September 16, 2019, https://www.washingtonpost.com/world/asia-pacific/solomon-islands-recognizes-beijing-as-diplomatic-stranglehold-tightens-around-taiwan/2019/09/16/615520bc-d867-11e9-ala5-162b8a9c9ca2_story.html; and "PM Sogavare Addresses UN General Assembly," *Solomon Star*, September 25, 2017, <https://www.solomonstarnews.com/un-urged-to-give-taiwan-a-chance/>.
- 47 "Solomons' Premier Promised Big Bribe to Back China Switch," RNZ, September 24, 2019, <https://www.rnz.co.nz/international/pacific-news/399501/solomons-premier-promised-big-bribe-to-back-china-switch>.
- 48 Michael Miller, "China's Growing Reach Is Transforming a Pacific Island Chain," *Washington Post*, August 11, 2022, <https://www.washingtonpost.com/world/2022/08/11/solomon-islands-china-australia-pacific/>; and Edward Cavanaugh, "When China Came Calling: Inside the Solomon Islands Switch," *The Guardian*, December 7, 2019, <https://www.theguardian.com/world/2019/dec/08/when-china-came-calling-inside-the-solomon-islands-switch/>.
- 49 "Distribution of Chinese Funds by Solomon Islands PM Raises Questions," Voice of America, August 25, 2022, <https://www.voanews.com/a/distribution-of-chinese-funds-by-solomon-islands-pm-raises-questions-/6715974.html>.
- 50 Angus Grigg, Stephanie March, and Amy Donaldson, "Australia urged to intervene as China tries to buy a strategic Solomon Islands port," ABC News, July 31, 2022, <https://www.abc.net.au/news/2022-08-01/china-trying-to-buy-solomon-islands-port-australia-urged-to-stop/101277348>.
- 51 "Solomon Islands PM Survives No-Confidence Vote after Unrest," BBC News, December 6, 2021, <https://www.bbc.com/news/world-asia-59501054>.
- 52 Michael E. Miller and Frances Vinall, "China Signs Security Deal with Solomon Islands, Alarming Neighbors," *Washington Post*, April 20, 2022, <https://www.washingtonpost.com/world/2022/04/20/solomon-islands-china-security-agreement/>.
- 53 "National Security Risks Affecting the Australian Higher Education and Research Sector," Australian Parliamentary Joint Committee on Intelligence and Security, March 19, 2021, https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/commint/3ca6fe4f-b221-48f6-812e-ccfd3cd59d55/&sid=0000.
- 54 To understand the rough scale, the Council for the Promotion of the Peaceful Reunification of China (CPPRC) has hundreds of global chapters alone, including at least 36 in the United States as of 2019. For more see, John Dotson, "The United Front Work Department Goes Global: The Worldwide Expansion of the Council for the Promotion of the Peaceful Reunification of China," Jamestown Foundation, May 9, 2019, <https://jamestown.org/program/the-united-front-work-department-goes-global-the-worldwide-expansion-of-the-council-for-the-promotion-of-the-peaceful-reunification-of-china/>.

- 55 Filip Jirouš, "The Role of Coopted Diaspora Groups in Czech and European United Front Work," Jamestown Foundation, September 16, 2020, <https://jamestown.org/program/the-role-of-coopted-diaspora-groups-in-czech-and-european-united-front-work/>; and Livia Codarin, Laura Harth, and Jichang Lulu, "Hijacking the mainstream: CCP influence agencies and their operations in Italian parliamentary and local politics," *Sinopsis*, November 20, 2021, <https://sinopsis.cz/en/it/>.

7. Irregular Military Actions

- 1 贾宇 张小奕 [Jia Yu and Zhang Xiaoyi], "毛泽东、邓小平和习近平的海洋战略思想初探" [The Maritime Strategy of Mao Zedong, Deng Xiaoping and Xi Jinping], *边界与海洋研究* [Journal of Boundary and Ocean Studies], trans. Interpret: China, original work published May 1, 2018, <https://interpret.csis.org/translations/the-maritime-strategy-of-mao-zedong-deng-xiaoping-and-xi-jinping/>.
- 2 Ibid.
- 3 "Tian Kun Hao," Dredging Database, accessed October 20, 2022, <https://www.dredgepoint.org/dredging-database/equipment/tian-kun-hao>.
- 4 Ibid.; "What Is China's 'Magic Island-Making' Ship?," BBC News, November 6, 2017, <https://www.bbc.com/news/world-asia-china-41882081>; and W.J. Vlasblom, "Chapter 3: Cutter Suction Dredger," lecture notes, Delft University of Technology, 2005, <https://dredging.org/media/ceda/org/documents/resources/othersonline/vlasblom3-the-cutter-suction-dredger.pdf>.
- 5 See, for example, 习近平 [Xi Jinping], "习近平同志在中共中央政治局第八次集体学习时的讲话" [Comrade Xi Jinping's Remarks to the Eighth Collective Study Session of the CCP Politburo], *太平洋学报* [Pacific Journal], trans. Interpret: China, original work published July 30, 2013, <https://interpret.csis.org/translations/comrade-xi-jinpings-remarks-to-the-eighth-collective-study-session-of-the-ccp-politburo/>; and 贾宇 张小奕 [Jia Yu and Zhang Xiaoyi], "毛泽东、邓小平和习近平的海洋战略思想初探" [The Maritime Strategy of Mao Zedong, Deng Xiaoping and Xi Jinping] *边界与海洋研究* [Journal of Boundary and Ocean Studies], trans. Interpret: China, original work published May 1, 2018, <https://interpret.csis.org/translations/the-maritime-strategy-of-mao-zedong-deng-xiaoping-and-xi-jinping/>.
- 6 Andrew S. Erickson and Lyle J. Goldstein, "Studying History to Guide China's Rise as a Maritime Great Power," *Harvard Asia Quarterly* 12, no. 3-4 (Winter 2010): 31-38, https://www.andrewerickson.com/wp-content/uploads/2013/05/Erickson-Publication_Erickson-Goldstein-Studying-History-to-Guide-Chinas-Rise-as-a-Maritime-Great-Power_HAQ_2010-Winter.pdf.
- 7 习近平 [Xi Jinping], "习近平同志在中共中央政治局第八次集体学习时的讲话" [Comrade Xi Jinping's Remarks to the Eighth Collective Study Session of the CCP Politburo].
- 8 Jennifer Rice and Erik Robb, "China Maritime Report No. 13: The Origins of 'Near Seas Defense and Far Seas Protection,'" *CMSI China Maritime Reports*, February 1, 2021, <https://digital-commons.usnwc.edu/cmsi-maritime-reports/13>.
- 9 Shou Xiasong, ed., *In Their Own Words: Foreign Military Thought Science of Military Strategy (2013)* (Montgomery, AL: China Aerospace Studies Institute, 2021), <https://www.airuniversity.af.edu/CASI/In-Their-Own-Words/Article-Display/Article/2485204/plas-science-of-military-strategy-2013/>.
- 10 "China's Military Strategy (2015)," The State Council Information Office of the People's Republic of China,

May 15, 2015, http://english.www.gov.cn/archive/white-paper/2015/05/27/content_281475115610833.htm.

- 11 See, for example, Ryan D. Martinson, "Panning for Gold: Assessing Chinese Maritime Strategy from Primary Sources," *Naval War College Review* 69, no. 3 (2016): 22-44, <https://digital-commons.usnwc.edu/cqi/viewcontent/cqi?article=1160&context=nwc-review>; Linda Jakobson, *China's Unpredictable Maritime Security Actors* (Sydney: Lowy Institute for International Policy, December 11, 2014), https://www.lowyinstitute.org/sites/default/files/chinas-unpredictable-maritime-security-actors_3.pdf; and Shinji Yamaguchi, "Strategies of China's Maritime Actors in the South China Sea," *China Perspectives* 3 (September 2016): 23-31, doi:10.4000/chinaperspectives.7022.
- 12 Meia Nouwens and Lucie Béraud-Sudreau, "Xi Looks to China's Private Sector as He Pursues a Slimmer, Smarter PLA," *War on the Rocks*, February 23, 2018, <https://warontherocks.com/2018/02/xi-looks-chinas-private-sector-pursues-slimmer-smarter-pla/>.
- 13 Ibid.; 习近平 [Xi Jinping], "习近平同志代表十八届中央委员会向大会作的报告" [Xi Jinping's Speech to the 19th National Congress of the Communist Party of China] 新华社 [Xinhua News Agency], trans. Xinhua, October 18, 2017, http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf.
- 14 习近平 [Xi Jinping], "习近平同志代表第十九届中央委员会向大会作的报告" [Xi Jinping's Speech to the 20th National Congress of the Communist Party of China], *Bloomberg*, trans. Low De Wei and Bloomberg News, original published October 17, 2022, trans. October 18, 2022, <https://www.bloomberg.com/news/articles/2022-10-18/full-text-of-xi-jinping-s-speech-at-china-20th-party-congress-2022>.
- 15 倪桂桦 朱锋 [Ni Guihua and Zhu Feng], "拜登政府对华战略竞争的态势与困境" [The Situation and Dilemmas of the Biden Administration's Strategic Competition with China], *亚太安全与海洋研究* [Asia-Pacific Security and Maritime Affairs], trans. Interpret: China, original work published January 26, 2022, <https://interpret.csis.org/translations/the-state-and-dilemmas-of-the-biden-administrations-strategic-competition-with-china/>.
- 16 习近平 [Xi Jinping], "习近平同志在中共中央政治局第八次集体学习时的讲话" [Comrade Xi Jinping's Remarks to the Eighth Collective Study Session of the CCP Politburo].
- 17 Vlasblom, "Chapter 3: Cutter Suction Dredger."
- 18 "Tian Jing Hao," Dredging Database; and "What Is China's 'Magic Island-Making' Ship?," BBC News.
- 19 Bethany Allen-Ebrahimian, "Beijing Calls South China Sea Island Reclamation a 'Green Project,'" *Foreign Policy*, May 26, 2016, <https://foreignpolicy.com/2016/05/26/china-calls-south-china-sea-island-reclamation-a-green-project-sprately-islands/>.
- 20 "南沙岛礁扩建工程不会对海洋生态环境造成破坏" [The Nansha Islands and Reefs Expansion Project Will Not Cause Damage to the Marine Ecological Environment], 国家海洋局 [State Oceanic Administration of the People's Republic of China], June 18, 2015, archived September 11, 2018, https://web.archive.org/web/20180911033858/www.soa.gov.cn/xw/hyww_90/201506/t20150618_38598.html.
- 21 "Foreign Ministry Spokesperson Hong Lei's Regular Press Conference on May 6, 2016," Ministry of Foreign Affairs of the People's Republic of China, May 6, 2016, archived December 2, 2020, https://web.archive.org/web/20201202123453/https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1361284.shtml.

