

SCOTT W. HAROLD, NATHAN BEAUCHAMP-MUSTAFAGA,
JEFFREY W. HORNUNG

CHINESE DISINFORMATION EFFORTS ON SOCIAL MEDIA

For more information on this publication, visit www.rand.org/t/RR4373z3.

About RAND

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

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

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

Published by the RAND Corporation, Santa Monica, Calif.

© 2021 RAND Corporation

RAND® is a registered trademark.

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

ISBN: 978-1-9774-0719-1

Cover: James Thew/Adobe Stock; imaginima/Getty Images.

Limited Print and Electronic Distribution Rights

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

Preface

How are countries using social media—particularly disinformation campaigns—to influence the competitive space? How have governments, the private sector, and civil society responded to this threat? What more can be done? And what do all these conditions mean for future U.S. Air Force and joint force training and operations?¹ This report attempts to answer some of these questions as part of a broader study of disinformation campaigns on social media and the implications of those campaigns in great-power competition and conflict. The other volumes in this series are:

- Raphael S. Cohen, Nathan Beauchamp-Mustafaga, Joe Cheravitch, Alyssa Demus, Scott W. Harold, Jeffrey W. Hornung, Jenny Jun, Michael Schwille, Elina Treyger, and Nathan Vest, *Combating Foreign Disinformation on Social Media: Study Overview and Conclusions*, Santa Monica, Calif.: RAND Corporation, RR-4373/1-AF, 2021
- Elina Treyger, Joe Cheravitch, and Raphael S. Cohen, *Russian Disinformation Efforts on Social Media*, Santa Monica, Calif.: RAND Corporation, RR-4373/2-AF, forthcoming
- Raphael S. Cohen, Alyssa Demus, Michael Schwille, and Nathan Vest, *U.S. Efforts to Combat Foreign Disinformation on Social Media*, Santa Monica, Calif.: RAND Corporation, 2021, Not available to the general public.

¹ This report was completed before the creation of the U.S. Space Force and therefore uses the name “U.S. Air Force” to refer to both air and space capabilities.

The research reported here was commissioned by the Air Force Special Operations Command and conducted within the Strategy and Doctrine Program of RAND Project AIR FORCE as part of a larger study entitled “Bringing Psychological Operations and Military Information Support Operations into the Joint Force: Counterinformation Campaigns in the Social Media Age,” which was designed to assist the Air Force in evaluating the threat of foreign influence campaigns on social media and assessing possible Air Force, joint force, and U.S. government countermeasures.

This report should be of value to the national security community and interested members of the public, especially those with an interest in how global trends will affect the conduct of warfare.

RAND Project AIR FORCE

RAND Project AIR FORCE (PAF), a division of the RAND Corporation, is the Department of the Air Force’s (DAF’s) federally funded research and development center for studies and analyses, supporting both the United States Air Force and the United States Space Force. PAF provides the DAF with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future air, space, and cyber forces. Research is conducted in four programs: Strategy and Doctrine; Force Modernization and Employment; Manpower, Personnel, and Training; and Resource Management. The research reported here was prepared under contract FA7014-16-D-1000.

Additional information about PAF is available on our website:
www.rand.org/paf/

This report documents work originally shared with the DAF in September 2019. The draft report, issued on September 20, 2019, was reviewed by formal peer reviewers and DAF subject-matter experts.

Contents

Preface	iii
Summary	ix
Figures and Tables	vii
Acknowledgments	xiii
Abbreviations	xv

CHAPTER ONE

Introduction	1
Methodology	7
Overview	9

CHAPTER TWO

Chinese Social Media–Based Disinformation Operations in Theory ...	11
Chinese Approaches to Information Operations	11
No PLA Doctrine for Social Media	13
PLA Messaging Strategy of Content Tailoring and Audience Targeting ...	16
Other Uses of Social Media	28
Conclusion	31

CHAPTER THREE

Chinese Social Media–Based Information Operations in Practice	33
China’s Initial Social Media–Based Operations	34
Chinese Command and Control for Social Media Operations	36
Where Chinese Social Media Actors Are Headquartered	38
The Scale of Chinese Social Media Operations	39
China’s Reach to Foreign Audiences	41

Social Media Disinformation Campaign Execution..... 46
Enablers of Chinese Disinformation Operations..... 50
Service Spotlight: The PLAAF’s Approach to Social Media..... 59
Conclusion..... 63

CHAPTER FOUR

**Case Study: Insights from Taiwan’s Experience as China’s Main
Target for Social Media Disinformation** 65
Examples of Chinese Social Media Disinformation Against Taiwan..... 67
Conclusion..... 73

CHAPTER FIVE

Regional Experiences and Responses to Chinese Disinformation 77
Singapore..... 78
Philippines..... 88
Japan..... 102
Conclusion..... 112

CHAPTER SIX

Conclusion and Recommendations 119
Notional PRC Employment of Social Media Disinformation to
Target the U.S. Military..... 119
Policy Options and Recommendations..... 127
Recommendations for Air Force Special Operations Command and
the Joint Force..... 127
Recommendations for DoD..... 130
Recommendations for the Interagency..... 131
Recommendations for U.S. Government..... 133
Future Trends..... 136
Final Thoughts..... 137

APPENDIX

**Potential Chinese Vulnerabilities to Social Media–Based
Information Operations** 139

References 155

Figures and Tables

Figures

2.1.	Progression of Chinese Military Attention to Social Media	16
3.1.	Purported Image of Chinese Bomber Flying Near Mountains in Taiwan	59

Tables

3.1.	Overall Social Media Penetration in Select Countries	43
3.2.	Percentage Penetration of Specific Social Media Platforms in Select Countries.	43
3.3.	WeChat Penetration in Select Countries.	44
6.1.	Summary of Recommendations	128

Summary

Issue

The People’s Republic of China (PRC) is a near-peer competitor to the United States, with a large, technologically sophisticated set of military capabilities that could be deployed in a conflict over Taiwan, over contested features in the East China Sea or the South China Sea, in the event of a renewal of war in Korea, or in other contingencies. Given China’s emphasis on the role of information in warfare, understanding how the PRC—primarily the Chinese Communist Party’s Central Propaganda Department and the People’s Liberation Army (PLA) but also other organs of the Party-state—thinks about the use of disinformation campaigns on social media has emerged as an important question for U.S. national security policymakers and defense planners. China’s use of social media disinformation campaigns has expanded in the wake of the military reorganization of the PLA that was launched in 2015, which included the establishment of the PLA Strategic Support Force (PLASSF) as a new, separate service stood up with a mission focus on the conduct of information warfare. If the PLA or other Chinese Party-state organs were to be ordered to target the United States and its armed forces (especially the U.S. Air Force¹) using social media during a crisis or contingency, how would they do so?² What data,

¹ This report was completed before the creation of the U.S. Space Force and therefore uses the name “U.S. Air Force” to refer to both air and space capabilities.

² Since the drafting of this report in August 2019, Chinese officials and state media have employed disinformation against the United States, claiming that coronavirus disease 2019

evidence, and examples might be studied now to help better prepare defenses that are designed to deter Chinese social media disinformation campaigns by denying them a high prospect of succeeding?

Approach

We studied Chinese writings about information warfare and conducted more than two dozen interviews with subject-matter experts on China's actual practice of targeting Taiwan over the past three years. In doing so, we derived insights regarding how the PRC conducts social media disinformation campaigns. We also researched the experiences of other key U.S. allies and partners in Asia, such as Singapore, the Philippines, and Japan, including via interviews with subject-matter experts in those countries, to explore whether China had targeted these countries with disinformation spread via social media.

Conclusions

We conclude that:

- China is using Taiwan as a test bed for developing attack vectors using disinformation on social media.
- To date, in the case of Taiwan, China's use of disinformation has achieved mixed and somewhat limited results that are primarily in the political, not operational, domain.
- China has not carried out substantial disinformation attacks on other U.S. allies or partners (such as Singapore, the Philippines, or Japan).

(COVID-19) was a bioweapon brought to China by the U.S. Army and alleging that Taiwan was covering up a large-scale COVID-19 death toll. This report does not analyze these developments in depth because they occurred after the period of our primary data collection, but they are largely consonant with our findings about how China employs disinformation for political and psychological warfare.

- Nonetheless, Chinese disinformation campaigns still could be used to target the United States in the event of a crisis or conflict.

Recommendations

The U.S. Air Force Special Operations Command, the joint force, and the U.S. government should consider several possible steps in light of these findings.

The Air Force should:

- Incorporate adversary social media disinformation into training.
- Engage communities around U.S. bases and overseas military installations to build and increase trust.
- Raise awareness of PLA malign activity online.

In addition, the joint force and/or the U.S. government should:

- Consider building a database of PRC disinformation operations so as to identify patterns and vectors of delivery.
- Train the joint force and the broader Department of Defense workforce to recognize and resist foreign (and, in this case, specifically Chinese) disinformation campaigns.
- Explore the advantages and opportunities of using human versus technological solutions to identify and possibly counter or defeat disinformation efforts.
- Establish a trusted presence in all important social media platforms used across the Indo-Pacific so as to compete in the information domain.
- Establish a presence on Chinese-language social media platforms so as not to cede these valuable communications territories to the PRC government uncontested.
- Engage Chinese-American and Taiwanese-American military personnel and provide them with resources to identify and defeat Chinese disinformation operations that they might be exposed to.

- Engage with allies and/or partners to share information and best practices for identifying and countering Chinese disinformation on social media.
- Assess where best to allocate scarce resources—countering Chinese disinformation operations or responding to other forms of Chinese influence and interference operations.

Acknowledgments

The authors would like to thank Brig. Gen. Brenda Cartier, Maj. Shaun Owenby, Capt. Laura Jones, and Air Force Special Operations Command for their support and direction throughout the project. In addition, we wish to thank Ted Harshberger for unit leadership of RAND Project AIR FORCE (PAF) and Paula Thornhill for support from the PAF Strategy and Doctrine program that this study was conducted within. Overall project lead Raphael S. Cohen provided clear, consistent guidance and helpful feedback throughout, successfully managing the project's staffing and budgetary needs and ensuring we both had situational awareness of timelines and maintained fidelity to sponsor interests. Upon completion of an initial draft, Michael S. Chase and Chris Paul provided very useful comments as internal reviewers; from outside RAND, Anne-Marie Brady at the University of Canterbury in New Zealand gave us additional insights that helped tighten and sharpen our analysis. As we promised anonymity to our interviewees in Singapore, the Philippines, Japan, and Taiwan, we have opted not to thank them by name or institution but instead to trust that they know we are grateful for the generous support in terms of the time and resources they shared with us in the course of our research and to thank them collectively here. Of course, any errors of either fact or analysis that remain are solely those of the authors.