- 22 Matthew Southerland, *China's Island Building in the South China Sea: Damage to the Marine Environment, Implications, and International Law* (Washington, DC: U.S.-China Economic and Security Review Commission, April 12, 2016), https://permanent.fdlp.gov/gpo174412/China's%20Island%20Building%20in%20the%20South%20China%20Sea_0.pdf.
- 23 "China Tracker," CSIS, *Asia Maritime Transparency Initiative*, accessed October 20, 2022, <https://amti.csis.org/island-tracker/china/>.
- 24 Mischief Reef is located within the EEZ of the Philippines, is controlled by China, and is also claimed by Taiwan and Vietnam. Mischief Reef is also referred to as Meiji Jiao [美濟礁] by China, Panganiban Reef by the Philippines, Meiji Reef [美濟礁] by Taiwan, and Đà Nẵng Khãn by Vietnam. See "Mischief Reef," Asia Maritime Transparency Initiative, CSIS, accessed October 25, 2022, <https://amti.csis.org/mischief-reef/>; and David E. Sanger and Rick Gladstone, "Piling Sand in a Disputed Sea, China Literally Gains Ground," *New York Times*, April 8, 2015, <https://www.nytimes.com/2015/04/09/world/asia/new-images-show-china-literally-gaining-ground-in-south-china-sea.html>.
- 25 Sanger and Gladstone, "Piling Sand in a Disputed Sea, China Literally Gains Ground"; and Seth G. Jones, *Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare* (New York: W.W. Norton, 2021), 156–59.
- 26 陳志偉 [Chen Zhiwei], "[金門海域大陸船舶新興違法態樣與危機研析]" [Research and Analysis on the Emerging Illegal Patterns and Crisis of Mainland Ships in the Kinmen Sea], *Golden Horse*, Kinmen Branch, Fuchien High Prosecutor's Office, Ministry of Justice of the Republic of China (Taiwan), July 8, 2022, <https://www.kmh.moj.gov.tw/media/80132/311814463156.pdf>; and Yimou Lee, "China's Latest Weapon against Taiwan: The Sand Dredger," Reuters, February 5, 2021, <https://graphics.reuters.com/TAIWAN-CHINA/SECURITY/ibvvrnzerve/>.
- 27 "取締違法大陸抽砂船成" [Effectiveness of Banning Illegal Mainland Sand Pumping Ships], 海洋委員會海巡署 [Coast Guard Administration of the Republic of China (Taiwan)], October 13, 2022, <https://www.cga.gov.tw/GipOpen/wSite/ct?xItem=139485&ctNode=11298&mp=marine>; Matthew Strong, "Taiwan Coast Guard Chases Illegal Chinese Dredgers Away," *Taiwan News*, September 25, 2020, <https://www.taiwannews.com.tw/en/news/4017032>; and 邱筠 [Yun Qiu], "中國抽砂船非法盜採海砂 大型艦艇接力守護馬祖" [China's Sand Pumping Ships Illegally Stole Sea Sand and Large Ships Relay to Protect Matsu], Central News Agency, September 25, 2020, <https://www.cna.com.tw/news/firstnews/202009250284.aspx>.
- 28 "表11-1 其他海巡績效統計—按月份分(續2完)" [Table 11-1 The Statistics of Other Business Performance—by Month (Cont.2, End)], 110年海巡統計年報 [110th Coast Guard Statistical Annual Report], 海洋委員會海巡署 [Coast Guard Administration of the Ocean Affairs Council], accessed November 4, 2022, <https://www.cga.gov.tw/GipOpen/wSite/public/Attachment/f1649862332064.pdf>; and "表11-1 其他海巡績效統計—按月份分(續2完)" [Table 11-1 The Statistics of Other Business Performance—by Month (Cont.2, End)], 111年09月績效統計月報 [111th September Performance Statistics Monthly Report], 海洋委員會海巡署 [Coast Guard Administration of the Ocean Affairs Council], accessed November 4, 2022, <https://www.cga.gov.tw/GipOpen/wSite/public/Attachment/f1667380233487.pdf>.
- 29 Shen Jianguang, "China's 'Six Priorities' and Fiscal Stimulus Will Spearhead Its COVID-19 Recovery," World Economic Forum, June 8, 2020, <https://www.weforum.org/agenda/2020/06/china-stimulus-covid19-economic-recovery/>.
- 30 "China's Full Year Infrastructure Investment in 2020 Set to Exceed \$3.6 Trillion Following COVID-19," China Banking News, April 21, 2020, <https://www.chinabankingnews.com/2020/04/21/chinas-full-year-infrastructure-investment-set-to-exceed-3-6-trillion-following-covid-19/>.
- 31 Caroline Meinhardt, "China Bets on 'New Infrastructure' to Pull the Economy Out of Post-Covid Doldrums," MERICS, June 4, 2020, <https://merics.org/en/short-analysis/china-bets-new-infrastructure-pull-economy-out-post-covid-doldrums>; and Frank Tang, "China Mega Projects: 6 Controversial Infrastructure Plans for the World's No 2 Economy," *South China Morning Post*, January 30, 2022, https://www.scmp.com/economy/china-economy/article/3165123/china-mega-projects-6-controversial-infrastructure-plans?module=perpetual_scroll_0&pgtype=article&campaign=3165123.
- 32 "Xiamen Xiang'an Airport," Centre for Aviation (CAPA), accessed February 9, 2023, <https://centreforaviation.com/data/profiles/newairports/xiamen-xiangan-airport>.
- 33 "表11-1 其他海巡績效統計—按月份分(續2完)" [Table 11-1 The Statistics of Other Business Performance—by Month (Cont.2, End)], and "表11-1 其他海巡績效統計—按月份分(續2完)" [Table 11-1 The Statistics of Other Business Performance—by Month (Cont.2, End)], 110年海巡統計年報 [110th Coast Guard Statistical Annual Report].
- 34 Feliz Solomon and Rajesh Roy, "As a Tiny Island Is Militarized, India Worries about China's Growing Footprint," *Wall Street Journal*, April 15, 2023, <https://www.wsj.com/articles/as-a-tiny-island-is-militarized-india-worries-about-chinas-growing-footprint-7e2c7f0e>.
- 35 Gregory Poling, "The Conventional Wisdom on China's Island Bases Is Dangerously Wrong," War on the Rocks, January 10, 2020, <https://warontherocks.com/2020/01/the-conventional-wisdom-on-chinas-island-bases-is-dangerously-wrong/>.
- 36 Elisabeth Braw, "China Is Stealing Taiwan's Sand," *Foreign Policy*, July 11, 2022, <https://foreignpolicy.com/2022/07/11/china-stealing-taiwan-sand/>; and Lee, "China's Latest Weapon against Taiwan."
- 37 Ibid.
- 38 Southerland, *China's Island Building in the South China Sea*; Danwei Huang et al., "Extraordinary Diversity of Reef Corals in the South China Sea," *Marine Biodiversity* 45, no. 2 (June 2015): 157–68, doi:10.1007/s12526-014-0236-1; Allen-Ebrahimian, "Beijing Calls South China Sea Island Reclamation a 'Green Project';" and UN General Assembly, *Convention on the Law of the Sea*, 1833 U.N.T.S. 397, December 10, 1982, <https://www.refworld.org/docid/3dd8fdb4.html>.
- 39 Xinmin Ma, "China and the UNCLOS: Practices and Policies," *Chinese Journal of Global Governance* 5, no. 1 (March 2019): 1–20, doi:10.1163/23525207-12340036; Tuan N. Pham, "China Can't Just 'Pick and Choose' from the Law of the Sea," East Asia Forum, July 27, 2018, <https://www.eastasiaforum.org/2018/07/27/china-cant-just-pick-and-choose-from-the-law-of-the-sea/>; and Jon Marek, "US-China International Law Disputes in the South China Sea," Wild Blue Yonder, Air University, July 9, 2021, <https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/2685294/us-china-international-law-disputes-in-the-south-china-sea/>.
- 40 Bonny Lin et al., *Competition in the Gray Zone: Countering China's Coercion Against U.S. Allies and Partners in the Indo-Pacific* (Santa Monica, CA: RAND, 2022), v, <https://www.rand.org/pubs/research-reports/RRA594-1.html>.
- 41 "China's Military Conducts Assault Drills in Seas near Taiwan," Defense News, August 17, 2021, <https://www.defensenews.com/training-sim/2021/08/17/chinas-military-conducts->