Abbreviations

C2	command and control
CCP	Chinese Communist Party
CCPPNR	China Council for the Promotion of Peaceful National Reunification
COFA	China Overseas Friendship Association
COVID-19	coronavirus disease 2019
CPAFFC	Chinese People's Association for Friendship with Foreign Countries
CPD	Central Propaganda Department
CRI	China Radio International
CZG	China Zhi Gong Party
DoD	U.S. Department of Defense
DPP	Democratic Progressive Party
ISIS	Islamic State
KMT	Kuomintang (Nationalist Party)
MDT	Mutual Defense Treaty
MSS	Ministry of State Security (China)
NGO	nongovernmental organization
PLA	People's Liberation Army
PLAAF	PLA Air Force
PLASSF	PLA Strategic Support Force

PRC	People's Republic of China
PTT	Professional Technology Temple
ROC	Republic of China (Taiwan)
TAO	Taiwan Affairs Office
UFWD	United Front Work Department (of the CCP)
USAF	U.S. Air Force

Introduction

The People's Republic of China (PRC)'s People's Liberation Army (PLA) is the closest peer or near-peer foreign military competitor that the United States faces worldwide, and its military buildup has received substantial and growing attention in recent years.¹ Although numerous previous studies have described the evolution of the PLA into an informatized force designed to “fight and win” local, limited wars, little research to date has examined how China thinks about and engages in disinformation campaigns via social media in advance of or during a

¹ Recent work on the PLA includes the following: Roger Cliff, *China's Military Power: Assessing Current and Future Capabilities*, New York: Cambridge University Press, 2015; John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era*, Washington, D.C.: National Defense University Press, 2018; Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win*, Washington, D.C., 2019; Jeffrey Engstrom, *System Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*, Santa Monica, Calif.: RAND Corporation, RR-1708-AF, 2018; M. Taylor Fravel, *Active Defense: China's Military Strategy Since 1949*, Princeton, N.J.: Princeton University Press, 2019; Scott W. Harold, *Defeat, Not Merely Compete: China's View of Its Military Aerospace Goals and Requirements in Relation to the United States*, Santa Monica, Calif.: RAND Corporation, RR-2588-AF, 2018; Eric Heginbotham, Michael Nixon, Forrest E. Morgan, Jacob L. Heim, Jeff Hagen, Sheng Li, Jeffrey Engstrom, Martin C. Libicki, Paul DeLuca, David A. Shlapak, David R. Frelinger, Burgess Laird, Kyle Brady, and Lyle J. Morris, *The U.S-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017*, Santa Monica, Calif.: RAND Corporation, RR-392-AF, 2015; Joe McReynolds, ed., *China's Military Strategy*, Washington, D.C.: Brookings Institution Press, 2016; Phillip C. Saunders, Arthur S. Ding, Andrew Scobell, Andrew N. D. Yang, and Joel Wuthnow, eds., *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*, Washington, D.C.: National Defense University Press, 2019; U.S. Department of Defense (DoD), *Annual Report to Congress on Military and Security Developments Involving the People's Republic of China*, Washington, D.C., 2001–2009.

conflict.² U.S. experts generally tend to assess the prospects of a conventional kinetic conflict with China as being fairly low, but there are several potential flashpoints, the main ones being a possible Chinese invasion of Taiwan, a clash over disputed features in the East China Sea or South China Sea, a contingency on the Korean peninsula, or a border war with India.³ Moreover, because the costs of an outright military clash are likely to be unacceptably high, many observers assess China as more likely to pursue its aims through gray-zone tactics as a first step, and such tactics could continue up to and through any conflict that ends up in a physical clash. Additionally, United Front and propaganda work—such as narrative-shaping; public opinion management; influence operations; and information warfare, including disinformation campaigns—are activities that the Chinese regime is engaged in at all times, including during what is nominally considered a period of “peacetime competition” by Western analysts.⁴ In light of this possibility, it is imperative that U.S. national security policymakers and defense planners understand how the Chinese Party-state at

² There are a few exceptions, notably Nathan Beauchamp-Mustafaga and Michael Chase, *Borrowing a Boat out to Sea: The Chinese Military's Use of Social Media for Influence Operations*, Washington, D.C.: John Hopkins SAIS, 2019; Anne-Marie Brady, *Magic Weapons: China's Political Influence Activities Under Xi Jinping*, Washington, D.C.: Wilson Center, 2017a; Larry Diamond and Orville Schell, eds., *Chinese Influence and American Interests: Promoting Constructive Vigilance*, Stanford, Calif.: Hoover Institution, 2018; Insikt Group, *Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion*, Boston, Mass.: Recorded Future, 2019; and Daniel Kliman, Andrea Kendall-Taylor, Kristine Lee, Joshua Fitt, and Carisa Nietzsche, *Dangerous Synergies: Countering Chinese and Russian Digital Influence Operations*, Washington, D.C.: Center for a New American Security, May 7, 2020. For previous RAND Corporation work on the topic, see Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends*, Santa Monica, Calif.: RAND Corporation, RR-2713-OSD, 2019, pp. 105–166.

³ James Dobbins, Andrew Scobell, Edmund J. Burke, David C. Gompert, Derek Grossman, Eric Heginbotham, and Howard Shatz, *Conflict with China Revisited: Prospects, Consequences, and Strategies for Deterrence*, Santa Monica, Calif.: RAND Corporation, PE-248-A, 2017.

⁴ Anne-Marie Brady, “On the Correct Use of Terms,” *China Brief*, Vol. 19, No. 9, May 9, 2019a.

the broadest level⁵—and the PLA, more specifically—might employ a social media disinformation campaign to target the United States; the U.S. armed forces; and, specifically, the U.S. Air Force (USAF).⁶ How might China wage such a campaign?⁷

In our research, we found that, despite having a long history of interest in information warfare, China was relatively slow to get into the disinformation business (Chapter Two). Since moving into this space, however, China has been quite active in using disinformation to target Taiwan (Chapters Three and Four), although how effective this has been in achieving China's broader aims remains under debate. Generally speaking, Chinese disinformation efforts nest within a broader architecture of Chinese influence operations, information campaigns, and political warfare. Beyond Taiwan, there is little evidence to date of China leveraging disinformation to target other key actors in the Indo-Pacific, notably Singapore, the Philippines, or Japan (Chapter Five), despite seemingly having both strategic motivation and opportunity to do so; this could be because China feels it has other, more-effective tools available to influence these countries' foreign and security policy choices, or it could be that China has simply chosen to prioritize other issues. However, it is possible that, in a future crisis or contingency, China might decide to target the United States more actively, using disinformation in support of its direct political-military goals; if it does so, one target set is likely to be ethnic Chinese-Americans or Taiwanese-Americans, whom Beijing regards as both more accessible (via Chinese-language communi-

⁵ We refer here to the Central Propaganda Department (CPD), the United Front Work Department (UFW), the Ministry of State Security (MSS), and other Party-state organs. These are discussed further below.

⁶ This report was completed before the creation of the U.S. Space Force and therefore uses the name "U.S. Air Force" to refer to both air and space capabilities.

⁷ Since the drafting of this report in August 2019, Chinese officials and state media employed disinformation against the United States, claiming that coronavirus disease 2019 (COVID-19) was a bioweapon brought to China by the U.S. Army, and alleging that Taiwan was covering up a large-scale death toll in the south of the country because of COVID-19. This report does not analyze these developments in depth because they occurred after the period of our primary data collection, but they are largely consonant with our findings about how China employs disinformation for political and psychological warfare.

cations) and more amenable to the PRC's influence.⁸ In advance of any Chinese effort to target the United States (and specifically USAF) with disinformation, USAF and U.S. government should evaluate options for deterrence by denial (Chapter Six). The appendix offers an initial consideration of the alternative of deterrence by punishment.

To date, much of what China has learned about disinformation warfare has been by engaging in the practice while targeting Taiwan society, notably specific individuals who are deemed to be influencers, political parties across the political spectrum, youth, retired military officers, and other key demographics. China's messages seek to sow discord, undermine trust in the central government, spur doubt about the nation's military competence, present an image of China as a land of opportunity and as a force that cannot be checked or resisted, and create an impression that Taiwan is isolated and cannot rely on either the United States or its formal diplomatic partners for assistance. China has approached Taiwan media consumers across a variety of social media platforms and through more traditional media, and uses social media to reinforce broader messages it is sending through its diplomatic, economic, covert and clandestine activities, and its overt military posturing. To succeed, China requires a wide variety of pre-existing conditions and prepositioned architecture. With these in place, China has been able to conduct three types of social media disinformation operations: target of opportunity attacks, steady-state disinformation campaigns, and longer-term projects built around creating narratives tied to predictable large-scale events (such as elections).

Many of these disinformation campaigns have been conducted by the new PLA Strategic Support Force (PLASSF), which was established in 2015 through wide-ranging reforms of the PLA that have "accelerated China's use of disinformation significantly."⁹ As noted in Chapter Three, however, the PLA Air Force (PLAAF) also has been involved in messaging via social media, and the CPD, UFWD, MSS, and Taiwan

⁸ Anne-Marie Brady, "Are We Real Friends? China–Albania Relations in the Xi Era," *Sinopsis*, October 17, 2019b.

⁹ Interview with Taiwan academic, interview 8, Taipei, January 2019.

Affairs Office (TAO) are likely also involved.¹⁰ As one Taiwan expert on PLA information operations commented, “the PLASSF is the main source of disinformation campaigns . . . the United Front Work Department and the Ministry of State Security basically target overseas Chinese.”¹¹ For a multiethnic society like the United States and a multiethnic organization like USAF, this means Chinese command and control (C2) for disinformation operations could involve multiple organizations, depending on whether Beijing’s intent is to target diaspora Chinese-Americans or non-ethnic Chinese.

We believe one of China’s first targets of disinformation on social media will be ethnic Chinese U.S. military officers and service members. This assessment is based on how Chinese experts write about extending China’s influence generally, and how the PRC has sought to target communities of overseas ethnic Chinese overseas historically, notably in Australia, New Zealand, and Taiwan.¹² Some likely vectors are platforms that China controls (such as WeChat [微信] and Weibo [微博]), and other platforms (such as Facebook or Twitter); through these, U.S. military personnel who communicate in Chinese will be more exposed to Chinese disinformation.¹³ PRC scholars write about

¹⁰ The Chinese Party-state follows a saturation approach to propaganda and influence operations, with multiple institutions collaborating and coordinating to carry out various parts of an operation. Although intra-agency and government-military coordination can prove challenging in the Chinese system (as elsewhere), the general model is one of “unified leadership, separated management, separated responsibility, but in coordination” [统一领导，分口管理，分口负责，协调配合] (Brady, 2019a). We thank reviewer Anne-Marie Brady for these insights.

¹¹ Interview with Taiwan think-tank analyst, interview 2A, Taipei, January 2019. It is important to note, however, that the UFWD, MSS, various front organizations, and other parts of the Party-state also actively target non-ethnic Chinese foreigners, seeking to dupe, co-opt, compromise, and otherwise turn such individuals as they see as having value into either active supporters or neutralized and nonthreatening. See Brady, 2017a.

¹² James Jiann Hua To, *Hand to Hand, Heart to Heart: Qiaowu and the Overseas Chinese*, University of Canterbury, New Zealand, thesis, 2009.

¹³ As this report was being drafted, the Chinese video-sharing app TikTok exploded in popularity in the United States, especially with younger Americans. In December 2019, DoD banned the use of TikTok for all U.S. military personnel. Because TikTok did not feature in any of our interviews or primary data collection, we do not cover it in the report. In March 2020, however, U.S. government officials contacted the firm over allegations of disinform-

the Chinese diaspora as a vector for influence because of a presumed common linguistic and cultural background and an ability to explain to their own societies why Beijing's policies are correct.¹⁴ Thus, service members' extended families and friends could also be an indirect vector for China to reach U.S. troops.

China also might seek to degrade U.S. military operations by targeting local communities around U.S. military bases in host nations with disinformation. Our interviews in Taiwan suggest that China has already specifically targeted local communities around Republic of China (ROC) military installations,¹⁵ so it is likely that PRC efforts to disrupt or degrade U.S. military operations in advance of or during a conflict might seek to sow rumors and disinformation in base-hosting communities in third countries—such as Japan, South Korea, or the Philippines (and in those in the continental United States, Alaska, Hawai'i, Guam, or other overseas territories). Such disinformation campaigns could strive to shut down operations by generating popular opposition; create an impression that the military is engaged in covering up accidents, crimes, or military setbacks; sow doubt about the wisdom and necessity of undertaking military operations in the face of Chinese opposition as a way to degrade morale; or encourage broader political opposition to decisions made in Washington, D.C., including by striving to split any allied war effort.

mation. Alfred Ng, "US Officials in Contact with TikTok over Political Disinformation," CNET.com, March 3, 2020. Separately, U.S. officials allege that China spread disinformation that same month inside the United States via text message, which points up that social media is (1) only one vector by which the PRC sows disinformation and seeks influence and (2) likely to be part of a broader strategic messaging campaign. See Edward Wong, Matthew Rosenberg, and Julian E. Barnes, "Chinese Agents Helped Spread Messages That Sowed Virus Panic in U.S., Officials Say," *New York Times*, April 22, 2020.

¹⁴ PRC writings on diasporic Chinese as vectors for Chinese influence include Liu Juntao, "Overseas Chinese and Chinese Soft Power from the Economic Perspective: The Case of Indonesia," *Science-Economy-Society* [科学经济社会], No. 3, December 2012; and Xu Mei, "The Driving Force and Restraining Factors of Southeast Asian Chinese in the Promotion of Chinese Soft Power," *Southeast Asian Studies* [东南亚研究], Vol. 6, 2010.

¹⁵ The Taiwan military refers to itself as the Republic of China Armed Forces; for brevity, we use ROC in this report.

To respond effectively, the United States will need to consider crafting policy in advance to manage service members' access to social media platforms that might constitute threat vectors during the run-up to and throughout the course of a conflict. The U.S. military should seriously consider training its forces to recognize and resist disinformation campaigns; it might wish to provide additional training and resources to its ethnic Chinese-American members to help them identify and resist any PRC disinformation operations targeting them. One option might be to strive to incorporate aspects of Red-team disinformation operations in future wargames as a way to surface and address vulnerabilities; this also could be undertaken with U.S. allies and partners to help sensitize them to the ways in which they could be targeted. U.S. information operations teams also might need to gain access and build trusted profiles on social media if they are going to counter PLA operations on these platforms. Finally, it might be worth taking a closer look at a holistic approach to countering Chinese social media disinformation campaigns at the national level by examining the roles of legislative action, campaigns aimed at raising social media literacy, the role of civil society, efforts to elicit cooperation from social media-hosting companies, and technical solutions (such as artificial intelligence) that can quickly flag disinformation.

Methodology

In this report, we examine how China thinks about the role and utility of social media disinformation campaigns for achieving political and military outcomes. We drew on open-source Chinese-language writings on social media campaigns and information operations for descriptions of how PRC analysts and writers talk about this subject. In addition, we derived insights into Chinese thinking and practice from the recent experience of Taiwan. Since mid-2017, China has been targeting Taiwan society, key political actors, and the ROC Armed Forces with disinformation spread across a variety of platforms, such as WeChat [微信]; Facebook; LINE; and the Professional Technology Temple (PTT), a popular bulletin board service. We carried out

a weeklong data collection effort in Taiwan in early 2019, meeting with more than 75 subject-matter experts. Our interviewees included high-ranking ROC Republic of China government officials, think-tank analysts, academics, members of the private sector, nongovernmental organization (NGO) workers from civil society striving to combat disinformation, and U.S. diplomats and military officers on temporary secondment to the American Institute in Taiwan (the unofficial body that helps manage interactions with Taiwan in the absence of formal diplomatic relations). We also derived insights from secondary source writings by Western experts on China and the PLA and from open-source media reports and commentary on China's activities worldwide—especially activities focused on Taiwan but also activities focused on U.S. allies and partners in Singapore, the Philippines, and Japan. The draft report was completed in August 2019 and updated only minimally thereafter to account for developments that either confirmed or required caveating our findings as they stood at that point in time.

A caveat is in order before proceeding further. Disinformation campaigns and efforts to sow discord are clandestine activities (i.e., the goal is for efforts to go unrecognized as disinformation)—failing that, such activities should at a minimum be covert (i.e., deniable and not attributable to specific Chinese state actors). This substantially complicates the ability to research this topic; in the absence of substantial time and access resources, much of what is reported is, of necessity, not definitive. We have sought, where possible, to note the level of certainty in our findings, but much of what we learned is impressionistic and drawn from plausible and widespread interpretations by local actors in Taiwan of what are believed to be disinformation events originating from China. Although some doubt could be raised about specific incidents of information on social media, which might or might not originate in China, we believe that, in the main, we capture the way that authoritative Chinese sources think about and undertake disinformation campaigns on social media.

Although we are interested in the general phenomenon of China's efforts to shape narratives and, in so doing, structure (or restructure) the international environment in ways favorable to the interests of the

Chinese Communist Party (CCP) and the PRC, our specific focus for this report is more narrowly on disinformation campaigns spread on social media. By *disinformation*, we are not referring to China's ahistorical or factually challenged claims about the righteousness of its policies or territorial claims. Instead, we are referring specifically to false, distorted, and/or decontextualized information, almost always about a temporally and spatially bounded concrete event or purported development, usually located in a foreign country, that is intended to achieve a relatively short-term behavioral or public opinion change in an overseas actor. By *social media*, we mean online personal networking websites, applications, and other platforms that enable individuals to upload, broadcast, share, comment on, receive, and otherwise distribute information, whether through closed or open groups.

Overview

The remainder of this report unfolds as follows. Chapter Two describes China's overall approach to social media, with an emphasis on its messaging strategy and tactics. In Chapter Three, we examine how China applies this theoretical approach to social media in practice, focusing on types of campaigns, key targets, and key enablers. In Chapter Four, we explore our main case study, Taiwan, and document more than ten examples of suspected Chinese disinformation on Taiwan social media. Chapter Five expands the aperture to the wider region, with specific looks at Singapore, the Philippines, and Japan for whether they are experiencing similar Chinese disinformation and how they might be responding. Chapter Six relays our main findings, recommendations, and trends to watch in the future. The appendix presents some considerations on the Chinese government's own concerns about social media as a vulnerability and whether targeting China through this means represents a viable operational approach for USAF.

Chinese Social Media–Based Disinformation Operations in Theory

China’s approach to social media is largely an extension of its long-standing propaganda and psychological warfare strategy into a new medium. Since its founding, the CCP has understood the power of using information to manipulate both domestic and foreign audiences. Each new way to communicate with audiences—television, the internet, and now social media—has led to more continuity than change in the CCP’s overarching information strategy, with minor updates and improvements as necessary. The Chinese military views information as the key enabler for success in a future conflict, and because the PLA is one of the main actors likely to use hostile disinformation in a contingency, this chapter summarizes PLA writings on strategies for social media operations.

Chinese Approaches to Information Operations

The Chinese Party-state and the military view information as the single most critical domain for success in contemporary and especially next-generation warfare. The PLA uses a variety of terms that align, to at least some degree, with Western conceptions of influence operations. Traditionally, the PLA has talked about using *political work* [政治工作] and *external propaganda* [对外宣传] to communicate Chinese messages to foreign audiences and undermine enemy forces.¹

¹ Mark Stokes and Russell Hsiao, “The People’s Liberation Army General Political Department: Political Warfare with Chinese Characteristics,” Project 2049 Institute, October 14,

Following the 2003 U.S. invasion of Iraq, the PLA adopted a framework of the *three warfares* [三战], which comprise *psychological warfare* [心理战], *public opinion warfare* [舆论战], and *legal warfare* [法律战], as a way to conceptualize different vectors for influence.² Most recently, the PLA has developed an emerging concept called *cognitive domain operations* [认知域作战] that represents next-generation psychological warfare hardware and tactics focused on affecting an adversary's cognitive abilities.³ Fundamentally, as the armed wing of the CCP in an era of *informatized operations* [信息化作战], the PLA is in the business of using information to influence foreign perceptions and behaviors against a variety of foreign entities, such as enemy military and political forces and neutral or allied third parties.

China's national military guidelines, which are the equivalent of its military doctrine and reflected in its 2015 defense white paper, focus on the need to prepare to fight "informationized local wars [信息化局部战争]."⁴ This central focus on information in warfare dates to China's observations of the U.S. way of war since the Gulf War in the early 1990s. The U.S. military's rapid defeat of a Soviet-style Iraqi military that had much of the same organization and command structure as the PLA shocked the Chinese leadership into abandoning its Maoist strategy of "people's war" in favor of preparing for "local wars under high-tech conditions."⁵ Subsequent updates to

2013; Wang Juntao and Anne-Marie Brady, "Sword and Pen: The Propaganda System of the People's Liberation Army," in Anne-Marie Brady, ed., *China's Thought Management*, London: Routledge, 2011.

² Dean Cheng, "Chinese Lessons from the Gulf Wars," in Andrew Scobell, David Lai, and Roy Kamphausen, eds., *Chinese Lessons from Other Peoples' Wars*, Carlisle, Pa.: U.S. Army War College Strategic Studies Institute, 2011; Elsa Kania, "The PLA's Latest Strategic Thinking on the Three Warfares," *China Brief*, Vol. 16, No. 13, August 22, 2016; Peter Mattis, "China's 'Three Warfares' in Perspective," *War on the Rocks*, January 30, 2018.

³ Nathan Beauchamp-Mustafaga, "Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations," *China Brief*, Vol. 19, No. 16, September 6, 2019.

⁴ State Council Information Office of the People's Republic of China, *China's Military Strategy*, May 27, 2015.

⁵ Fravel, 2019; Andrew Scobell, David Lai, and Roy Kamphausen, eds., *Chinese Lessons from Other Peoples' Wars*, Carlisle, Pa.: Strategic Studies Institute, 2011.

this strategy have been made by each generation of leadership, with then-leader Hu Jintao changing it in 2004 to “local wars under the conditions of informationization” and now Xi’s “informationized local wars.”⁶ The PLA’s focus of modernization has been on “informationized” (network) warfare, for which Xi has set 2035 as a deadline, but the military is now transitioning to “intelligentized” (artificial intelligence–enabled) warfare.⁷ In short, the PLA has focused on informationized warfare for most of the past three decades.

No PLA Doctrine for Social Media

For the PLA specifically, and the Party-state more broadly, social media is an element of its information warfare strategy—though it is unclear how well it has been or will be integrated into actual military operations. PLA authors generally describe social media as a dream-come-true platform for next-generation messaging with content tailored for specific audiences, but there are few indications so far that the PLA has conclusively determined the role of social media in its military strategy. Many questions remained unanswered (likely for both the PLA and its potential adversaries), and it is quite possible that the true extent of the PLA’s social media capabilities will only become clear when fully employed for a crisis or wartime.

Within informationized warfare, social media falls most often under psychological warfare. According to a recent RAND report, the PLA approaches modern armed conflict as systems confrontation and system-destruction warfare, seeing operations in a system-of-systems framework, with each mission and unit nested in a hierarchy of operational systems.⁸ Information warfare is framed as the “information-confrontation system,” with information attack and information

⁶ M. Taylor Fravel, “China’s New Military Strategy: ‘Winning Informationized Local Wars,’” *China Brief*, Vol. 15, No. 13, July 2, 2015.

⁷ Elsa Kania, “AlphaGo and Beyond: The Chinese Military Looks to Future ‘Intelligentized’ Warfare,” *Lawfare*, June 5, 2017.

⁸ For more on the PLA’s systems confrontation approach to warfare, see Engstrom, 2018.

defense as the two key elements that the PLA must master.⁹ *Information attack* comprises the psychological categories of propaganda inducement, deterrent, influence, and deception. These can be translated into a Western context as “undermining enemy morale, confusing enemy decisionmakers, convincing countries not to fight, and using disinformation to degrade enemy decisionmaking.”¹⁰ Another framework for information warfare is the PLA’s three warfares,¹¹ which, in a sense, is more about tools while the information-confrontation system is more about missions and tasks. Still, both frameworks center on using multiple types of information, broadly defined, to accomplish a variety of objectives, and both frameworks treat information as a critical part of the PLA’s warfighting strategy.

Although the PLA’s approach to offensive uses of social media is adopted from psychological warfare, the PLA has no official doctrine on social media. Social media [社交媒体], or *social networks* [社交网络], are not referenced in any of the PLA’s most-authoritative texts on military strategy, but the military is clearly both interested in the possibilities that social media presents and concerned about the threat posed by social media to PLA operations—and, more broadly, to CCP rule. The rise of social media in the early 2000s and its rapid worldwide proliferation in the 2010s came too late to be included in such classic texts as the 2006 *Science of Campaigns* or even the 2013 *Science of Military Strategy*, published by the Academy of Military Science.¹² Chinese defense white papers in 2013, 2015, and even 2019 did not mention it, either. The only reference in core PLA texts is in the 2015 version of *Science of Military Strategy*, published by the National Defense Univer-

⁹ For a discussion about the similar Russian concept, see Elina Treyger, Joe Cheravitch, and Raphael S. Cohen, *Russian Disinformation Efforts on Social Media*, Santa Monica, Calif: RAND Corporation, RR-4373/2-AF, forthcoming.

¹⁰ Beauchamp-Mustafaga and Chase, 2019.

¹¹ For an overview of the three warfares, see Mattis, 2018.

¹² People’s Liberation Army Academy of Military Science Military Strategy Department, *Science of Military Strategy* [战略学], 3rd ed., Beijing, China: Academy of Military Science Press, 2013; Zhang Yuliang [张玉良], ed., *The Science of Campaigns* [战役学], Beijing, China: National Defense University Press [国防大学出版社], 2006.

sity.¹³ It is unclear why the PLA has not written more texts explicitly about social media, though some prominent writings on the overall media landscape do address it.¹⁴

This illustrates that the broader PLA was slow to adopt social media as a tool for psychological warfare, though some researchers saw early promise. A May 2011 journal article touted the “potential” of Facebook and Twitter for use in offensive psychological warfare, such as leveraging user data from platforms for enhanced message targeting, using opinion leaders to artificially influence public discussion, and conducting subliminal messaging.¹⁵ Yet PLA authors overall only increased their attention to social media around 2014 and again in 2016, as is made evident in Figure 2.1. This is likely because the Chinese military was initially focused on developing defensive approaches domestically, and there was no immediate requirement for employment because Taiwan under Ma Ying-Jeou in 2008–2016 was generally pursuing improved relations with China.