- [assault-drills-in-seas-near-taiwan/](#); and Ellis Kim, "China Starts Biggest-Ever Military Drills around Taiwan in Wake of Pelosi's Visit," CBS News, August 5, 2022, <https://www.cbsnews.com/news/china-missiles-waters-around-taiwan-regional-tensions-highest-levels-decades/>.
- 42 "China's Military Conducts Assault Drills in Seas near Taiwan," Defense News; and Kim, "China Starts Biggest-Ever Military Drills around Taiwan in Wake of Pelosi's Visit."
- 43 "UPDATE: China Risks Flare-Up Over Malaysian, Vietnamese Gas Resources," CSIS, Asia Maritime Transparency Initiative, December 13, 2019, <https://amti.csis.org/china-risks-flare-up-over-malaysian-vietnamese-gas-resources/>.
- 44 Jim Garamone, "General Cites 'Broader' Pattern of Chinese Harassment," U.S. Department of Defense, March 2, 2023, <https://www.defense.gov/News/News-Stories/Article/Article/3317545/general-cites-broader-pattern-of-chinese-harassment/>.
- 45 Michael Peck, "Vivid New Photos Give You a Rare Look at the South China Sea Islands That a Top US Commander Says China Has Fully Militarized," Business Insider, December 26, 2022, <https://www.businessinsider.com/photos-show-details-of-chinese-south-china-sea-military-bases-2022-12>; "More Than 5,000 Chinese Military Staff Live on Islands in the South China Sea," Radio Free Asia, October 11, 2022, <https://www.rfa.org/english/news/southchinasea/chinese-islands-10112022033029.html>; David Brunstrom, "China Installs Weapons Systems on Artificial Islands: U.S. Think Tank," Reuters, December 14, 2016, <https://www.reuters.com/article/us-southchinasea-china-arms/china-installs-weapons-systems-on-artificial-islands-u-s-think-tank-idUSK8N14310K>; Sanger and Gladstone, "Piling Sand in a Disputed Sea, China Literally Gains Ground;" and Jones, *Three Dangerous Men*, 156–59.
- 46 Matthew P. Funaiole et al., "China Is Deepening Its Military Foothold along the Indian Border at Pangong Tso," CSIS, ChinaPower Project, November 28, 2022, <https://chinapower.csis.org/analysis/china-satellite-imagery-military-pangong-tso/>.
- 47 "国防白皮书:中国武装力量的多样化运用" [National Defense White Paper: The Diversified Use of China's Armed Forces], 中华人民共和国国务院新闻办公室 [Information Office of the State Council of the People's Republic of China], originally published April 16, 2013, archived April 9, 2021, https://web.archive.org/web/20210409213940/http://www.mod.gov.cn/affair/2013-04/16/content_4442839.htm; Conor M. Kennedy and Andrew S. Erickson, "China Maritime Report No. 1: China's Third Sea Force, The People's Armed Forces Maritime Militia: Tethered to the PLA," U.S. Naval War College, *CMSI China Maritime Reports*, March 1, 2017, <https://digital-commons.usnwc.edu/cmsi-maritime-reports/1>; Gregory B. Poling, Tabitha Grace Mallory, and Harrison Prétat, *Pulling Back the Curtain on China's Maritime Militia* (Washington, DC: CSIS Asia Maritime Transparency Initiative and the Center for Advanced Defense Studies, November 2021), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/211118_Poling_Maritime_Militia.pdf?y5iaJ4NT8eITSIAKTr.TWxtDHuLiq7wR; and Shuxian Luo and Jonathan G. Panter, "China's Maritime Militia and Fishing Fleets: A Primer for Operational Staffs and Tactical Leaders," *Military Review*, February 2021, 6–21, <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2021/Panter-Maritime-Militia/>.
- 48 Derek Grossman and Logan Ma, "A Short History of China's Fishing Militia and What It May Tell Us," RAND Corporation, April 6, 2020, <https://www.rand.org/blog/2020/04/a-short-history-of-chinas-fishing-militia-and-what.html>; and Poling, Mallory, and Prétat, "Pulling Back the Curtain on China's Maritime Militia."
- 49 Poling, Mallory, and Prétat, "Pulling Back the Curtain on China's Maritime Militia."
- 50 Luo and Panter, "China's Maritime Militia and Fishing Fleets"; "Regulations of the People's Republic of China on the Work of the Militia," Central Military Commission of the People's Republic of China, December 24, 1990, archived May 6, 2021, https://web.archive.org/web/20210506103422/http://www.mod.gov.cn/regulatory/2016-02/12/content_4618055.htm; and Benjamin Jebb and Laura Jones, interview with Gregory B. Poling and Sean Berg, "Little Blue Men in the South China Sea: Unmasking China's Maritime Militia," *Irregular Warfare Podcast*, podcast audio, May 6, 2022, <https://mwi.usma.edu/little-blue-men-in-the-south-china-sea-unmasking-chinas-maritime-militia/>.
- 51 Grossman and Ma, "A Short History of China's Fishing Militia and What It May Tell Us."
- 52 Poling, Mallory, and Prétat, "Pulling Back the Curtain on China's Maritime Militia;" and Jebb and Jones, "Little Blue Men in the South China Sea."
- 53 Poling, Mallory, and Prétat, "Pulling Back the Curtain on China's Maritime Militia;" Jebb and Jones, "Little Blue Men in the South China Sea"; and "南沙骨干渔船雇用员工合同书" [Spratly Backbone Fishing Vessel Employment Contract], 百度文库 [Baidu Library], February 12, 2019, <https://wenku.baidu.com/view/206be013f4335a8102d276a20029bd64783e62eb.html>.
- 54 Poling, Mallory, and Prétat, "Pulling Back the Curtain on China's Maritime Militia."
- 55 Ibid.
- 56 Luo and Panter, "China's Maritime Militia and Fishing Fleets."
- 57 Nguyen Hong Thao and Binh Ton-Nu Thanh, "Maritime Militias in the South China Sea," National Bureau of Asian Research (NBR), July 13, 2019, <https://www.nbr.org/publication/maritime-militias-in-the-south-china-sea/>; Mark J. Valencia, "The Standoff at Sandy Cay in the South China Sea," East Asia Forum, May 24, 2019, <https://www.eastasiaforum.org/2019/05/24/the-standoff-at-sandy-cay-in-the-south-china-sea/>; and Edcel John Ibarra, "The Controversy Surrounding Sandy Cay: Examining the Public Evidence," *The Maritime Review*, March 29, 2022, <https://maritimereview.ph/the-controversy-surrounding-sandy-cay-examining-the-public-evidence/>.
- 58 Ibarra, "The Controversy Surrounding Sandy Cay: Examining the Public Evidence."
- 59 Ibid.
- 60 Katie Zeng Xiaojun, "Background: GNSS Spoofing in China and Beyond," RiskIntelligence, June 29, 2021, <https://www.riskintelligence.eu/background-and-guides/background-gnss-spoofing-in-china-and-beyond>.
- 61 Xiaojun, "Background: GNSS Spoofing in China and Beyond"; Mark Harris, "Ghost Ships, Crop Circles, and Soft Gold: A GPS Mystery in Shanghai," *MIT Technology Review*, November 15, 2019, <https://www.technologyreview.com/2019/11/15/131940/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/>; and Dana A. Goward, "Patterns of GPS Spoofing at Chinese Ports," *The Maritime Executive*, December 19, 2019, <https://maritime-executive.com/editorials/patterns-of-gps-spoofing-at-chinese-ports>.
- 62 Xiaojun, "Background: GNSS Spoofing in China and Beyond."
- 63 Goward, "Patterns of GPS Spoofing at Chinese Ports."
- 64 "PRC Jamming and Spoofing Endanger Shipping, Threaten Civilian Air Navigation," Indo-Pacific Defense Forum, December 16, 2021, <https://ipdefenseforum.com/2021/12/prc-jamming-and-spoofing-endanger-shipping-threaten-civilian-air-navigation/>.

- 65 Alessandro Arduino, *China's Private Security Companies: The Evolution of a New Security Actor* (Washington, DC: National Bureau of Asian Research (NBR), September 2019), Special Report 80, 91–103, <https://www.nbr.org/wp-content/uploads/pdfs/publications/sr80-securing-the-belt-and-road-sep2019.pdf>; and Helena Legarda and Meia Nouwens, *Guardians of the Belt and Road* (Berlin: Mercator Institute for China Studies, August 2018), <https://www.merics.org/en/report/guardians-belt-and-road>.
- 66 Arduino, *China's Private Security Companies*.
- 67 “境外中资企业机构和人员安全管理指南” [Guidelines for the Safety Management of Overseas Chinese-Funded Enterprises and Personnel], 商务部对外投资和经济合作司 [Department of Foreign Investment and Economic Cooperation, Ministry of Commerce of the People's Republic of China], March 23, 2018, <http://images.mofcom.gov.cn/hzs/201803/20180323112639296.pdf>.
- 68 Ibid.; Meia Nouwens, “China's Use of Private Companies and Other Actors to Secure the Belt and Road across South Asia,” *Asia Policy* 14, no. 2 (2019): 13–20, <https://www.iiss.org/online-analysis/online-analysis/2019/04/china-bri>; and Legarda and Nouwens, *Guardians of the Belt and Road*.
- 69 For example, Frontier Services Group (先锋服务集团) acquired DeWe Security Limited—formerly part of the DeWe (Dulwich) International Security Group (德威国际安保集团)—on September 23, 2021. See “先丰签约收购海外安保公司, 大力提升核心安保能力” [Acquiring Overseas Security Company, FSG Enhances Security Capabilities Significantly], 先锋服务集团 [Frontier Services Group], originally published September 28, 2021, trans. published September 30, 2021, <http://www.fsgroup.com/news/show-681.html>.
- 70 Cortney Weinbaum, “China's Security Contractors Have Avoided the Fate of Russia's Military Contractors, So Far,” RAND Corporation, March 11, 2022, <https://www.rand.org/blog/2022/03/chinas-security-contractors-have-avoided-the-fate-of.html>.
- 71 Nouwens, “China's Use of Private Companies and Other Actors to Secure the Belt and Road across South Asia.”
- 72 Legarda and Nouwens, *Guardians of the Belt and Road*.
- 73 Alessandro Arduino, *The Footprint of Chinese Private Security Companies in Africa* (Washington, DC: School of Advanced International Studies, Johns Hopkins University, 2020), Working Paper No. 2020/35, <https://static.squarespace.com/static/5652847de4b033f56d2bdc29/t/5e7a733475a31172316a05d5/1585083189926/WP+35+-+Arduino+-+Chinese+Private+Security+Companies.pdf>; and Paul Nantulya, “Chinese Security Contractors in Africa,” Carnegie Endowment for International Peace, October 8, 2020, <https://carnegietsinghua.org/2020/10/08/chinese-security-contractors-in-africa-pub-82916>.
- 74 Arduino, *China's Private Security Companies*.
- 75 Yau Tsz Yan, “Chinese Private Security Moves Into Central Asia,” *The Diplomat*, July 3, 2019, <https://thediplomat.com/2019/07/chinese-private-security-moves-into-central-asia/>.
- 76 Ibid.
- 77 For more on Russian PMCs, see, for example, Seth G. Jones et al., *Russia's Corporate Soldiers: The Global Expansion of Russia's Private Military Companies* (Lanham, MD: Rowman & Littlefield, 2021), <https://www.csis.org/analysis/russias-corporate-soldiers-global-expansion-russias-private-military-companies>.
- 78 Yuan, “China's Private Security Companies and the Protection of Chinese Economic Interests Abroad”; and Jonas Parelló-Plesner and Mathieu Duchâtel, “China's Strong Arm: Protecting Citizens and Assets Abroad,” *Adelphi Papers* 54, no. 451 (2014), 1–155.
- 79 Christopher Spearin, “China's Private Military and Security Companies: ‘Chinese Muscle’ and the Reasons for U.S. Engagement,” National Defense University Press, *Prism*, vol. 8, no. 4, June 11, 2020, <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2217673/chinas-private-military-and-security-companies-chinese-muscle-and-the-reasons-f/>.
- 80 C. Todd Lopez, “U.S. Tracking High-Altitude Surveillance Balloon,” U.S. Department of Defense, February 2, 2023, <https://www.defense.gov/News/News-Stories/Article/Article/3287177/us-tracking-high-altitude-surveillance-balloon/>.
- 81 Ibid.
- 82 Ibid.; and Ellen Nakashima et al., “Chinese Balloon Part of Vast Aerial Surveillance Program, U.S. Says,” *Washington Post*, February 9, 2023, <https://www.washingtonpost.com/national-security/2023/02/07/china-spy-balloon-intelligence/>.
- 83 Biden, “Remarks by President Biden on the United States' Response to Recent Aerial Objects.”
- 84 Nakashima et al., “Chinese Balloon Part of Vast Aerial Surveillance Program, U.S. Says.”
- 85 Ibid.
- 86 习近平 [Xi Jinping], “习近平同志在中共中央政治局第八次集体学习时的讲话” [Comrade Xi Jinping's Remarks to the Eighth Collective Study Session of the CCP Politburo].
- 87 中共中央印 [Central Committee of the Communist Party of China], “深化党和国家机构改革方案” [Plan for Deepening the Reform of Party and State Institutions], 新华社 [Xinhua News Agency], March 21, 2018, http://www.gov.cn/zhengce/2018-03/21/content_5276191.htm#1.
- 88 Ryan D. Martinson and Peter A. Dutton, “China Maritime Report No. 3: China's Distant-Ocean Survey Activities: Implications for U.S. National Security,” U.S. Army War College, *CMSI China Maritime Reports*, November 1, 2018, <https://digital-commons.usnwc.edu/cmsi-maritime-reports/3>.
- 89 Martinson and Dutton, “China Maritime Report No. 3.”
- 90 “国海洋经济发展规划纲要” [Outline for the National Marine Economy Development Plan], 国家海洋局 [State Oceanic Administration], May 9, 2003, archived May 17, 2017, https://web.archive.org/web/20170517122313/www.soa.gov.cn/zwqk/fwqgwyl/gwylfwyl/201211/t20121105_5261.html; 胡锦涛 [Hu Jintao], “胡锦涛在中国共产党第十八次全国代表大会上的报告” [Hu Jintao's Report at the 18th Congress of the Chinese Communist Party], 新华社 [Xinhua News Agency], November 17, 2012, archived June 30, 2022, https://web.archive.org/web/20220630161540/www.xinhuanet.com/18cpcnc/2012-11/17/c_113711665.htm; 习近平 [Xi Jinping], “习近平同志在中共中央政治局第八次集体学习时的讲话” [Comrade Xi Jinping's Remarks to the Eighth Collective Study Session of the CCP Politburo]; Martinson and Dutton, “China Maritime Report No. 3”; and Alexander B. Gray, “The Deep Seabed Is China's Next Target,” American Foreign Policy Council (AFPC), July 15, 2021, <https://www.afpc.org/publications/articles/the-deep-seabed-is-chinas-next-target>.
- 91 倪桂桦 朱锋 [Ni Guihua and Zhu Feng], “拜登政府对华战略竞争的态势与困境” [The Situation and Dilemmas of the Biden Administration's Strategic Competition with China].
- 92 “China's Arctic Policy,” State Council Information Office, Government of the People's Republic of China, January 26, 2018, http://english.www.gov.cn/archive/white-paper/2018/01/26/content_281476026660336.htm.