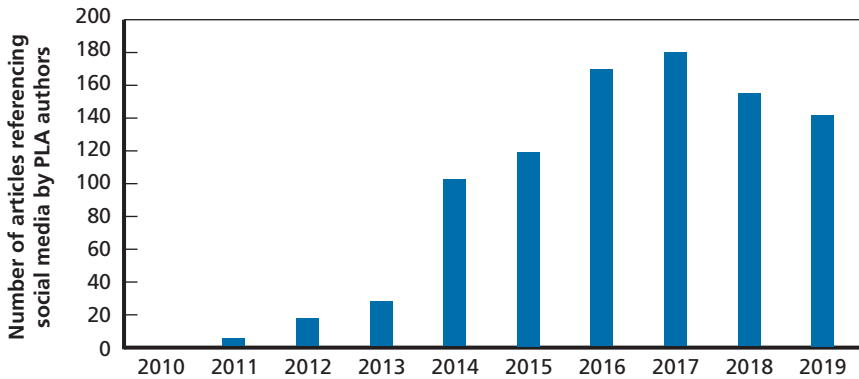
PLA interest in social media clearly grew dramatically from 2010 to 2017 but appears to have plateaued since then. On the surface, PLA attention to social media has declined slightly since a high in 2017, though it is possible our data collection overlooked some of the conversation (because of term selection) or was incomplete (if relevant articles were not part of the databases we accessed for the search). In practice, the PLA has accelerated its use of social media, both for the offen-

¹³ Xiao Tianliang [肖天亮], ed., *Science of Military Strategy* [战略学], Beijing, China: National Defense University Publishing House [北京国防大学出版社], 2015 (translation from Beauchamp-Mustafaga and Chase, 2019). The National Defense University version of *Science of Military Strategy* is generally considered slightly less authoritative than the 2013 Academy of Military Science version.

¹⁴ Zeng Huafeng [曾华峰] and Shi Haiming [石海明], *Mind Control: The Rules of War and National Security Strategy in the Era of Global Media* [制脑权：全球媒体时代的战争法则与国家安全战略], Beijing, China: People’s Liberation Army Publishing House [解放军出版社], 2014. Some PLA texts on *military propaganda* [军事宣传] do refer to *new media* [新媒体], a category that appears to include social media and other platforms; such discussions, however, have yet to reveal much about PLA doctrine for disinformation on social media.

¹⁵ Wu Yinsheng [吴银胜] and Mei Jianbing [梅建兵], “Some Inspirations Drawn from the Application of the Booming Social Media in Psychological Warfare [社交媒体的迅猛发展及心理战运用的几点启示],” *Defense Science and Technology* [国防科技], May 2011.

Figure 2.1
Progression of Chinese Military Attention to Social Media



SOURCE: Data from China National Knowledge Infrastructure database, (in Chinese), undated.

NOTE: We define PLA authors as those with affiliations that include the words *military* [军], *national defense* [国防], *unit* [部队], *theater command* [战区], *Xi'an Politics Institute* [西安政治学院], or *Nanjing Politics Institute* [南京政治学院].

sive applications of social media disinformation outlined in this report and simply for overt propaganda—all the services (except the PLASSF) had their own Weibo accounts by mid-2019. One explanation for the steady or even declining PLA writings on social media might be that the PLA believes it has caught up on the learning curve and is transitioning to a more operational focus.

PLA Messaging Strategy of Content Tailoring and Audience Targeting

The Chinese military frames its social media strategy as a nuanced, multipronged approach, but it is unclear how far beyond theoretical writings it has actually gone toward realizing its proposed approach and strategy. As a relatively new phenomenon, the PLA appears to still be developing its approach to social media, especially in wartime. So far, the PLA has largely treated social media as an extension of its traditional approach to psychological warfare. It has demonstrated some

willingness to use social media but so far has shown little if any innovation compared with other militaries. Instead, the PLA has drawn most of its specific insights on social media from how the United States, Russia, and others have employed social media in peacetime and in various conflicts, such as with Libya, Syria, and Ukraine.¹⁶ Despite reports that China has deployed disinformation operations against Taiwan, there are few authoritative Chinese writings to analyze that give insight into how China would actually leverage disinformation in a conflict.¹⁷ Therefore, we are largely forced to extrapolate from the available writings and interviews conducted in Taiwan about how the PLA considers social media disinformation campaigns as part of its broader strategy.

In practice, social media will serve two interrelated purposes: overt messaging and covert manipulation. The vast majority of publicly available Chinese military writings on social media are written by propaganda experts and thus focus on overt messaging rather than on such covert manipulation as disinformation and deniable accounts. Nevertheless, there are some available writings on deniable psychological operations in wartime.

Messaging Strategies

For overt messaging, PLA propagandists discuss three general strategies for influencing audiences: rapid response, agenda-setting, and adaptive narratives.¹⁸

- First, the PLA, and the Chinese government more broadly, understands that public opinion is heavily influenced by first impres-

¹⁶ Chen Hanghui [陈航辉], Fang Peng [芳鹏], Yang Lei [杨磊] and Xia Yuren [夏育仁], “Social Media Warfare: A New Dimension to Warfare in the Information Age [社交媒体战: 信息时代战争新维度],” *PLA Daily* [解放军报], September 25, 2015; Zhu Ningning [朱宁宁], “An Analysis of Russia’s Unfolding of Media Warfare Tactics amid the Turbulent Political Situation in Ukraine [乌克兰政局动荡中俄对乌舆论战谋略运用探析],” *Military Correspondent* [军事记者], May 2014.

¹⁷ For a review of some PLA articles that do openly acknowledge the use of disinformation, including for wartime, see Beauchamp-Mustafaga, 2019.

¹⁸ This section draws from Beauchamp-Mustafaga and Chase, 2019.

sions, so it is important for the PLA to quickly react to sudden events before public opinion hardens.¹⁹

- Second, in the absence of sudden events, the PLA seeks to shape audiences' perceptions by constantly focusing the narrative on specific issues favorable to the PLA, echoing a tactic hailed by President Xi Jinping in 2016.²⁰ This strategy appears to be heavily influenced by foreign research, and some writings even explicitly discuss subconscious messaging.²¹
- Third, the PLA realizes that sometimes its original messaging content will not sufficiently influence its intended audience, and

¹⁹ For examples of PLA responses to international events, see Jiang Tingting [姜婷婷], "Thoughts on Transmitting International Public Opinion with Regard to Discussions of the South China Sea [关于南海议题国际舆论传播的思考]," *Military Correspondent* [军事记者], December 2017; Pu Duanhua [濮端华], "An Analysis of China's Public Opinion Strategy in the Diaoyu Islands Dispute [钓鱼岛争端中的我舆论斗争策略探析]," *Military Correspondent* [军事记者], October 2012; Rui Han [芮晗], "An Analysis of Our Countermeasures Against the US Authorities' Indictment of Chinese Military Officers [美起诉我军官 '网络窃密' 的舆情应对策略探析]," *Military Correspondent* [军事记者], August 2014; Sun Wenjing [孙文静] and Wang Lin [王林], "The Scarborough Shoal Incident in the Eyes of Foreign Media and Revelations for Our Propaganda Abroad [外媒眼中的黄岩岛事件及对我外宣之启示]," *Military Correspondent* [军事记者], October 2012; and Yu Chunguang [于春光], "Enhance Public Opinion Guidance Capability for International Hotspot Events [提升国际热点事件舆论引导能力]," *Military Correspondent* [军事记者], July 2012.

²⁰ "CCP Central Politburo Holds 35 Collective Study [Session] [中共中央政治局进行第三十五次集体学习]," Xinhua, September 28, 2018. For PLA writings on agenda setting, see Jin Sicong [金思聪], "Characteristics and Public Sentiment Guidance for International Social Media Relating to Chinese Military Agenda Setting: Framework Analysis of Twitter Reporting During the China-U.S. UUV Incident [国际社交媒体涉华军事议题的特点与舆情引导: 中美无人潜航器事件推特报道的框架分析]," *Military Correspondent* [军事记者], August 2018; Liu Yi [刘轶], "Do Agenda Setting Well, Seize International Communication Right to Speak [搞好议题设置, 争取国际传播话语权]," *Military Correspondent* [军事记者], September 2018; and Xiao Fei [肖飞], "An Initial Exploration on Strategies for Guiding Public Opinion About New High-Tech Weapons and Equipment: Taking Reports About J-15 Shipborne Aircraft as an Example [高新技术武器装备的舆论引导对策初探: 以歼-15舰载机报道为例]," *Military Correspondent* [军事记者], May 2013.

²¹ For early Western research, see Maxwell E. McCombs and Donald L. Shaw, "The Agenda-Setting Function of Mass Media, *Public Opinion Quarterly*, Vol. 36, No. 2, Summer 1972.

PLA authors have called for iterative adaptation to make more-persuasive arguments over time.²²

Social media has the potential to dramatically enhance the effectiveness of all these strategies. Social media also allows for even quicker responses through the immediate dissemination of information, compared with waiting until the next day for a newspaper or even until the next hour for television news, and it allows for more immersive agenda-setting by inundating audiences with content. Furthermore, data analytics can help the PLA improve its messaging feedback loop for better content by revealing the content that audiences engage with, compared with traditional media, which has no direct feedback mechanism from the consumer (audience) to the producer (propagandists).

Some messaging themes are also worth noting from China's general propaganda narrative. Reading Chinese government reports and state-run media, China is portrayed as a peace-loving nation with no expansionist ambitions and a purely defensive military strategy. Much of China's overall messaging in a war—especially to U.S. allies and partners and to neutral countries—likely will include such themes. Yet another prominent theme is the inevitability of China's rise along with its geographic centrality and geopolitical dominance of the region—anyone who crosses China will surely lose, and Chinese victory is inevitable. This narrative could also be targeted at U.S. service members as a way to weaken their resolve.

Two special target audiences for China merit mention. First, the Chinese government often aims its disinformation operations and propaganda at the ethnic Chinese diaspora, and this approach likely extends to social media as well.²³ We assess that any disinformation by China would target ethnic Chinese first because (1) those who speak Chinese are easier for the PRC to reach via Chinese-language social

²² Xiao Fei [肖飞], "Analysis on the Countermeasures to Strengthen the Construction of Our Military's New Media Power [加强我军新媒体力量建设的对策探析]," *Military Correspondent* [军事记者], January 2017.

²³ Timothy Heath, "Beijing's Influence Operations Target Chinese Diaspora," *War on the Rocks*, March 1, 2018.

media and (2) Chinese propagandists appear to believe that ethnic Chinese abroad are more likely than other audiences to be receptive to CCP messaging.

Second, Chinese government and military writings pay special attention to the value of influencing foreign youth audiences because the worldviews of this group appear to be more malleable.²⁴ With younger populations around the world generally using social media at higher rates than older populations, the forum presents an attractive vector for China to fine-tune this messaging strategy.

Tactics

For covert manipulation, PLA writings suggest an interest in discrediting the enemy's leadership, undermining enemy morale, and influencing enemy public opinion. (These themes are discussed further in Chapter Five.)²⁵ One tactic drawn from U.S. information operations against Saddam Hussein and Muammar Gaddafi is "public opinion

²⁴ For nonmilitary writings on targeting youths, including those overseas, see Cai Yintong [蔡印同], "Promoting Communication in Life: Talking About How to Use Foreign Students to Communicate Abroad [在生活中促进交流: 谈如何利用外国留学生开展对外传播]," *International Communications* [国际传播], March 2011; Cai Yintong [蔡印同], "Study Abroad Students: An Important Force for People-to-People External Propaganda [留学生: 民间外宣的重要力量]," *International Communications* [国际传播], March 2009; Hu Xiao [胡晓], "Research on the Influence of Network Propaganda on the Observing Behavior of Young Audiences [网络宣传对青年受众观影行为的影响研究]," *Radio & TV Journal* [视听], July 2016; Liu Xiao [刘肖], "International Communication: Analysis of the Path of Evaluation Indicator Construction and Communication Effectiveness Improvement [国际传播力: 评估指标构建与传播效力提升路径分析]," *Jianghuai Tribune* [江淮论坛], April 2017; and Wu Xiujuan [吴秀娟], Wu Wei [吴瑛], Zhan Yating [詹雅婷], and Xu Bowen [徐博文], "Communication and Awareness of the Concept of Community for Common Destiny in the Post-Soviet Space [人类命运共同体理念在后苏联空间的传播与认同]," *International Communications* [国际传播], March 2018. For an article by PLA authors, see Wang Linyao [王锦尧] and Li Jiaxin [李嘉鑫], "Cultivation of New Media Audience in Military Culture Communication [军事文化传播中新媒体受众的培养]," *Military Correspondent* [军事记者], February 2016. For a domestic focus on younger audiences, see William Zheng, "How Official Chinese Propaganda Is Adapting to the Social Media Age as Disaffection Spreads Among Millennials," *South China Morning Post*, February 10, 2019.

²⁵ For a broader discussion of Chinese psychological warfare tactics, see Ye Zheng [叶征], *Lectures on the Science of Information Operations* [信息作战学教程], Beijing, China: Academy of Military Science Press [军事科学出版社], 2013.

decapitation [舆论斩首].”²⁶ This calls for “demonizing the leader of the enemy side” as a way to “[cripple] the enemy leader’s command authority and weaken his command and control ability.”²⁷ PLA authors have similarly mentioned the United States’ use of targeted messages to senior Iraqi military officers as a way to “undermine the morale of the enemy’s military forces and civilian populace, so as to deliver a ‘soft kill’ that forces surrender.”²⁸ Lastly, some Chinese military authors have touted the impact of “creating information chaos” and “exaggerating the conflict of interests within the enemy camp.”²⁹ This echoes claims that China’s interference in Taiwan’s 2018 elections was carried out by “cyberwarfare specialists familiar with social issues in Taiwan [who injected] divisive commentary into discussions on controversial topics in an attempt to create social strife.”³⁰

PLA authors also note the importance of “spreading all kinds of rumors and information.”³¹ The PLASSF has also been accused of social media manipulation in Taiwan’s November 2018 elections, and, even before the elections, National Security Bureau Director-General Peng Sheng-Chu said publicly that, “Beijing and the PLA were behind a propaganda campaign to interfere with the nation’s democratic elections by creating disinformation and fake news targeting Taiwan media outlets, radio and television programs, and Web sites.”³² Specifically tying

²⁶ Sheng Peilin [盛沛林] and Li Xue [李雪], “On ‘Public Opinion Decapitation’ [论 ‘舆论斩首’],” *Journal of the PLA Nanjing Institute of Politics*, May 2006; Wu Rui [吴瑞], “Be On Guard Against Other Kinds of Soft Warfare” [“警惕另类软战争”], *Military Correspondent* [军事记者], November 2013.

²⁷ Sheng Peilin [盛沛林] and Li Xue [李雪], 2006.

²⁸ Sheng Peilin [盛沛林] and Li Xue [李雪], 2006; Chen Zhengzhong [陈正中], “Preliminary Thoughts About Strengthening Cyber News Media in Wartime [加强战时网络新闻舆论管控刍议],” *Military Correspondent* [军事记者], July 2014.

²⁹ Wu Rui [吴瑞], “Be On Guard Against Other Kinds of Soft Warfare [警惕另类软战争],” *Military Correspondent* [军事记者], November 2013.

³⁰ Chung Li-hua and William Hetherington, “China Targets Polls with Fake Accounts,” *Taipei Times*, November 5, 2018.

³¹ Wu Rui [吴瑞], 2013.

³² Chung Li-hua and Hetherington, 2018. Also see Chris Horton, “Specter of Meddling by Beijing Looms over Taiwan’s Elections,” *New York Times*, November 22, 2018. For more

this activity to social media, then-Premier William Lai said China was engaging in the “dissemination of disinformation through mass media and social media.”³³

Another way to manipulate enemy public opinion is through *astroturfing*, or manipulating public opinion by masking the sponsor or originator of a message to make it appear as if it emerges from a segment of society. The PLA has paid very close attention to U.S. military efforts to conduct astroturfing against the Islamic State (ISIS) and could adopt this tactic itself.³⁴ Indeed, Taiwan researchers have accused the PLA of doing just this.³⁵ One recent report found a 2017 article by a student at the PLA’s Nanjing Political Institute that could be considered a guidebook for mainland speakers to appear like local users on PTT, Taiwan’s most important social media platform for political discussions.³⁶ One critical question is the PLA’s ability to create convincing foreign-language content, especially disinformation. This would require advanced language skills, which some in the PLA certainly possess (see Chapter Four). China, on the whole, has demonstrated at least some ability to conduct foreign-language disinformation, evident in Twitter and Facebook’s disclosures of English-language posts on their platforms targeting the Hong Kong protests that they attributed to the Chinese government, some of which are alleged to have been posted by

recent comments by President Tsai on China’s overall pressure, see Yimou Lee, “Taiwan Says China Has Stepped Up Infiltration Efforts,” Reuters, May 9, 2019b.

³³ Jason Pan, “China Subverting Elections: Premier,” *Taipei Times*, November 2, 2018.

³⁴ Chen Qingbao [陈庆宝], “Analysis and Countermeasure Research on the US ‘Online Astroturf Army’ [对美国‘网络水军’的分析及对策研究],” *Military Correspondent* [军事记者], November 2016. For the likely origin story, see Nick Fielding and Ian Cobain, “Revealed: US Spy Operation That Manipulates Social Media,” *The Guardian*, March 17, 2011.

³⁵ Li Ruobing [李若冰], “China’s Astroturf and Cyber Army Train Mind Superiority with 2020 Elections as Target [中國水軍、網軍九合一練兵「制腦權」, 目標2020大選],” *Storm*, November 23, 2018.

³⁶ Lai Dongwei [赖东威], “An Analysis of the Sentence Patterns and the Use of Vocabulary in Taiwanese Social Media [台湾社交媒体中的闽南语句式 and 词汇使用现象探析],” *Journal of News Research* [新闻研究导刊], 2017, cited in Beauchamp-Mustafaga and Chase, 2019.

large-scale automated accounts, or bots.³⁷ Although the specific Chinese actor (or actors) behind the attacks on the Hong Kong protesters remains unidentified, the PLA is clearly interested in running bot networks, as evidenced by a June 2019 article by researchers affiliated with Base 311, the PLASSF’s lead psychological warfare unit.³⁸

Chinese military authors also identify the value of disguising Chinese messaging through the authentic voice of third parties, especially well-known figures who intentionally or unintentionally reflect and amplify CCP narratives to new and larger audiences.³⁹ This means that overt state-run media can retweet celebrities who promote CCP rhetoric, or covertly can either amplify this message or even hack their accounts to capture their followers.

Additionally, China might outsource its social media messaging and disinformation efforts to patriotic netizens (internet users). Although the CCP generally seeks tight control over domestic social media discussion and prohibits Chinese citizens from using foreign social media, it has also found that there are benefits to those who *climb the wall*, [翻墙] or employ virtual private networks to circumvent censorship and access foreign social media.⁴⁰ In January 2016, when

³⁷ For one analysis of the disclosures that includes some foreign-language content, see John Dotson, “Chinese Covert Social Media Propaganda and Disinformation Related to Hong Kong,” webpage, Jamestown Foundation, September 6, 2019; on China’s use of trolls on Twitter to attack Hong Kong protesters, see Raymond Zhong, Steven Lee Myers, and Jin Wu, “How China Unleashed Twitter Trolls to Discredit Hong Kong’s Protesters,” *New York Times*, September 18, 2019. Nick Monaco has also evaluated China’s likely use of bots; see Nicholas J. Monaco, “Beijing’s Computational Propaganda Goes Global: The Significance of China’s Debut as a Disinformation Actor,” Digital Intelligence Lab via Medium, September 12, 2019a; and Nicholas J. Monaco, “Welcome to the Party: A Data Analysis of Chinese Information Operations,” Digital Intelligence Lab via Medium, September 18, 2019b.

³⁸ Li Bicheng [李弼程], Hu Huaping [胡华平], and Xiong Ya [熊尧], “Intelligent Agent Model for Online Public Opinion Guidance [网络舆情引导智能代理模型],” *National Defense Science & Technology* [国防科技], No. 3, June 2019.

³⁹ Yu Chunguang [于春光], 2012.

⁴⁰ The Chinese government blocks many foreign social media platforms and has used physical policing to stop some Chinese citizens who use them anyway through virtual private networks. See Gary Shih, “Chinese Censors Go Old School to Clamp Down on Twitter: A Knock on the Door,” *Washington Post*, January 4, 2019.

Tsai Ing-Wen was elected president of Taiwan, thousands of users in China accessed Facebook, nominally banned by China's own censorship technology (known colloquially as the Great Firewall), and posted critical comments on Tsai's Facebook page.⁴¹ This campaign, referred to as a "Diba Expedition [帝吧出征]" was mentioned in at least four articles by Chinese authors, with some praising the campaign as a modern version of the "people's war" and grassroots assistance to "online ideological struggle."⁴² Western researchers found the campaign was human-conducted, and Chinese articles treated it as an organic movement (i.e., not one initiated or coordinated by the Chinese government), though one article did note it was "tacitly approved" by the state and suggested that this type of activity will be "normalized" over time.⁴³

China could also manipulate foreign social media's self-policing function. PLA texts suggest that Chinese military analysts have learned from Israel's consideration of domestic legislation to force Western social media to censor foreign content for them.⁴⁴ Ahead of the 30th

⁴¹ Marco Huang, "Chinese Netizens Flood Tsai Ing-Wen's Facebook Page with Anti-Taiwan Independence Posts," *Wall Street Journal*, January 21, 2016; Nicholas J. Monaco, "Computational Propaganda in Taiwan: Where Digital Democracy Meets Automated Autocracy," Computational Propaganda Research Project, working paper, June 2017.

⁴² For an article referencing patriotism of the post-1990s generation and the "people's war," see Liu Weichao [刘伟超] and Zhou Jun [周军], "New Ideas to Improve Our Army's Network Public Opinion Capability [新理念提升我军网络舆论引导能力]," *New Media* [网络传播] July 2018. For an article framing "expeditions" as an ideological struggle, see Li Yuanyuan [李媛媛], "Fight Against Attacks in the Online Ideology Battle [打好网络意识形态斗争进攻仗]," *Political Workers* [政工导刊], April 2017. For an article concerned about greater expectation, see Su Juan [苏娟], "Analysis on the Characteristics of the Spread of Military-Related Public Opinion on the Internet [网络涉军舆情传播特点探析]," *Military Correspondent* [军事记者], March 2017.

⁴³ Lou Sijia [娄思佳], "On Military Broadcasting to Taiwan: Strategies for Leveraging Non-Native Social Media [论对台军事广播: 借力非本土社交媒体的策略]," *China Broadcasts* [中国广播], August 2017. The *People's Daily* WeChat account gave a positive review of the campaign, clearly reflecting this tacit approval, even if after the fact. See "People's Daily Comments on Emperor's Expedition on FB: Post-90s [Generation], We Believe in You! [人民日报评帝吧出征FB: 90后, 相信你们!]," Sina.com, January 22, 2016.

⁴⁴ Wu Yanlin [吴艳林], "Process and Characteristics of the Development of Israel's Online Public Opinion Offense and Defense [以色列网络舆论攻防的发展历程及特点]," *Military*

anniversary of Tiananmen in June 2019, reports emerged that Twitter had suspended anti-China accounts, leading some to suspect they had been reported by the Chinese government. However, Twitter denied this and argued it was part of “routine action” to eliminate “platform manipulation.”⁴⁵ This is yet another approach that China could implement as a way to alter the information environment on foreign social media in China’s favor, and it could be done on platforms where China does not actually have direct control for censorship.

The PLA also understands the importance of tailoring messages to targeted audiences, especially in wartime. For example, the 2013 edition of *Science of Military Strategy* argued that “new media,” specifically internet-based platforms, could help seek “the sympathy and support of international society” in wartime under the three warfares concept.⁴⁶ One report found that propagandists had discussed various target audiences, including “a matrix approach to targeting, breaking into four groups: one’s own people, one’s allies, the enemy’s people, and neutral countries; and three levels: leadership, troops, and the common people,” and various ways to tailor their messaging, such as those “based on people’s beliefs, value systems, or inclinations in order to influence people from different countries, political parties, or cultural groups.”⁴⁷ Social media can play a key role in improving this targeting and is used by younger audiences around the world. (For more on targeting in the case of Taiwan, see Chapter Three.)

Correspondent [军事记者], October 2018. For analysis of the proposed legislation, see Tehilla Shwartz Altshuler and Rachel Aridor-Hershkovitz, “Israel’s Proposed ‘Facebook Bill,’” *Lawfare*, August 6, 2018.

⁴⁵ Andrew Galbraith, “Twitter Apologizes for Blocked China Accounts Ahead of Tiananmen Anniversary,” Reuters, June 2, 2019.

⁴⁶ People’s Liberation Army Academy of Military Science Military Strategy Department, 2013, p. 131.