- 93 Matthew P. Funaiolo et al., "Frozen Frontiers: China's Great Power Ambitions in the Polar Regions," Hidden Reach, CSIS, April 18, 2023, <https://features.csis.org/hiddenreach/china-polar-research-facility/>.
- 94 Ibid.; and The White House, *National Strategy for the Arctic Region* (Washington, DC: the White House, October 2022), <https://www.whitehouse.gov/wp-content/uploads/2022/10/National-Strategy-for-the-Arctic-Region.pdf>.
- 95 肖天亮 [Xiao Tianliang, ed.], *战略学* [The Science of Military Strategy], 164; and Funaiolo, "Frozen Frontiers: China's Great Power Ambitions in the Polar Regions."
- 96 "Icebreaker Returns to Shanghai after Completing Arctic Research Expedition," Xinhua News Agency, September 26, 2018, http://www.xinhuanet.com/english/2018-09/26/c_137494647.htm.
- 97 王妍 [Wang Yan], "北极科考:随冰漂流" [Arctic Exploration: Drifting with the Ice], 中外对话海洋 [China Dialogue Ocean], March 2, 2020, <https://chinadialogueocean.net/zh/2/77438/>.
- 98 Sheena Chesnut Greitens, "Xi Jinping's Quest for Order," *Foreign Affairs*, October 3, 2022, <https://www.foreignaffairs.com/china/xi-jinping-quest-order>.
- 99 "Xi Jinping Delivers a Keynote Speech at the Opening Ceremony of the Boao Forum for Asia Annual Conference 2022," Ministry of Foreign Affairs of the People's Republic of China, April 21, 2022, https://www.fmprc.gov.cn/eng/zxxx_662805/202204/t20220421_10671083.html.
- 100 Chen Xiangyang, Dong Chunling, and Han Liquan, "Deep Comprehension of the Global Security Initiative: Coordinating Our Own Security and Common Security," Interpret: China, May 9, 2022, <https://csis-website-prod.s3.amazonaws.com/s3fs-public/event/220629-Global-Security%20-Initiative.pdf?Jz3L5nhX0xQWEdCLOzi48lmiizARlHr>.
- 101 "The Global Security Initiative," Ministry of Foreign Affairs of the People's Republic of China, concept paper, February 21, 2023, https://www.fmprc.gov.cn/mfa_eng/wbwx/202302/t20230221_11028348.html.
- 102 Carla Freeman and Alex Stephenson, "Xi Kicks Off Campaign for a Chinese Vision of Global Security," United States Institute of Peace, October 5, 2022, <https://www.usip.org/publications/2022/10/xi-kicks-campaign-chinese-vision-global-security>.
- 103 肖天亮 [Xiao Tianliang, ed.], *战略学* [The Science of Military Strategy], 36.
- 104 Alex Stone and Peter Wood, "China's Military-Civil Fusion Strategy," China Aerospace Studies Institute, June 15, 2020, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Other-Topics/2020-06-15%20CASI_China_Military_Civil_Fusion_Strategy.pdf.
- 105 Stone and Wood, "China's Military-Civil Fusion Strategy"; and Shawna Sinnott and Laura Jones, interviewing David Shear and Zack Cooper, "China's Strategically Irregular Approach: The Art of the Gray Zone," Irregular Warfare Podcast, podcast audio, August 27, 2021, <https://mwi.usma.edu/chinas-strategically-irregular-approach-the-art-of-the-gray-zone/>.
- 106 Paul Nantulya, "Chinese Security Firms Spread along the African Belt and Road," Africa Center for Strategic Studies, June 15, 2021, <https://africacenter.org/spotlight/chinese-security-firms-spread-african-belt-road/>.
- 107 On lawfare and Chinese challenges to rules-based international order, see, for example, Matthew H. Ormsbee, "Lawcraft: China's Evolving Approach to International Law and the Implications for American National Security," *Fordham Law Review Online* 90, no. 1 (2021), 1-22, <https://ir.lawnet.fordham.edu/flro/vol90/iss1/1/>.

Orde F. Kittrie, "The Chinese Government Adopts and Implements a Lawfare Strategy," in *Lawfare: Law as a Weapon of War*, ed. Orde F. Kittrie (Oxford, UK: Oxford University Press, 2016), 191-96, doi:10.1093/acprof:oso/9780190263577.003.0004; and Robert D. Williams, "International Law with Chinese Characteristics: Beijing and the 'Rules-Based' Global Order," Brookings Institution, October 2020, https://www.brookings.edu/wp-content/uploads/2020/10/FP_20201012_international-law-china-williams.pdf; and Jebb and Jones, "Little Blue Men in the South China Sea."

- 108 习近平 [Xi Jinping], "习近平同志在中共中央政治局第八次集体学习时的讲话" [Comrade Xi Jinping's Remarks to the Eighth Collective Study Session of the CCP Politburo].

8. Economic Coercion

- 1 "Action Plan on the Belt and Road Initiative," The State Council, People's Republic of China, March 30, 2015, http://english.www.gov.cn/archive/publications/2015/03/30/content_281475080249035.htm.
- 2 "推动共建丝绸之路经济带和21世纪海上丝绸之路的愿景与行动" [Promoting the Vision and Actions of Jointly Building the Silk Road Economic Belt and the 21st Century Maritime Silk Road], 新华社 [Xinhua News Agency], March 28, 2015, [https://www.gov.cn/xinwen/2015-03/28/content_2839723.htm](http://www.gov.cn/xinwen/2015-03/28/content_2839723.htm).
- 3 Linda Robinson et al., *The Growing Need to Focus on Modern Political Warfare* (Santa Monica, CA: RAND, 2019), 1-2, <https://www.rand.org/pubs/research-briefs/RB10071.html>.
- 4 George F. Kennan, "The Inauguration of Organized Political Warfare," History and Public Policy Program Digital Archive, April 30, 1948, <https://history.state.gov/historicaldocuments/frus1945-50Intel/d269>.
- 5 For one account of the decrees, see Robert J. Bonner, "The Megarian Decrees," *Classical Philology* 16, no. 3 (July 1921): 238-45, doi:10.1086/360360.
- 6 Hal Brands, *The Twilight Struggle: What the Cold War Teaches Us About Great-Power Rivalry Today* (New Haven, CT: Yale University Press, 2022), 103-29.
- 7 For an overview of these indicators, see: Wayne M. Morrison, *China's Economic Rise: History, Trends, Challenges, and Implications for the United States*, CRS Report No. RL33534 (Washington, DC: Congressional Research Service, June 25, 2019), https://www.everycrsreport.com/files/20190625_RL33534_088c5467dd11365dd4ab5f72133db289fa10030f.pdf.
- 8 See, for example, Victor Cha, "How to Stop Chinese Coercion," *Foreign Affairs*, vol. 102, no. 1, January/February 2023, 89-101, <https://www.foreignaffairs.com/world/how-stop-china-coercion-collective-resilience-victor-cha>; and Matthew Reynolds and Matthew P. Goodman, *Deny, Deflect, Deter: Countering China's Economic Coercion* (Washington, DC: CSIS, March 2023), <https://www.csis.org/analysis/deny-deflect-deter-countering-chinas-economic-coercion>.
- 9 Robert Blackwill and Jennifer Harris, *War by Other Means: Geoeconomics and Statecraft* (Boston: Harvard University Press, April 2016), 149.
- 10 Curtis J. Milhaupt and Wentong Zheng, *Why Mixed-Ownership Reforms Cannot Fix China's State Sector* (Chicago, IL: Paulson Institute, January 2016), https://www.paulsoninstitute.org/wp-content/uploads/2017/01/PPM_SOE-Ownership_Milhaupt-and-Zheng_English_R.pdf.
- 11 Blackwill and Harris, *War by Other Means*, 149-150.
- 12 This definition borrows heavily from China scholars who have previously elaborated definitions of economic coercion.

- See, for example, Bonnie Glaser, "How China Uses Economic Coercion to Silence Critics and Achieve its Political Aims Globally," testimony before the 117th Congress, 1st. sess., Congressional-Executive Commission on China, 2021, <https://www.cecc.gov/sites/chinacommission.house.gov/files/documents/CECC%20Hearing%20Testimony%20-%20Bonnie%20Glaser.pdf>.
- 13 习近平 [Xi Jinping], "弘揚人民友誼 共創美好未來" [Promote People's Friendship and Create a Better Future Together], (speech, Nazarbayev University, Astana, Kazakhstan, September 7, 2013), https://www.beltandroad.gov.hk/important-speeches_20130907_tc.html.
 - 14 The total number of BRI MOUs in March 2022 was estimated to be between 140 to 147. Seven of these MOUs lacked clear independent confirmation. See Christoph Nedopil, "Countries of the Belt and Road Initiative (BRI) – Green Finance & Development Center," Green Finance & Development Center, March 2022, <https://greenfdc.org/countries-of-the-belt-and-road-initiative-bri/>.
 - 15 Frank Mourtiz, "China's Economic Coercion," in *China's Global Influence: Perspectives and Recommendations*, ed. Scott D. McDonald and Michael C. Burgoyne (Honolulu: Daniel K. Inouye Asia-Pacific Center for Security Studies, 2019), 174–89, <https://dkiapcss.edu/chinasglobalinfluence/>.
 - 16 Chris Horton and Steven Lee Myers, "Panama Establishes Ties With China, Further Isolating Taiwan," *New York Times*, June 13, 2017, <https://www.nytimes.com/2017/06/13/world/asia/taiwan-panama-china-diplomatic-recognition.html>; and Merrit Kennedy, "Panama Cuts Ties With Taiwan, Opts to Support China Instead," NPR, June 13, 2017, <https://www.npr.org/sections/thetwo-way/2017/06/13/532788702/panama-cuts-ties-with-taiwan-opts-to-support-china-instead>.
 - 17 Brooke Dunn, "Belt and Road Hazards, Coming to the Americas," *American Affairs Journal* 5, no. 3 (Fall 2021), <https://americanaffairsjournal.org/2021/08/belt-and-road-hazards-coming-to-the-americas/>.
 - 18 Chris Horton, "In Blow to Taiwan, Solomon Islands Is Said to Switch Relations to China," *New York Times*, September 16, 2019, <https://www.nytimes.com/2019/09/16/world/asia/solomon-islands-taiwan-china.html>; and Edward Cavanough, "When China Came Calling: Inside the Solomon Islands Switch," *The Guardian*, December 7, 2019, <https://www.theguardian.com/world/2019/dec/08/when-china-came-calling-inside-the-solomon-islands-switch>.
 - 19 Cavanough, "When China Came Calling," Peter Hartcher, "There's Gold in the Solomon Islands, but Not for the People Who Live There," *Sydney Morning Herald*, November 29, 2021, <https://www.smh.com.au/world/oceania/there-s-gold-in-the-solomon-islands-but-not-for-the-people-who-live-there-20211128-p59cx5.html>; and Damien Cave, "China Is Leasing an Entire Pacific Island. Its Residents Are Shocked," *New York Times*, October 16, 2019, <https://www.nytimes.com/2019/10/16/world/australia/china-tulagi-solomon-islands-pacific.html>.
 - 20 "Solomon Islands Signs China Pact, Defying Australia," *Taipei Times*, April 20, 2022, <https://www.taipeitimes.com/News/front/archives/2022/04/20/2003776902>; and "China Funds Solomon Islands' Telecoms Deal after Signing Security Pact," *Financial Times*, August 19, 2022, <https://www.ft.com/content/39ca5645-fd50-48a1-9f7f-e58170e0ad1c>.
 - 21 Sebastian Horn, Carmen M. Reinhart, and Christoph Trebesch, "How Much Money Does the World Owe China?," *Harvard Business Review*, February 26, 2020, <https://hbr.org/2020/02/how-much-money-does-the-world-owe-china>.
 - 22 "International Debt Statistics," The World Bank, accessed February 9, 2023, <https://www.worldbank.org/en/programs/debt-statistics/ids>.
 - 23 "Laos Grants 25-Year Concession to Chinese Company to Manage Power Grid," *Radio Free Asia*, March 16, 2021, <https://www.rfa.org/english/news/laos/grid-03162021152622.html>.
 - 24 Kai Schultz, "Sri Lanka, Struggling With Debt, Hands a Major Port to China," *New York Times*, December 12, 2017, <https://www.nytimes.com/2017/12/12/world/asia/sri-lanka-china-port.html>; Maria Abi-Habib, "How China Got Sri Lanka to Cough Up a Port," *New York Times*, June 25, 2018, <https://www.nytimes.com/2018/06/25/world/asia/china-sri-lanka-port.html>; Lauren Frayer, "In Sri Lanka, China's Building Spree Is Raising Questions About Sovereignty," NPR, December 13, 2019, <https://www.npr.org/2019/12/13/784084567/in-sri-lanka-chinas-building-spree-is-raising-questions-about-sovereignty>; and Seth G. Jones, *Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare* (New York: W.W. Norton, 2021).
 - 25 Ishaan Tharoor, "China Has a Hand in Sri Lanka's Economic Calamity," *Washington Post*, July 20, 2022, <https://www.washingtonpost.com/world/2022/07/20/sri-lanka-china-debt-trap/>; and Alexander Saeedy, Philip Wen, and Photographs by Ishan Tankha, "Sri Lanka's Debt Crisis Tests China's Role as Financier to Poor Countries," *Wall Street Journal*, July 13, 2022, <https://www.wsj.com/articles/sri-lankas-debt-crisis-tests-chinas-role-as-financier-to-poor-countries-imf-bailout-11657735179>.
 - 26 See, for example, Deborah Brautigam, "A Critical Look at Chinese 'Debt-trap Diplomacy': The Rise of a Meme," *Area Development and Policy* 5, no. 1 (2020): 1–15, doi:10.1080/23792949.2019.1689828; Lee Jones and Shahar Hameiri, *Debunking the Myth of 'Debt-trap Diplomacy': How Recipient Countries Shape China's Belt and Road Initiative* (London: Chatham House, 2020), <https://www.chathamhouse.org/2020/08/debunking-myth-debt-trap-diplomacy>; Ajit Singh, "The Myth of 'Debt-trap Diplomacy' and Realities of Chinese Development Finance," *Third World Quarterly* 42, no. 2 (2021): 1–15, doi:10.1080/01436597.2020.1807318; and Shahar Hameiri, "Debunking the Myth of China's 'Debt-trap Diplomacy,'" Lowy Institute, The Interpreter, September 9, 2020, <https://www.loyvinstitute.org/the-interpreter/debunking-myth-china-s-debt-trap-diplomacy>.
 - 27 On unique terms of Chinese lending, see, for example, Anna Gelpern et al., "How China Lends: A Rare Look into 100 Debt Contracts with Foreign Governments," *Economic Policy*, eiac054, (2022), <https://www.aiddata.org/publications/how-china-lends-journal-article>.
 - 28 Ibid.
 - 29 Alex Vines, Creon Butler, and Yu Jie, *China's Evolving Approach to African Debt Relief and Future Lending* (London: Chatham House, 2022), <https://www.chathamhouse.org/2022/12/response-debt-distress-africa-and-role-china/03-chinas-evolving-approach-african-debt>.
 - 30 See, for example, Dr. Harry Verhoeven's remarks in Kate Bartlett, "China Cancels 23 Loans to Africa Amid 'Debt Trap' Debate," *Voice of America*, August 25, 2022, <https://www.voanews.com/a/china-cancels-23-loans-to-africa-amid-debt-trap-debate-/6716397.html>.
 - 31 Xi Jinping, "Full Text: Keynote Speech by Chinese President Xi Jinping at Opening Ceremony of 8th FOCAC Ministerial Conference," Forum on China-Africa Cooperation, trans. Xinhua News Agency, December 2, 2021, http://www.focac.org/eng/qdtp/202112/t20211202_10461080.htm.
 - 32 Jyhjong Hwang and Oyintarelado (Tarela) Moses, "China's Interest-Free Loans to Africa," Boston University, Global