⁴⁷ Liao Yiwen [廖毅文], “Measures for Guiding Public Opinion on the Internet When Major Surprise Incidents Occur [重大突发事件的互联网舆论引导对策],” *Military Correspondent* [军事记者], June 2011, pp. 20–21; Dong Tao [董涛], “Advancing International Communications for Military News [Toward] Differentiated Audiences [推进军事新闻分众化的国际传播],” *Military Correspondent* [军事记者], September 2018, quoted in Beauchamp-Mustafaga and Chase, 2019.

Judging solely from its publicly available writings, the PLA's interest in social media appears to focus much more on open and public platforms, such as Facebook and Twitter, than on closed platforms, such as WhatsApp.⁴⁸ There are both benefits and downsides for the PLA to use closed platforms. One benefit is that Chinese-injected disinformation is more difficult for Taiwan or others to track and counteract; furthermore, because users are more likely to know each other, the disinformation might be trusted more than it would if it came from an unknown public account. The downside is that the same lack of public analytic data that makes it difficult for Taiwan authorities to track disinformation also makes it difficult for the PLA to assess that disinformation's effectiveness. Additionally, the closed or private nature of the platforms limit the speed and extent of the spread of information on such platforms. One public post on Facebook can be seen by everyone; a WhatsApp message has to be forwarded within groups (though some groups can be quite large). Limited PLA writings on closed platforms perhaps should be expected—public discussion by the PLA mostly focuses on overt propaganda and not covert manipulation. However, Taiwan media accounts suggest that part of the PLA's political interference in the November 2018 election occurred on LINE. If this is correct, that could mean that available information about PLA thinking reflects only a portion of the Chinese military's overall strategy for social media campaigns.⁴⁹

An August 2017 article by a propagandist at China Central Radio's military propaganda center suggests that Chinese analysts are well aware of the differential value of the various types of platforms they can operate across. The article's author argues that Facebook was good for wide-scale interactions while LINE was good for instant mes-

⁴⁸ For an early implicit reference to this, see Miao Jian [苗健], "With the Help of Overseas Open Internet Information Platform: Seeking Equal Right to Speak [借助海外开放式互联网信息平台: 谋求对等话语权]," *Southeastern Communication* [东南传播], August 2014, pp. 7–9.

⁴⁹ Chung Li-hua and Hetherington, 2018; Keoni Everington, "China's 'Troll Factory' Targeting Taiwan with Disinformation Prior to Election," *Taiwan News*, November 5, 2018b.

saging and rapid, more-targeted communications.⁵⁰ An October 2014 article by a *PLA Daily* [解放军报] editor references LINE as an instant messaging platform with a curated “friend circle,” but this appears to be in the context of work colleagues for improved editorial efficiency.⁵¹ A February 2015 article in *Military Correspondent* mentions LINE and WhatsApp as popular social media platforms in Southeast Asia, along with Twitter, Facebook, and WeChat.⁵² Yet this article does not remark on the differences between these types of platforms or whether a different messaging approach is necessary to reach audiences on closed platforms. Moreover, it was written by a *People’s Daily* correspondent based in Thailand, which reveals civilian state-run media support for PLA propaganda but does not shed light on the PLA’s understanding of LINE. Similarly, a researcher at the Nanjing Political Institute,⁵³ in a May 2016 article, noted that ISIS usually posts on Twitter but “when necessary switches to encrypted communication applications such as SnapChat and WhatsApp.”⁵⁴

⁵⁰ Lou Sijia [娄思佳], 2017.

⁵¹ Luo Ji [罗辑], “Using Instant Messaging Tools to Build a Full Media Editing Platform [运用即时通信工具构建全媒体编务平台初探],” *Military Correspondent* [军事记者], October 2014.

⁵² Sun Guangyong [孙广勇], “New Media: The Double Edged Sword in a Changing South-east Asian Society [新媒体: 东南亚社会转型的双刃剑],” *Military Correspondent* [军事记者], February 2015.

⁵³ The PLA has two main research institutions for propaganda, political warfare, and psychological warfare. According to Kamphausen, the Nanjing Political Institute and Xi’an Political Institute (placed under the National Defense University in the PLA reorganization) are responsible for “[training] political commissars at the initial entry and intermediate levels.” He further argues that “it is informally understood that the Nanjing academy specializes in liaison work and Xi’an emphasizes legal/judicial preparations.” The National University of Defense Technology also conducts more operationally and technically focused research on psychological warfare, and the Information Engineering University, under the PLASSF, conducts some research on social media. See Roy Kamphausen, “The General Political Department,” in Kevin Pollpeter and Kenneth W. Allen, eds., *The PLA as Organization v2.0*, Dunn Loring, Va.: Defense Group Inc., 2015.

⁵⁴ Zhou Yang [周洋], “Analysis of ISIS’ Social Media Organization Structure and Public Opinion Strategy [ISIS 社交媒体组织架构与舆论策略解析],” *Military Correspondent* [军事记者], May 2016.

In contrast with Russia, up until the outbreak of COVID-19, China does not appear to have regularly employed bots as a core component of its approach to social media manipulation. Indeed, one 2017 report found that the vast majority of Chinese-language bots on Twitter were actually run by activists critical of the Chinese government, though this was during the relatively early days of Chinese hostile activity on social media.⁵⁵ Although the two public examples of specific accounts attributed to the Chinese government include the use of multiple fake accounts to spread similar messages, the scale—in the low hundreds—is nothing like that of Russia. However, Taiwan government statements paint the picture of large-scale messaging, which could have been accomplished with either massive human resources (certainly possible in China) or bot accounts.⁵⁶ Furthermore, at least two PLA articles have noted the benefits of bots on social media by Russia and Cambridge Analytica.⁵⁷ Moreover, the 2019 article by members of the PLA’s psychological warfare unit focused on the value of AI for running botnets, suggesting this could tactic could be used more in the future.⁵⁸ With no actual details released from Taiwan, it is impossible to determine the role that bots play in Chinese interference against Taiwan.

Other Uses of Social Media

The PLA also understands the value of social media for wartime targeting. As early as 2012, PLA authors noted that NATO used social media for targeting adversary troops in Libya, concluding that “for NATO,

⁵⁵ Monaco, 2017.

⁵⁶ Everington, 2018b.

⁵⁷ Ma Chao [马超] and Sun Hao [孙皓], “The Characteristics of Russian Public Opinion Propagation: Taking ‘Russia Today’ TV Station as an Example [俄罗斯对外舆论传播的特点:以‘今日俄罗斯’电视台为列],” *Military Correspondent* [军事记者], June 2018; Dong Tao [董涛], 2018.

⁵⁸ Li Bicheng [李弼程], Hu Huaping [胡华平], and Xiong Ya [熊尧], 2019.

the information on Twitter has tactical intelligence value.”⁵⁹ The authors also noted that NATO cannot actually use the intelligence acquired from social media without coordination from other military assets—early warning and reconnaissance aircraft, spies, and satellites are also necessary. PLA researchers have worked on using social media to determine a user’s location, and although that work was focused on domestic Chinese users, the 2015 article explicitly said that the methodology could be translated to foreign social media platforms.⁶⁰

Social media is also a great resource for open-source intelligence collection, evidenced by the PLAAF’s discussion of this vulnerability for the PLA. Remarking on the dangers of lax use of social media, one article in the service’s newspaper said, “in the process of some officers and enlisted men using WeChat, sometimes it can result in an accidental mishap, such as not keeping secrets when chatting, not taking into account the location when being on video, or participating in activities such as soliciting votes online and bargaining.”⁶¹ This is because “WeChat possesses the capability to take photographs, conduct video chats, have real-time dialogue, and [capture] information on geographic positioning.”⁶² Despite this, “Of course, we can neither totally ban the internet and social media for units in spite of the risks and challenges posed to security and stability, nor can we allow unimpeded access.”⁶³

Catfishing, or the use of fake identities designed to lure people into the mistaken belief that they have developed an online relationship (romantic or professional), is another vulnerability that the PLA could turn into an attack vector. A 2015 article in *PLA Daily* [解放军

⁵⁹ Yuan Ke [袁轲], Zhang Haijuan [张海娟], and Liu Zhe [刘哲], “Research on the New Trend of Information and Network Warfare [信息网络战新趋势研究],” *Digital Technology & Application* [数字技术与应用], December 2012.

⁶⁰ Wang Kai [王凯], Yu Wei [余伟], Yang Sha [杨莎], Wu Min [吴敏], Hu Yahui [胡亚慧], and Li Shijun [李石君], “Location Inference Method in Online Social Media with Big Data [种大数据环境下的在线社交媒体位置推断方法],” *Journal of Software* [软件学报], Vol. 26, No. 11, 2015.

⁶¹ Peng Xingdou, “A Look at WeChat Management Through ‘the Boyfriend Who Shelled Chestnuts,’” *Huojianbing Bao*, March 3, 2017.

⁶² Peng Xingdou, 2017.

⁶³ Peng Xingdou, 2017.

报] noted that “social media is increasingly valued by national intelligence agencies and has become an important channel for intelligence personnel to obtain valuable intelligence.”⁶⁴ The article also points out that the United States and Israel have struggled with operational security and quotes DoD personnel as saying that 80 percent of U.S. intelligence is from open-source information, with a growing percentage from social media.⁶⁵ Social media requires “complete personal information, including gender, age, education level, work status, marital status, real photos, and mobile phone numbers,” and

some intelligence experts pointed out that the internal situation of some secret equipment and military facilities can be analyzed only by the work photos of an ordinary soldier in Weibo. Accounts in social media often have clear personal tags, and their published content will also include geographic location and other information, which make social media a “bountiful mine” to obtain intelligence information.⁶⁶

Chinese authors note that “the personal information of users on the information publishing end is becoming clearer and clearer, the audience situation at the receiving end of the information is constantly changing,” and that “the risk of revealing personal information through social networks and even leaking secrets is increasing.”⁶⁷ A second *PLA Daily* [解放军报] article extends its focus beyond the PLA and notes

⁶⁴ Xia Yuren [夏育仁], ‘Beware of the ‘Fisher’ in the ‘Friend Circle’ [警惕 ‘朋友圈’ 中的 ‘钓鱼人’],” *PLA Daily* [解放军报], September 25, 2015.

⁶⁵ This number is unverified but appears to be a recurring number in Chinese and U.S. writings. See David R. Lands, “Publicly Available Information: The Secret to Unclassified Data, Part I,” *Over the Horizon*, April 8, 2019; and “Information of 10,000 U.S. Troops Leaks: Military Network Security Attracts Attention [美国十万军人信息外流 军事网络安全引人关注],” *Sohu*, July 13, 2006.

⁶⁶ Xia Yuren [夏育仁], 2015.

⁶⁷ Xia Yuren [夏育仁], 2015.

that informed civilians can leak classified information, such as details on weapon systems.⁶⁸

Conclusion

Our analysis of writings by Chinese government and military researchers indicates that China's strategy on social media largely resembles its strategy for more-traditional forms of disinformation operations. Beyond overt propaganda, China realizes that its message is unlikely to be well received by many overseas audiences, and thus Chinese researchers have explored a broad variety of tactics to obscure the origins of such messaging—including laundering the message through opinion leaders. This muddying of the information waters is likely only one part of a broader Chinese strategy for manipulating and exploiting the information domain in a conflict. The next several chapters will document and analyze known or suspected Chinese efforts on social media, which align well with the Chinese writings we have discussed in this chapter.

⁶⁸ Liu Xiaodong [刘晓东] and Fan Jingyu [樊净芷], "Be Careful with Posts, Be Wary of Online 'Fishing' [跟帖须谨慎, 警惕网络"钓鱼]," *PLA Daily* [解放军报], November 22, 2015. For a recent *People's Daily* reference, see Qian Yibin [钱一彬] and Zhou Xiaoyuan [周小苑], "Cut Off the Network Fraud Black Industry Chain [斩断网络诈骗黑色产业链钱]," *People's Daily*, July 5, 2018.

Chinese Social Media–Based Information Operations in Practice

Over the past three years, the PLA (particularly the PLASSF and the PLAAF) has increased its attention to social media disinformation campaigns. These campaigns have been used (to a limited extent) to achieve effects in the prekinetic phase of conflict of conveying the impression that an enemy is increasingly isolated, poorly led, and domestically divided, and preparing for an unnecessary conflict it cannot hope to win. The PLA has also taken steps to try to guard against vulnerabilities of its own on social media, use the medium to bolster its own society's morale and trust in its leadership and armed forces, and convey an image of responsibility and strength. Some of these messages are conveyed through attributed accounts; others appear to derive from covert and unattributed (sock puppet) accounts. We assess that, although the PLA might run some of these unattributed accounts, other parts of the Chinese Party-state likely run their own as well.