- Development Policy Center, *GCI Policy Brief* no. 015, September 2022, https://www.bu.edu/gdp/files/2022/09/GCI_PB_015_FIN.pdf.
- 33 Deborah Brautigam and Yinxuan Wang, "Global Debt Relief Dashboard: Tracking Chinese Debt Relief in the COVID-19 Era," China Africa Research Initiative (CARI), Johns Hopkins University School of Advanced International Studies, Version 1.6, January 2021, <http://www.sais-cari.org/debt-relief>.
 - 34 "Ecuador Reaches Deal with China to Restructure Debt," Reuters, September 20, 2022, <https://www.reuters.com/world/americas/ecuador-reaches-deal-with-china-restructure-debt-2022-09-20/>.
 - 35 Alex He, "The Digital Silk Road and China's Influence on Standard Setting," Centre for International Governance Innovation, CIGI Papers No. 264, April 2022, https://www.cigionline.org/static/documents/no.264_JN9TbQC.pdf; and "Action Plan on the Belt and Road Initiative," The State Council, People's Republic of China, March 30, 2015, http://english.www.gov.cn/archive/publications/2015/03/30/content_281475080249035.htm.
 - 36 Xi Jinping, "Work Together to Build the Silk Road Economic Belt and The 21st Century Maritime Silk Road," Xinhua News Agency, trans. Xinhua News Agency, Belt and Road Forum for International Cooperation, May 14, 2017, https://www.xinhuanet.com/english/2017-05/14/c_136282982.htm.
 - 37 See, for example, Jonathan E. Hillman, *The Digital Silk Road: China's Quest to Wire the World and Win the Future* (New York: Harper Business, 2021); and Robert Greene Triolo Paul, "Will China Control the Global Internet Via its Digital Silk Road?," Carnegie Endowment for International Peace, May 8, 2020, <https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857>.
 - 38 Samantha Hoffman and Nathan Attrill, "Supply Chains and the Global Data Collection Ecosystem," Australian Strategic Policy Institute, Policy Brief Report No. 45/2021, June 2021, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2021-06/Supply%20chains.pdf?VersionId=56J_t8xYXYsMuhriQt5dSsr92ADaZH.
 - 39 Hillman, *The Digital Silk Road*, 14; "A Addis-Abeba, le siège de l'Union africaine espionné par Pékin," *Le Monde*, January 26, 2018, https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html; and John Aglionby, "African Union Accuses China of Hacking Headquarters," *Financial Times*, January 29, 2018, <https://www.ft.com/content/c26a9214-04f2-11e8-9650-9c0ad2d7c5b5>.
 - 40 Hillman, *The Digital Silk Road*, 14; "A Addis-Abeba, le siège de l'Union africaine espionné par Pékin," *Le Monde*; and Aglionby, "African Union Accuses China of Hacking Headquarters."
 - 41 Hillman, *The Digital Silk Road*, 14; and Raphael Sutter, "EXCLUSIVE: Suspected Chinese Hackers Stole Camera Footage from African Union," Reuters, December 16, 2020, <https://www.reuters.com/world/china/exclusive-suspected-chinese-hackers-stole-camera-footage-african-union-memo-2020-12-16/>.
 - 42 Hillman, *The Digital Silk Road*, 14; and Sutter, "EXCLUSIVE: Suspected Chinese Hackers Stole Camera Footage from African Union."
 - 43 "中共中央 国务院印发'国家标准化发展纲要'" [The Chinese Communist Party Central Committee and the State Council Publish the 'National Standardization Development Outline'], 新华社 [Xinhua News Agency], October 10, 2021, trans. Etcetera Language Group, Inc. for Center for Security and Emerging Technology, https://cset.georgetown.edu/wp-content/uploads/t0406_standardization_outline_EN.pdf.
 - 44 He, "The Digital Silk Road and China's Influence on Standard Setting," Hoffman and Attrill, "Supply Chains and the Global Data Collection Ecosystem"; and Elsa Kania, "China's Play for Global 5G Dominance—Standards and the 'Digital Silk Road,'" Australia Strategic Policy Institute, *The Strategist*, June 27, 2018, <https://www.aspistrategist.org.au/chinas-play-for-global-5g-dominance-standards-and-the-digital-silk-road/>.
 - 45 Daniel Fuchs and Sarah Eaton, "Diffusion of Practice: The Curious Case of the Sino-German Technical Standardization Partnership," SSRN, January 6, 2021, doi:10.2139/ssrn.3723303.
 - 46 Hillman, *The Digital Silk Road*, 217–23.
 - 47 David Uren, "Economic Coercion: Boycotts and Sanctions—Preferred Weapons of War," Australian Strategic Policy Institute, October 15, 2020, <https://www.aspi.org.au/report/economic-coercion-boycotts-and-sanctions-preferred-weapons-war>; and Charles Miller, "Explaining China's strategy of implicit economic coercion. Best left unsaid?," *Australian Journal of International Affairs* 76, no. 5 (2022): 507–21, doi:10.1080/10357718.2022.2061418.
 - 48 "Huawei and ZTE Handed 5G Network Ban in Australia," BBC News, August 23, 2018, <https://www.bbc.com/news/technology-45281495>; Raymond Zhong, "Australia Bars China's Huawei From Building 5G Wireless Network," *New York Times*, August 23, 2018, <https://www.nytimes.com/2018/08/23/technology/huawei-banned-australia-5g.html>; and Nic Fildes, "Australia Rides out Chinese Sanctions as Exports Boom," *Financial Times*, October 26, 2022, <https://www.ft.com/content/e4fb5cdc-da92-4ced-a56d-451f42336ba7>.
 - 49 Kirsty Needham and Stephanie Nebehay, "Australia Seeks Probe into Coronavirus Spread, France and UK Say Now Not the Time," Reuters, April 22, 2020, <https://www.reuters.com/article/us-health-coronavirus-australia-idUSKCN2240IK>.
 - 50 James Laurenceson, Michael Zhou, and Thomas Pantle, "Interrogating Chinese economic coercion: the Australian experience since 2017," *Security Challenges* 16, no. 4 (2020): 3–23, <https://www.jstor.org/stable/10.2307/26976255>.
 - 51 Ron Wickes, Mike Adams, and Nicolas Brown, "Economic Coercion by China: The Impact on Australia's Merchandise Exports," Institute for International Trade, University of Adelaide, Working Paper 04, July 2021, https://cisp.cachefly.net/assets/articles/attachments/86052_wp04-economic-coercion-by-china-the-effects-on-australias-merchandise-exports.pdf.
 - 52 Natasha Kassam, *Poll 2022: Understanding Australian Attitudes to the World* (Sydney, Australia: Lowy Institute for International Policy, June 2022), 18, <https://poll.loyyinstitute.org/files/loyyinsitutepoll-2022.pdf>.
 - 53 Katrin Bennhold and Jack Ewing, "In Huawei Battle, China Threatens Germany 'Where It Hurts': Automakers," *New York Times*, January 16, 2020, <https://www.nytimes.com/2020/01/16/world/europe/huawei-germany-china-5g-automakers.html>; "Chinese Ambassador Accused of Threatening German Car Industry If Huawei Is Frozen Out," *South China Morning Post*, December 15, 2019, <https://www.scmp.com/news/china/diplomacy/article/3042190/chinese-ambassador-accused-threatening-german-car-industry-if>; and Jones, *Three Dangerous Men*, 167–68.
 - 54 "Germany Resists US Pressure for Blanket Huawei Ban," *South China Morning Post*, December 3, 2022, <https://www.scmp.com/news/world/europe/article/3201933/germany-resists-us-pressure-blanket-huawei-ban>; and Sarah Marsh, "Germany Ups Reliance on Huawei for 5G despite Security Fears – Survey," Reuters, December 16, 2022, <https://www>.

[reuters.com/technology/germany-ups-reliance-huawei-5g-despite-security-fears-survey-2022-12-16/](https://www.reuters.com/technology/germany-ups-reliance-huawei-5g-despite-security-fears-survey-2022-12-16/).

- 55 "Taiwan to Open Its Representative Office in Lithuania," Ministry of Foreign Affairs of the Republic of Lithuania, July 20, 2021, <https://urm.lt/default/en/news/taiwan-to-open-its-representative-office-in-lithuania>.
- 56 "Foreign Ministry Spokesperson's Statement on China's Decision to Recall Its Ambassador to Lithuania," Foreign Ministry of the People's Republic of China, August 10, 2021, https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2535_665405/202108/t20210810_9170842.html.
- 57 Miller, "Explaining China's strategy of implicit economic coercion. Best left unsaid?," 507-21; "Chinese Embassy Suspends Visas in Lithuania," Delfi, November 26, 2021, <https://www.delfi.lt/a/88783959>; Andy Bounds, "Lithuania Complains of Trade 'Sanctions' by China after Taiwan Dispute," *Financial Times*, December 3, 2021, <https://www.ft.com/content/0ebaa7c7-761d-445e-b3e4-f5d2c9b4768f>; and Orange Wang and Finbarr Bermingham, "Suspicion of Counterfeiting: China Bans Lithuanian Beef, Dairy and Alcohol," *South China Morning Post*, February 10, 2022, <https://www.scmp.com/economy/china-economy/article/3166507/chinas-lithuanian-beef-import-ban-labelled-unilateral>.
- 58 Vaida Kalinkaitė-Matuliauskienė, "We Have Been Sacrificed" - Laser Sector Representatives Decry Lithuania's China Policy," Lithuanian Radio and Television (LRT), January 20, 2022, <https://www.lrt.lt/en/news-in-english/19/1592701/we-have-been-sacrificed-laser-sector-representatives-decry-lithuania-s-china-policy>.
- 59 Teddy Ng, "Beijing to Sanction US Firms Linked to US \$2.2 Billion Taiwan Arms Deal," *South China Morning Post*, July 12, 2019, <https://www.scmp.com/news/china/diplomacy/article/3018419/beijing-impose-sanctions-us-firms-involved-us22-billion-taiwan>; and Raymond Zhong, "China Vows Sanctions on U.S. Firms Selling Arms to Taiwan," *New York Times*, July 12, 2019, <https://www.nytimes.com/2019/07/12/world/asia/taiwan-arms-china-sanctions.html>.
- 60 Miller, "Explaining China's strategy of implicit economic coercion."
- 61 Ibid.; Park Byong-su, "South Korea's 'Three No's' Announcement Key to Restoring Relations with China," *Hankyoreh*, November 2, 2017, https://english.hani.co.kr/arti/english_edition/e_international/817213.html; and Jo He-rim, "China Demands Korea Uphold 'Three Nos' Policy," *The Korea Herald*, July 28, 2022, <https://www.koreaherald.com/view.php?ud=20220728000666>.
- 62 Hillman, *The Digital Silk Road*, 230.

9. Countering China

- 1 U.S. Department of Defense, *2022 National Defense Strategy of the United States of America* (Washington, DC: U.S. Department of Defense, 2022), <https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF>.
- 2 White House, *National Security Strategy of the United States of America* (Washington, DC: White House, 2022), 4-6, <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>.
- 3 Lai Lin Thomala, "Box Office Revenue of the Most Successful Movies of All Time in China as of March 2, 2023," Statista, accessed February 2023, <https://www.statista.com/statistics/260007/box-office-revenue-of-the-most-successful-movies-of-all-time-in-china/>.

- 4 These goals were based, in part, on National Security Decision Directive 75, U.S. Relations with the USSR, January 17, 1983, <https://irp.fas.org/offdocs/nsdd/nsdd-75.pdf>.
- 5 Freedom House, *Freedom in the World 2023: Marking 50 Years in the Struggle for Democracy* (Washington, DC: March 2023), https://freedomhouse.org/sites/default/files/2023-03/FIW-World-2023_DigitalPDF.pdf; Sara Repucci and Amy Slipowitz, "Authoritarians on Offense," *Journal of Democracy* 33, no. 2 (April 2022): 45-59, doi:10.1353/jod.2022.0017; and Freedom House, *Beijing's Global Media Influence* (Washington, DC: 2022), 1, https://freedomhouse.org/sites/default/files/2022-09/BGMI_final_digital_090722.pdf.
- 6 Freedom House, *Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet* (Washington, DC: 2022), <https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf>.
- 7 On the Chinese practice of blocking internet sites and digital platforms, see Stony Brook University, University of Massachusetts Amherst, University of California Berkeley, and Citizen Lab at the University of Toronto, "GFWatch Dashboard," GFWatch, accessed June 11, 2023, <https://gfwwatch.org/overview>; and Peter C. Oleson, "Chinese Offensive Intelligence Operations," Association of Former Intelligence Officers, *The Intelligence: Journal of U.S. Intelligence Studies* 26, no. 1 (Fall 2020): 9-17, https://www.afio.com/publications/OLESON-Chinese-Offensive-Intelligence-Operations_AFIO_Vol26_No1-INTEL-Fall-2020.pdf.
- 8 Freedom House, *Freedom on the Net 2022*, 1.
- 9 See, for example, Adrian Shahbaz, *The Rise of Digital Authoritarianism* (Washington, DC: Freedom House, 2018), https://freedomhouse.org/sites/default/files/2020-02/10192018_FOTN-2018_Final_Booklet.pdf.
- 10 "Cyber Operations Enabling Expansive Digital Authoritarianism," National Intelligence Council, NICA 2020-027, April 7, 2020, <https://www.dni.gov/files/ODNI/documents/assessments/NICM-Declassified-Cyber-Operations-Enabling-Expansive-Digital-Authoritarianism-20200407--2022.pdf>.
- 11 John Locke, *Second Treatise of Government*, ed. C.B. Macpherson (Indianapolis: Hackett Publishing Company, 1952), 9.
- 12 Hal Brands, *The Twilight Struggle: What the Cold War Teaches Us About Great-Power Rivalry Today* (New Haven, CT: Yale University Press, 2022).
- 13 C. Textor, "English Language Training (ELT) Market Size in China in 2017 and 2022," Statista, September 23, 2019, <https://www.statista.com/statistics/967696/china-english-language-training-market-size>.
- 14 "English Language Training Market in China by End-user and Learning methods," PR Newswire, September 2022, <https://www.technavio.com/report/english-language-training-market-in-china-industry-analysis>.
- 15 "Language Instruction in the U.S., Market Size 2004-2029," IBIS World, July 29, 2022, <https://www.ibisworld.com/industry-statistics/market-size/language-instruction-united-states/>.
- 16 The per capita numbers include \$54 per person in China compared to \$4 per person in the United States.
- 17 See, for example, Peter Mattis, "How to Spy on China," *Foreign Affairs*, April 28, 2023, <https://www.foreignaffairs.com/china/how-to-spy-china-beijing-technology-mattis>.
- 18 Lingling Wei, "U.S. Think Tank Reports Prompted Beijing to Put a Lid on Chinese Data," *Wall Street Journal*, May 7, 2023, <https://www.wsj.com/articles/u-s-think-tank-reports-prompted-beijing-to-put-a-lid-on-chinese-data-5f249d5e>.