In addition to Chinese writings on the roles of information and disinformation in peacetime and war, the experience of Taiwan as a target of Chinese disinformation operations since 2016 can provide substantial insights into how the PRC conducts targeting of adversary societies and organizations. This chapter discusses how China is believed to have actually executed disinformation campaigns on social media, the types of campaigns it has executed, and the groups in Taiwan that Beijing has tended to target.

A wide-ranging social media disinformation campaign publicly attributed to Beijing was revealed just as this report was being completed. In August 2019, Twitter, Facebook, and YouTube all publicly

announced they had suspended accounts that were suspected of being part of a coordinated state-run campaign—which the companies attributed to China—that targeted the Hong Kong protests.¹ Most noteworthy for researchers, all three companies released the first specific posts and metadata for the accounts, allowing independent analysis of Chinese social media disinformation on foreign platforms. Some early analysis of the available data has already been conducted; this will be detailed throughout this chapter.²

China's Initial Social Media–Based Operations

The Chinese government's first foreign social media account was created by China Radio International (CRI; now China Plus News) on Twitter in 2009. By 2012, most of China's main state-run media had accounts—notably the publications *China Daily*, *People's Daily*, and *Global Times* and the news agency Xinhua.³ CRI is well known for being a conduit of Chinese influence operations in the information sphere around the world and for covertly owning mainly foreign radio channels, so the fact that it led the way onto Twitter is not surprising.⁴ The move to social media followed a perhaps slow but sustained adoption of foreign communication technologies to bring the Chinese nar-

¹ Nathaniel Gleicher, “Removing Coordinated Inauthentic Behavior From China,” Facebook Newsroom, August 19, 2019; Shane Huntley, “Maintaining the Integrity of Our Platforms,” Google, August 22, 2019; Twitter Safety, “Information Operations Directed at Hong Kong,” Twitter Blog, August 19, 2019.

² Dotson, 2019; Zhong, Myers and Jin Wu, 2019; Tom Uren, Elise Thomas, and Jacob Wallis, “Tweeting Through the Great Firewall,” Australian Strategic Policy Institute, September 3, 2019.

³ For a review of China's international social media engagement, see Joyce Y. M. Nip and Chao Sun, “China's News Media Tweeting, Competing with US Sources,” *Westminster Papers in Communication and Culture*, Vol. 13, No. 1, 2018.

⁴ Koh Gui Qing and John Shiffman, “Beijing's Covert Radio Network Airs China-Friendly News Across Washington, and the World,” Reuters, November 2, 2015.

rative to the wider world, with China launching its first foreign television channel in 1992 and first foreign website in 1997.⁵

Accusations of Chinese disinformation on foreign social media first began in Taiwan following President Tsai's election in 2016. Many of the early examples focused on undermining support for Tsai by claiming that she was mismanaging the military or damaging traditional Taiwan's traditional culture.⁶ However, one report in 2014 identified fake Twitter accounts (bots) that were broadcasting positive messages about Tibet, suggesting at least some parts of the Chinese government had a covert presence on foreign social media before 2016.⁷ Moreover, reports emerged in 2015 and again in 2016 that state-run media accounts on Twitter were buying followers as a way to artificially increase their influence, suggesting interest in covert tactics before 2016.⁸ Chinese intelligence has also been accused of using social media for recruitment since at least 2017, evidence that the Chinese government sees value in social media beyond simply propaganda.⁹ Based on the released Twitter information, it appears that those accounts, at least, were acquired by China in 2017, aligning well with other known data points.¹⁰ Taken together, these are indications of improper Chinese government uses of social media and early uses of social media for disinformation, so it would not have been a leap for China to use social media disinformation for election interference against Taiwan in 2018.

⁵ Nip and Chao Sun, 2018.

⁶ "Authorities Deny Rumor of Ban on Incense, Ghost Money Burning," *FocusTaiwan*, July 21, 2017; J. Michael Cole, "Fake News at Work: President Tsai 'Persecutes Religion in Taiwan,'" *Taiwan Sentinel*, July 20, 2017.

⁷ Jonathan Kaiman, "Free Tibet Exposes Fake Twitter Accounts by China Propagandists," *The Guardian*, July 22, 2014.

⁸ Nicholas Confessore, Gabriel J. X. Dance, Richard Harris, and Mark Hansen, "The Follower Factory," *New York Times*, January 27, 2018; Tom Grundy, "Did China's State-Run News Agency Purchase Twitter Followers?" *Hong Kong Free Press*, April 14, 2015; Alexa Olesen, "Where Did Chinese State Media Get All Those Facebook Followers?" *Foreign Policy*, July 7, 2015.

⁹ "German Spy Agency Warns of Chinese LinkedIn Espionage," BBC, December 10, 2017.

¹⁰ Uren, Thomas, and Wallis, 2019.

Chinese Command and Control for Social Media Operations

China's broader social media operations are likely run and/or coordinated by a combination of the CPD [中央宣传部], the UFWD, and the PLA, but it is difficult to attribute any actions to specific organizations and institutions beyond the acknowledged account holder.¹¹ Compared with information about Russian social media activity, there is less public research and fewer government reports focusing on China's online presence. The majority of China's overt propaganda on social media is conducted through accounts acknowledged to be operated by state-run media, such as Xinhua's Twitter presence. China's Ministry of Foreign Affairs uses Twitter, Facebook, and other platforms for public diplomacy—the Chinese ambassador in Washington, D.C., just opened a Twitter account.¹² Other foreign social media accounts are held by Chinese state-owned enterprises operating abroad (such as Sinopec on Twitter) and high-profile infrastructure projects (such as the China-Pakistan Economic Corridor—part of the Belt and Road Initiative).¹³ The CCP's International Liaison Department joined Twitter in April 2020, reflecting the Party-state's deepening embrace of the platform it bans at home.¹⁴

Within the CCP and government bureaucracy, state-run media is directly controlled by the CCP's CPD, so any social media activity will ultimately fall under its purview. Higher-level guidance from CCP leadership and coordination across Party-state bureaucracies and the military likely occurs but is difficult to definitively track. One recent study on Chinese state-run media messaging on U.S. social media

¹¹ On China's propaganda system, see Anne-Marie Brady, *Marketing Dictatorship: Propaganda and Thought Work in Contemporary China*, New York: Rowman and Littlefield, 2009; and Samantha Hoffman, *Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion*, Sydney, Australia: Australian Strategic Policy Institute, 2019.

¹² Cui Tiankai, Twitter account, undated.

¹³ CPEC Official, @CPEC_Official, Twitter account, undated; Sinopec, @SinopecNews, Twitter account, undated. The China-Pakistan Economic Corridor account appears to be maintained by the Chinese embassy (Ministry of Foreign Affairs) in Pakistan.

¹⁴ Hu Zhaomin, @SpokespersonHZM, Twitter account, undated.

found that there appeared to be some synchronized campaigns, or at least common themes, across different accounts, reflecting this possible combination of high-level coordination and/or guidance.¹⁵ One part of that guidance is likely the general propaganda guidance provided to state-run media by the CPD.¹⁶

The released Twitter information supports our belief that multiple Chinese government actors are involved in broader social media disinformation activity. We assess that the Twitter accounts targeting the Hong Kong protests were run by the CPD and/or the UFWD, especially because, so far, researchers have not identified any evidence linking this data set with the concerted campaign against the 2018 election as it was described by the Taiwan government.¹⁷ Instead, early research suggests that these accounts have focused on several political opponents of the CCP who were publicly very critical, such as dissident Guo Wengui (also known in English as Miles Kwok).¹⁸ This points to at least two different groups within China conducting hostile social manipulation on foreign platforms. Our hypothesis is that the PLASSF is responsible for long-term, advanced, broad, and (high-quality) covert manipulation of targeted events, such as Taiwan’s 2018 elections, which would allow for months or perhaps years of careful planning and preparations leveraging the PLASSF’s computing power and expertise. Meanwhile, the CPD and/or UFWD can occasionally be asked to respond to immediate crises that the PLA Strategic Support Force is not prepared for and use a relatively basic bot infrastructure to conduct operation, as occurred in the case

¹⁵ Insikt Group, 2019.

¹⁶ For the best public record of this guidance, see “Directives from the Ministry of Truth,” China Digital Times, undated.

¹⁷ Because of staffing limitations, both the CPD and UFWD might find it expedient to contract out aspects of social media disinformation campaigns to teams that run content farms [内容农场], and to trolls or paid posters [五毛党]. Such forces help support China’s efforts to develop a whole-of-government, whole-of-society approach to conflict, providing additional vectors and complicating adversary defense efforts.

¹⁸ A basic Chinese state-run campaign against Guo was suspected early on when he began making revelations about CCP leadership. See Mazarr et al., 2019, p. 142. For analysis of the Hong Kong–linked accounts targeting Guo and others, see Uren, Thomas, and Wallis, 2019.

with Hong Kong. If we are correct, this could mean the PLASSF's covert manipulation on Western social media platforms has so far gone undetected, or at least remains unattributed.

Where Chinese Social Media Actors Are Headquartered

The vast majority of China's propaganda bureaucracy, like the rest of its government and ruling class, is based in Beijing. The CPD, UFDW, and PLA all have headquarters in the Beijing area, close to the Chinese leadership. However, the more-operational aspects of China's social media operations are spread outside Beijing. Within China, some of the propaganda apparatus targeting Taiwan is based in Fujian, the province across from Taiwan. This is the location of Base 311 (Unit 61716), the PLASSF unit responsible for psychological warfare targeting Taiwan.¹⁹ Beyond China, at least some (and perhaps the majority) of China's state-run media employees targeting foreign audiences are based in those audiences' countries, with China's main global television station, CGTN, employing roughly 180 people in the United States alone.²⁰

It is difficult to determine with certainty the provenance of most disinformation efforts, but some anecdotal evidence for China is available. One Taiwan interviewee claimed that China is attacking Taiwan with as many as 2,400 separate pieces of disinformation every day.²¹ A Taiwan government official said the PLASSF had 300,000 troops.²² If even one-third of those are for psychological operations and a portion

¹⁹ For analysis of this organization, see J. Michael Cole and Shelley Shan, "PRC Steps Up Psychological Warfare Targeted at Taiwan," *Taipei Times*, August 26, 2011; and Stokes and Hsiao, 2013.

²⁰ Paul Mozur, "Live from America's Capital, a TV Station Run by China's Communist Party," *New York Times*, February 28, 2019a; Paul Mozur, "Facing Legal Scrutiny, China's State TV Recalls Its U.S. Head," *New York Times*, March 8, 2019b.

²¹ Interview with Taiwan-based think-tank analyst, interview 3, Taipei, January 2019; Gavin Ellis, "China Could Be Using Taiwan as a Testing Ground for Disinformation Campaigns," *New Zealand Listener*, February 16, 2019.

²² Pan, 2018.

of those are focused on social media, that would still be potentially thousands of people available to engage in disinformation on social media. This is one area where the size of China's population, especially government propaganda and military personnel, is an advantage.

The Scale of Chinese Social Media Operations

Measuring the extent of any country's social media presence and activity is daunting, even when looking only at its overseas activities. China reportedly spends at least \$10 billion a year on propaganda, meaning that even if only a small portion of this goes toward social media, it would have a large impact.²³ Compared with Russia, which spends several hundred million dollars per year on information efforts abroad, China's budget appears larger, which means it might be able to simply overwhelm the information environment overtly and thus have less need to resort to covert manipulation.²⁴ The largest share of the Chinese government's effort on propaganda, including social media, is probably focused domestically, with studies suggesting that somewhere between 0.6 percent and 16.7 percent of all domestic posts are manufactured by those affiliated with the CCP in some form.²⁵ Looking abroad, one study reported that "the selected public accounts run by Xinhua News, *People's Daily*, and CCTV News/CGTN have established a significant presence in the Twittersphere in the six-and-a-half years or so since they started their accounts," though they still

²³ David Shambaugh, "China's Soft-Power Push," *Foreign Affairs*, July 2015. Others have suggested that \$10 billion might be an underestimate. See Anne-Marie Brady, "Plus ça change? Media Control Under Xi Jinping," *Problems of Post-Communism*, Vol. 64, No. 3, 2017b.

²⁴ For a discussion of Russia's budget, see Treyger, Cheravitch, and Cohen, forthcoming.