- 19 See, for example, Interpret: China (<https://interpret.csis.org/>), the Center for Security and Emerging Technology at Georgetown University (<https://cset.georgetown.edu/>), and the Department of the Air Force's China Aerospace Studies Institute (<https://www.airuniversity.af.edu/CASI/In-Their-Own-Words/>).
- 20 U.S. Department of Justice, "People's Republic of China Citizen Arrested for Stalking," Press Release, December 14, 2022, <https://www.justice.gov/usao-ma/pr/peoples-republic-china-citizen-arrested-stalking>.
- 21 "National Security Risks Affecting the Australian Higher Education and Research Sector," Australian Parliamentary Joint Committee on Intelligence and Security, March 19, 2021, https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/commint/3ca6fe4f-b221-48f6-812e-ccfd3cd59d55/Gsid=0000.
- 22 "Confucius Teaches Cultures," *China Daily*, June 25, 2014, https://www.chinadaily.com.cn/opinion/2014-06/25/content_17613251.htm; and Elizabeth Redden, "Confucius Controversies," Inside Higher Ed, July 24, 2014, <https://www.insidehighered.com/news/2014/07/24/debate-renews-over-confucius-institutes>.
- 23 "Petition to the Committee of the Council," Inside Higher Ed, 2014, [https://www.insidehighered.com/sites/default/files/files/Chicago%20Petition%20re%20Confucius%20Institute%20\(2\).docx](https://www.insidehighered.com/sites/default/files/files/Chicago%20Petition%20re%20Confucius%20Institute%20(2).docx).
- 24 Elizabeth Redden, "Rejecting Confucius Funding," Inside Higher Ed, April 29, 2014, <https://www.insidehighered.com/news/2014/04/29/chicago-faculty-object-their-campus-confucius-institute>.
- 25 "How Many Confucius Institutes Are in the United States?" National Association of Scholars, March 22, 2023, <https://www.nas.org/blogs/article/how-many-confucius-institutes-are-in-the-united-states>.
- 26 "Harvard University Professor Convicted of Making False Statements and Tax Offenses," U.S. Department of Justice, December 21, 2021, <https://www.justice.gov/opa/pr/harvard-university-professor-convicted-making-false-statements-and-tax-offenses>.
- 27 See, for example, "Thousand Talents Plan," Public Safety Canada, November 27, 2020, <https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20201201/020/index-en.aspx>; and Robert Fife and Steven Chase, "CSIS warns about China's efforts to recruit Canadian scientists," *Globe and Mail*, August 6, 2020, <https://www.theglobeandmail.com/politics/article-csis-warns-about-chinas-efforts-to-recruit-canadian-scientists/>.
- 28 "CanSino Vaccine," Public Safety Canada, August 20, 2021, <https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/19-en.aspx>.
- 29 See, for example, New Jersey Office of Homeland Security and Preparedness, *Annual Report: State Fiscal Year 2022* (Trenton, NJ: New Jersey Office of Homeland Security and Preparedness, 2022), <https://static1.squarespace.com/static/54d79f88e4b0db3478a04405/t/63ee99ff779318408c487006/1676581379978/NJOHSP+SFY22+Annual+Report.pdf>; and "Non-Kinetic Warfare Challenging U.S. Global Stance," New Jersey Office of Homeland Security and Preparedness, June 25, 2021, <https://static1.squarespace.com/static/54d79f88e4b0db3478a04405/t/60d5d99ac03cf36ddc2f4a65/1624627610414/Non-Kinetic+Warfare+Challenging+US+Global+Stance.pdf>.
- 30 "Cyber Operations Enabling Expansive Digital Authoritarianism," National Intelligence Council, April 7, 2020, NICA 2020-027, <https://www.dni.gov/files/ODNI/documents/assessments/NICM-Declassified-Cyber-Operations-Enabling-Expansive-Digital-Authoritarianism-20200407--2022.pdf>.
- 31 See, for example, "Soviet Active Measures," Hearings Before the Permanent Select Committee on Intelligence, U.S. Congress, House of Representatives, 97th Cong., 2nd sess., July 13, 14, 1982; and "Soviet Covert Action (The Forgery Offensive)," Hearings before the Subcommittee on Oversight of the Permanent Select Committee on Intelligence, U.S. Congress, House, 96th Cong., 2nd sess., February 6, 19, 1980.
- 32 Letter from George Washington to John Trumbull, June 25, 1799, in George Washington, *The Papers of George Washington*, Retirement Series, Vol. 4, 20 April 1799–13 December 1799, ed. W. W. Abbot (Charlottesville, VA: University Press of Virginia, 1999), 156–59.
- 33 A growing body of evidence suggests that there are numerous weaknesses and vulnerabilities with Chinese economic coercion. See Matthew Reynolds and Matthew P. Goodman, *Deny, Deflect, Deter: Countering China's Economic Coercion* (Washington, DC: CSIS, March 2023), <https://www.csis.org/analysis/deny-deflect-deter-countering-chinas-economic-coercion>.
- 34 Victor Cha, "How to Stop Chinese Coercion," *Foreign Affairs*, vol. 102, no. 1, January/February 2023, 89–101, <https://www.foreignaffairs.com/world/how-stop-china-coercion-collective-resilience-victor-cha>.
- 35 Ladislav Bittman, *The KGB and Soviet Disinformation: An Insider's View* (Washington, DC: Pergamon-Brassey's, 1985); Statement of Ladislav Bittman, Former Deputy Chief of the Disinformation Department of the Czechoslovak Intelligence Service, "Soviet Covert Action (The Forgery Offensive)"; and Statement of Stanislav Levchenko, former KGB Major, in "Soviet Active Measures." Also see Ilya Dzhirkvelov, *Secret Servant: My Life with the KGB and the Soviet Elite* (New York: Harper & Row, 1987).
- 36 The CIA covert action problem to aid Solidary was called QRHELPFUL. See, for example, Seth G. Jones, *A Covert Action: Reagan, the CIA, and the Cold War Struggle in Poland* (New York: W.W. Norton, 2018).
- 37 Intelligence and Security Committee of Parliament, *China* (London: His Majesty's Stationery Office, 2023), 2, <https://isc.independent.gov.uk/wp-content/uploads/2023/07/ISC-China.pdf>.
- 38 See, for example, Charles T. Cleveland, *The American Way of Irregular Warfare: An Analytical Memoir* (Santa Monica, CA: RAND, 2020), <https://www.rand.org/pubs/perspectives/PEA301-I.html>.
- 39 See, for example, "Minerals Security Partnership," U.S. Department of State, June 14, 2022, <https://www.state.gov/minerals-security-partnership/>.
- 40 Cha, "How to Stop Chinese Coercion."
- 41 See, for example, Michael J. Mazarr and Ashley L. Rhoades, *Testing the Value of the Postwar International Order* (Santa Monica, CA: RAND, 2018), https://www.rand.org/pubs/research_reports/RR2226.html; and Charles L. Glaser, "A Flawed Framework: Why the Liberal International Order Concept is Misguided," *International Security* 43, no. 4 (Spring 2019), 51–87, doi:10.1162/isec_a.00343.
- 42 "Six Things You May Not Know about Chinese Millennials," HSBC, 2018, <https://www.business.hsbc.com/navigator/made-for-china/six-things-you-may-not-know-about-chinese-millennials>.
- 43 Richard M. Langworth, ed., *Churchill by Himself: The Definitive Collection of Quotations* (New York: PublicAffairs, 2008), 574.

Appendix

- 1 Jingdong Yuan, "China's Private Security Companies and the Protection of Chinese Economic Interests Abroad," *Small Wars & Insurgencies* 33, no. 1-2 (2022): 173-95, doi:10.1080/09592318.2021.1940646; "About Us," Dulwich International Security Group, accessed November 18, 2022, <http://www.dewesecurity.com/qvwm>; Ahram Kharief, "China's Discreet Game in North Africa – Private Military Companies," *Rosa Luxemburg Stiftung*, March 2022, <https://rosaluxna.org/publications/chinas-discreet-game-in-north-africa-private-military-companies/>; Anuradha Dinam, "China's New Found Interest in Private Security Companies: An Assessment," Centre for Land Warfare Studies, September 2022, https://www.claws.in/static/1B-361_China%E2%80%99s-New-Found-Interest-in-Private-Security-Companies--An-Assessment.pdf; "Backed by Beijing, security firm Frontier Services Group makes push into Southeast Asia," *Intelligence Online*, April 12, 2022, <https://www.intelligenceonline.com/corporate-intelligence/2022/04/12/backed-by-beijing-security-firm-frontier-services-group-makes-push-into-southeast-asia,109767384-art>; Borges Nhamirre and Matthew Hill, "Erik Prince to Partner With Mozambique Hidden-Debt Companies," *Bloomberg*, December 12, 2017, <https://www.bloomberg.com/news/articles/2017-12-12/erik-prince-to-partner-with-mozambique-s-hidden-debt-companies?leadSource=uverify%20wall>; "Brief-China Security & Fire in Cooperation With China Security & Protection Group," *Reuters*, April 15, 2018, <https://www.reuters.com/article/brief-china-security-fire-in-cooperation/brief-china-security-fire-in-cooperation-with-china-security-protection-group-idUKH9NRO05J>; Paul Nantulya, "Chinese Security Contractors in Africa," Carnegie Endowment for International Peace, October 8, 2020, <https://carnegieendowment.org/2020/10/08/chinese-security-contractors-in-africa-pub-82916>; "德威国际集团" [Dulwich International Group], 快懂百科 [Baiké], accessed November 4, 2022, https://www.baiké.com/wikiid/2583948082012565212?prd=mobile&view_id=3ifpu5xdul8000; "Huadun Security Group," About Us, China Shield Security, accessed November 18, 2022, <https://chinashield.com.cn/about>; Paul Nantulya, "Chinese Security Firms Spread along the African Belt and Road," *Africa Studies for Strategic Studies*, June 15, 2021, <https://africacenter.org/spotlight/chinese-security-firms-spread-african-belt-road/>; "公司简介" [Company Profile], 关于CSTG [About CSTG], 中国安保技术集团 [China Security Technology Group], accessed November 4, 2022, <http://www.cstgkh.com/profile.html>; "中安保集团与巴布亚新几内亚(中国粤港澳大湾区)商务专员办事处签署战略合作协议" [China Security Group Signed a Strategic Cooperation Agreement with Papua New Guinea (China Guangdong-Hong Kong-Macao Greater Bay Area) Commercial Commissioner's Office], 集团新闻 [Group News], 中安保实业集团有限公司 [China Security & Protection Group Co., Ltd.], accessed November 18, 2022, <http://www.cspbj.com/News/Detail/597>; "中安保:打造中国保安行业领航企业" [China Security: Building a Leading Enterprise in China's Security Industry], 集团新闻 [Group News], 中安保实业集团有限公司 [China Security & Protection Group Co., Ltd.], accessed November 18, 2022, <http://www.cspbj.com/News/Detail/465>; "公司简介" [Company Profile], 关于我们 [About Us], 中安保实业集团有限公司 [China Security and Protection Group Co., Ltd.], accessed November 18, 2022, <http://www.cspbj.com/AboutUs>; "公司简介" [Company Profile], Overseas Security Guardians (HK) Co., Ltd., accessed November 18, 2022, <http://www.osqih.com/about/>; "中国安保技术集团有限公司与江苏省能源国际有限公司签署安保服务合作框架协议书" [China Security Technology Group Co., Ltd. and Jiangsu Energy International Co., Ltd. Signed a Security Service Cooperation Framework Agreement], 集团动态 [Group News], 中国安保技术集团 [China Security Technology Group], accessed November 4, 2022, <http://www.cstgkh.com/group/2238.html>; "总裁寄语" [Message from the President], 关于CSTG [About CSTG], 中国安保技术集团 [China Security Technology Group], accessed November 4, 2022, <http://www.cstgkh.com/message.html>; "CSP Handles Security for Beijing in Neighbouring Countries," *Intelligence Online*, April 11, 2020, <https://www.intelligenceonline.com/corporate-intelligence/2020/11/04/csp-handles-security-for-beijing-in-neighbouring-countries,109618883-art>; "中国安保技术集团巴基斯坦子公司与华为技术巴基斯坦(私有)有限公司续签安保服务合同" [China Security Technology Group Pakistan Subsidiary Renews Security Service Contract with Huawei Technologies Pakistan (Private) Co., Ltd.], 集团动态 [Group News], 中国安保技术集团 [China Security Technology Group], accessed November 4, 2022, <http://www.cstgkh.com/group/2237.html>; "中国安保技术集团斯里兰卡子公司签约中交四航局港口城项目" [China Security Technology Group's Sri Lanka Subsidiary Signed a Contract for the Port City Project of CCCC Fourth Navigation Bureau], 集团动态 [Group News], 中国安保技术集团 [China Security Technology Group], accessed November 4, 2022, <http://www.cstgkh.com/group/2225.html>; "China: Private Security Companies," Centre for China Analysis & Strategy, accessed November 18, 2022, <https://ccasindia.org/newsdetails.php?nid=1877>; "COSG, linked to China's People's Liberation Army in financial mess," *ANI*, March 22, 2022, <https://www.aninews.in/news/world/asia/cosg-linked-to-chinas-peoples-liberation-army-in-financial-mess20220322223811/>; "集团介绍" [About Us], 中国海外保安集团 [China Overseas Security Group], accessed November 18, 2022, <http://www.cosg-sg.com.cn/tjts/tjti/>; "Maritime Escort– [China Security] Sri Lanka Subsidiary," Ship Management Network, April 16, 2018, <http://www.shipmg.com/html/439.html>; Niva Yau and Dirk van der Kley, "The Growth, Adaptation, and Limitations of Chinese Private Security Companies in Central Asia," *Oxus Society for Central Asian Affairs*, October 13, 2020, <https://oxussociety.org/the-growth-adaptation-and-limitations-of-chinese-private-security-companies-in-central-asia/>; "About Us," Zhongjun Junhong Security Service Co., Ltd., accessed November 4, 2022, <https://www.zjihgroup.com/en/>; "汉卫国际对驻缅甸安保人员开展安全防恐培训" [Hanwei International Conducts Security and Anti-Terrorism Training for Security Personnel Stationed in Myanmar], 汉卫 国际安全护卫有限公司 [Hanwei International Security Services Co., Ltd.], accessed November 18, 2022, <http://www.hanweiss.com/news/show/862.html>; "服务范围" [Service Area], 公司简介 [Company Profile], Zhongjun, 中军弘保安服务有限公司 [Junhong Security Service Co., Ltd.], accessed November 18, 2022, <https://www.zjihgroup.com/Company/index.html>; Bongani Nkosi, "First China, SA security services," *Mail & Guardian*, December 21, 2014, <https://mg.co.za/article/2014-12-21-first-china-sa-security-services/>; "集团简介" [Group Profile], 关于先丰 [About First Fung], 先锋服务集团 [Frontier Services Group], accessed November 4, 2022, <http://www.fsgroup.com/aboutfsg.html>; "集团简介" [Group Profile], 关于我 [About Us], 华信中安(北京)保安服 [Huaxin Zhongan (Beijing) Security Service], accessed November 18, 2022, <http://www.hxzasecurity.com/intro/1.html>; "Global Risk Management," Huaxin Zhongan (Beijing) Security Services, accessed November 18, 2022, <http://www.hxzasecurity.com/intro/9.html>; "先丰服务集团核心业务" [Core Business of FSG Service Group], [先锋服务集团 [Frontier Services Group], accessed November 4, 2022, <http://www.fsgroup.com/index.html>; Rosalind Adams, "Blackwater Founder Erik Prince's New Company is Operating in Iraq," *Buzzfeed News*, April 26, 2019, <https://www.buzzfeednews.com/article/rosalindadams/blackwater-erik-prince-frontier-services-group-iraq>; "安全安保" [Safety and Security], 先丰服务集团核心业务 [Frontier

Services Group], accessed November 4, 2022, <http://www.fsgroup.com/save.html>; “先丰受邀参与尼日利亚中资企业联防联控” [First Fung Was Invited to Participate in the Joint Defense and Joint Protection of Chinese-Funded Enterprises in Nigeria], 新闻中心 [News Center], 先丰服务集团核心业务 [Frontier Services Group], accessed November 4, 2022, <http://www.fsgroup.com/news/show-741.html>; “先丰应邀为尼日利亚中资企业开展安全培训” [First Fung Was Invited to Carry Out Safety Training for Chinese-Funded Enterprises in Nigeria], 新闻中心 [News Center], 先丰服务集团核心业务 [Frontier Services Group], accessed November 4, 2022, <http://www.fsgroup.com/news/show-736.html>; “集团简介” [Group Profile], 关于华威 [About Huawei], Shandong Huawei Security Group Co., Ltd, accessed November 18, 2022, <http://www.hwbaoan.com/aboutus.html>; “Erik Prince company to build training centre in China’s Xinjiang,” Reuters, January 31, 2019, <https://www.reuters.com/article/us-china-xinjiang-idUSKCNIPPI69>; Gordon Feller, “An overview of foreign security involvement in Mozambique,” defenceWeb, April 7, 2021, <https://www.defenceweb.co.za/featured/an-overview-of-foreign-security-involvement-in-mozambique/>; “先丰签约收购海外安保公司, 大力提升核心安保能力” [Xianfeng Signed Contracts to Acquire Overseas Security Companies and Vigorously Improved Core Security Capabilities], 新闻中心 [News Center], 先丰服务集团核心业务 [Frontier Services Group], accessed November 4, 2022, <http://www.fsgroup.com/news/show-681.html>; “Frontier Services Group becomes first choice for Chinese firms in Africa after DeWe takeover,” Africa Intelligence, May 10, 2021, <https://www.africaintelligence.com/eastern-africa-and-the-horn/2021/10/05/frontier-services-group-becomes-first-choice-for-chinese-firms-in-africa-after-dewe-takeover.109696201-bre>; Alessandro Arduino, “The Footprint of Chinese Private Security Companies in Africa,” Johns Hopkins School of Advanced International Studies, China Africa Research Initiative, working paper no. 35, 2020, <https://static1.squarespace.com/static/5652847de4b033f56d2bdc29/t/5e7a733475a31172316a05d5/1585083189926/WP+35+-+Arduino+-+Chinese+Private+Security+Companies.pdf>; Helena Legarda and Meila Nouwens, “Guardians of the Belt and Road,” MERICS, August 16, 2018, <https://merics.org/en/report/guardians-belt-and-road>; Cortney Weinbaum et al., *China’s Weapons Exports and Private Security Contractors* (Santa Monica, CA: RAND Corporation, 2022), <https://www.rand.org/pubs/tools/TLA2045-1.html>; Scott Morgan, “China’s [Other] Presence in Africa,” *International Policy Digest*, July 16, 2020, <https://intpolicydigest.org/china-s-other-presence-in-africa/>; Valère Llobet, “Les Sociétés Militaires Privées Chinoises,” Centre Français de Recherche sur le Renseignement, August 2021, <https://cf2r.org/documentation/les-societes-militaires-privées-chinoises/>; Veerle Nouwens, “Who Guards the ‘Maritime Silk Road’?,” *War on the Rocks*, June 24, 2020, <https://warontherocks.com/2020/06/who-guards-the-maritime-silk-road/>; “VSS Introduction,” About Us, VSS Security Group, accessed November 18, 2022, <http://www.vss911.cn/EN/About.aspx?id=19>; “Our Services,” VSS Security Group, accessed November 18, 2022, <http://www.vss911.cn/EN/Services.aspx>; Valerio Fabbri, “Chinese Private Security Companies in Africa: A Tool of Interference,” *Geopolitica.info*, June 12, 2022, <https://www.geopolitica.info/chinese-private-security-companies-africa/>; Yau Tsz Yan, “Chinese Private Security Moves into Central Asia,” *The Diplomat*, July 3, 2019, <https://thediplomat.com/2019/07/chinese-private-security-moves-into-central-asia/>; Zi Yang, “China’s Private Security Companies: Domestic and International Roles,” Jamestown Foundation, *China Brief*, vol. 16, no. 15, October 2016, <https://jamestown.org/program/chinas-private-security-companies-domestic-international-roles/>; and Niva Yau, interview with Alessandro Arduino and Ameer Lutfi, *Boots Off the Ground*,

podcast audio, February 11, 2021, <https://mei.nus.edu.sg/event/boots-off-the-ground-security-in-transition-in-the-middle-east-and-beyond-episode-11-future-of-chinese-private-security-companies-in-central-asia/>

COVER DESIGN

HAMMER & SICKLE: EMBLEM OF THE COMMUNIST PARTY OF CHINA VIA WIKIMEDIA COMMONS (PUBLIC DOMAIN IN PEOPLE'S REPUBLIC OF CHINA)

CSIS | CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

**ROWMAN &
LITTLEFIELD**

Lanham • Boulder • New York • London
4501 Forbes Boulevard
Lanham, MD 20706
301-459-3366 | www.rowman.com