²⁵ Mary Gallagher and Blake Miller, "Can the Chinese Government Really Control the Internet? We Found Cracks in the Great Firewall," *Washington Post*, February 21, 2017; Gary King, Jennifer Pan, and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument," *American Political Science Review*, Vol. 111, No. 3, 2017.

trailed Russia's RT.²⁶ Another study examined just *People's Daily* and Xinhua on Instagram, stating that, "These two Chinese influence profiles reached a level of audience engagement roughly one-sixth as large as the entire Russian IRA-associated campaign targeting the United States on Instagram."²⁷ The Hong Kong data set also provides some hard numbers, though it is very likely only a portion of overall Chinese activity. Twitter identified 936 active accounts and another 200,000 accounts it had already suspended; Facebook identified five accounts, three pages, and seven groups; and YouTube identified 210 accounts.²⁸ Only Facebook tallied China's reach through this activity—roughly 18,000 users total, a number far short of similarly identified Russian and even Iranian activity.

For its part, although the PLA does not appear to have accounts on foreign social media platforms, it does have many accounts on Chinese-owned platforms. The PLA's official propaganda outlet, *PLA Daily*, is the first PLA organization known to have a social media account, opening its Weibo account in March 2010. The PLAAF was the first service to open a social media account (in October 2015 on Weibo and WeChat), and the PLA Navy was the most recent service to open an account (in April 2019).²⁹ In sum, it would appear that Russia is more active in social media operations, but China's involvement in such activities has been growing over the past half-decade. With China getting a slightly later start than Russia, it is possible that China is still improving and gaining traction with international audiences. Another possibility is that China has a broader set of tools for influence operations and thus, unlike Russia, it does not have to focus so much of its energy on the use of disinformation campaigns via social media.

²⁶ Nip and Chao Sun, 2018.

²⁷ Insikt Group, 2019.

²⁸ Gleicher, 2019; Huntley, 2019; Twitter, 2019.

²⁹ The SSF has not yet opened an official social media account, though it is suspected of operating foreign social media account covertly against Taiwan. "China's @PLA Navy Official Account Opens [中国@人民海军 官方微博正式开通]," Sina.com, April 15, 2019.

China’s Reach to Foreign Audiences

The Chinese government can reach foreign audiences through four main vectors. The first two are Chinese- and foreign-language content that spread on Chinese-owned platforms, such as WeChat; the second two are Chinese- and foreign-language content delivered on such foreign-owned platforms as Facebook, LINE, PTT, or other social media platforms. Many Chinese government organizations, including the PLA, have directly controlled accounts on WeChat and Weibo, allowing them to easily engage in the public conversation both at home and abroad. In addition, were a conflict between the United States and China to break out, depending on the location of the conflict, local populations and foreign audiences alike might turn to Chinese-run social media platforms, most likely WeChat. The majority of foreign users of WeChat are likely to be Chinese speakers, however, so content in other languages likely will be limited. By contrast, non–Chinese-speaking foreign audiences might be more likely to use Western social media platforms, but this is precisely where the PLA’s social media skills set is weakest.

The PLA has no official presence on foreign social media. This void is filled by Chinese state-run media outlets, which are allowed to have accounts on foreign platforms, including Xinhua on Twitter (12.5 million followers) and *China Daily* on Facebook (94 million followers).³⁰ Consequently, the PLA must rely on such outlets to relay content to users on those platforms. For example, China’s participation in the International Army Games has been promoted, with *China Daily* alone reaching 1.2 million people on Facebook in 2017. *China Daily* also initiated a dramatic expansion to 17 foreign platforms in 2018; it is unclear exactly how many foreign users were reached that year, but total audience including Chinese citizens was reportedly 120 million people.³¹ This relayed content can be reposted directly (because some

³⁰ Xinhua, Twitter account, undated; *China Daily*, Facebook account, undated.

³¹ Li Dayong [李大勇], Zhang Shengtao [张圣涛], and Xia Yun [夏云], “Focusing on Improving the Effectiveness of Propaganda for International Military Competition News: Reflection on Army Organized ‘International Army Games-2018’ Coverage [着力提升国际军事赛事新闻宣传效益：陆军承办‘国际军事比赛-2018’报道回眸],”

PLA propaganda has foreign-language subtitles) or dubbed, but our observation is that, most of the time, state-run media translate PLA-related content. There is some PLA frustration that the media outlets do not perform this function very well: In one example from November 2018, the *People's Daily* Twitter account posted a video clip of what it said was a DF-41 intercontinental ballistic missile.³² On closer inspection, it was more likely a new version of the DF-11 short-range ballistic missile.³³ Such occasions reflect the challenge of nonmilitary personnel accurately relaying detailed military information.

Another consequence of the PLA not having a direct presence is that it does not have its own data on how foreign audiences engage with its content—instead, it has to rely on social media analytics provided by state-run media.³⁴ Under the PLA's desire for a big, data-driven, tailored messaging strategy, this could be a critical limitation. Thus, some in the Chinese military are calling for the PLA to open its own foreign social media accounts. (We discuss this further later in this chapter.)

The PLA's lack of overt accounts on foreign social media could limit its ability to use these forums for operational effects. According to Hootsuite, a social media analytics company, 70 percent of East Asians use social media, as do 61 percent of Southeast Asians, 57 percent of those in Oceania, and 24 percent of South Asians.³⁵ Tables 3.1–3.3 break down rates of social media penetration.

For messaging, WeChat is the top application only in China. U.S.-based Facebook Messenger is the top messaging application in Cambodia, Thailand, and Mongolia; LINE, from South Korea, is the

Military Correspondent [军事记者], October 2018; Tan Yingshuai [谭英帅], "The Practice and Thinking of News Propaganda for the Army Hosting the 'International Military Competition-2017' [陆军承办"国际军事比赛—2017"新闻宣传的实践与思考]," *Military Correspondent* [军事记者], January 2018.

³² *People's Daily*, "Video Reveals DF-41," Twitter post, November 17, 2018.

³³ Scott LaFoy, "I Watch a Lot of CCTV," Twitter post, November 18, 2018.

³⁴ Zhang Gugu [张汨汨], "Actively Use Overseas Social Media to Participate in Military External Propaganda [积极利用海外社交媒体参与军事外宣]," *Military Correspondent* [军事记者], August 2016.

³⁵ Hootsuite, "Digital 2019 Vietnam (January 2019)," February 3, 2019f.

Table 3.1
Overall Social Media Penetration in Select Countries

	Japan	Philippines	Singapore	Taiwan	United States
Total internet users (percentage of population)	94	71	84	88	95
Social media users (percentage of population)	61	71	79	89	70
Total time on social media per day (hours)	0.6	4.2	2.1	1.9	2.0

SOURCES: Hootsuite, “Digital 2019 Japan (January 2019),” webpage, February 3, 2019b; Hootsuite, “Digital 2019 Philippines (January 2019),” webpage, February 3, 2019c; Hootsuite, “Digital 2019 South Korea (January 2019),” webpage, February 3, 2019d; Hootsuite, “Digital 2019 Taiwan (January 2019),” webpage, February 3, 2019e; Hootsuite, “Digital 2019 United States of America (January 2019),” webpage, January 31, 2019a.

Table 3.2
Percentage Penetration of Specific Social Media Platforms in Select Countries

Rank	Japan	Philippines	Singapore	Taiwan	United States
1	YouTube (75)	Facebook (97)	YouTube (87)	YouTube (90)	YouTube (82)
2	LINE (67)	YouTube (96)	WhatsApp (86)	Facebook (89)	Facebook (80)
3	Twitter (49)	FB Messenger (89)	Facebook (82)	LINE (84)	FB Messenger (57)
4	Facebook (36)	Instagram (64)	Instagram (59)	FB Messenger (57)	Instagram (51)
5	Instagram (33)	Twitter (54)	FB Messenger (52)	Instagram (49)	Twitter (42)
6	Ameblo (37)	Skype (44)	Twitter (34)	WeChat (32)	Pinterest (36)
7	FB Messenger (11)	LinkedIn (36)	LinkedIn (33)	Skype (25)	Snapchat (31)
8	Skype (8)	Viber (34)	WeChat (33)	Twitter (24)	LinkedIn (28)
9	Pinterest (4)	Pinterest (33)	Skype (28)	EYNY (22)	Reddit (19)
10	Tumblr (4)	Snapchat (28)	Pinterest (24)	WhatsApp (19)	Skype (19)

SOURCES: Hootsuite, 2019a–2019e.

Table 3.3
WeChat Penetration in Select Countries

	Japan	Philippines	Singapore	Taiwan	United States
Rank	15	13	8	6	15
Percentage	2	23	33	32	9

SOURCES: Hootsuite, 2019a–2019e.

top application in Japan and Taiwan. Also from South Korea is Kakao Talk, which is the top application there. Finally, Zalo is the top application in its country of origin, Vietnam. Social media messaging methods also vary by nation. For example in Vietnam, there is only 66 percent internet penetration among the population, but 90 percent of those users have social media on their phones (mobile social media use grew 16 percent in 2018); even more use social media on a computer.³⁶ By comparison, 95 percent of U.S. residents have internet connectivity, but only 64 percent of internet users use social media on their mobile phones.³⁷ WeChat penetration in the United States is very limited: One study found that less than 10 percent used it at least once a week in 2018.³⁸ It is likely, however, that WeChat penetration is higher among the Chinese-American population of roughly 4–5 million (and, more broadly, among Chinese-speaking communities, including U.S. scholars, policymakers, and analysts who work on or in China regularly). This might mean that China wields greater influence via WeChat than that platform’s penetration rate among the broader U.S. population would suggest.³⁹

Some countries in Asia use major U.S. platforms (such as Facebook and Twitter) and their own indigenous platforms. This means

³⁶ Hootsuite, 2019f.

³⁷ Hootsuite, 2019a.

³⁸ Statista, “Frequency of WeChat Use in the United States as of January 2018,” webpage, March 21, 2019. For analysis of WeChat in the United States, see Emily Parker, “Can WeChat Thrive in the United States?” *MIT Technology Review*, August 11, 2017.

³⁹ The authors thank reviewer Anne-Marie Brady for recommending that they include this point.

China likely will have to develop accounts and messaging strategies on these platforms, both for overt propaganda accounts and covert manipulation. As already mentioned, Kakao Talk is South Korea's most popular platform, with 83 percent penetration of that nation's internet users.⁴⁰ In Vietnam, 74 percent of internet users have accounts with Zalo, the fourth most popular platform.⁴¹ However, many South Korean and Vietnamese internet users also consume Western social media, so indigenous platforms are not the sole vector for China.

The lack of openly acknowledged PLA-owned accounts on foreign social media platforms appears to be a deliberate decision by high-level authorities against establishing a presence on those platforms.⁴² The Chinese military is clearly focused on influencing foreign perceptions about its capabilities and behaviors, so the decision to avoid Western social media is curious.⁴³

Some PLA officers want to address this shortcoming. According to one report, "PLA authors' arguments for opening accounts on Twitter, Facebook, YouTube, and Instagram, among others, include having direct access to its intended audiences, avoiding misinterpretation by Western media, being able to respond to negative stories abroad, and generally monitoring foreign discussions about the PLA."⁴⁴ The report found eight articles in PLA propaganda journals dating to 2014 that

⁴⁰ Hootsuite, 2019d. Kakao, LINE, and other social media platforms were blocked in June 2019, at least temporarily. See "Mainland Restrictions to Be Lifted on Line and KakaoTalk, South Korean Diplomat Says," *South China Morning Post*, June 13, 2019.

⁴¹ Hootsuite, 2019f. For more on Zalo, see Anh-Minh Do, "Zalo: Vietnam's Flagship Mobile Messaging App Has Arrived," *TechInAsia*, February 4, 2013; and Goran Bogunovic, "Zalo Is Vietnam's Answer to WhatsApp and It's Growing Big," *Domain.me*, November 7, 2018.

⁴² Chen Jie [陈捷], "Create a Shock Team for Military External Propaganda [打造军事外宣队伍的突击队]," *Military Correspondent* [军事记者], June 2015.

⁴³ Anne-Marie Brady, in a personal communication with the authors, points out that the PLA has posted recruitment ads on YouTube and cautions that the most rigorously accurate thing one can say about Chinese presence on Western social media platforms is that there are no openly acknowledged accounts. Whether the Chinese Party-state has used cutout accounts on Western social media platforms was something our research could not definitively determine.

⁴⁴ Beauchamp-Mustafaga and Chase, 2019.

argued for the PLA to have a direct presence on Facebook, Twitter, and others, and even more articles that touted the value of propaganda on these platforms but accepted the handling of that role of state-run media instead of the PLA.⁴⁵ As mentioned earlier, the Chinese ambassador in Washington, D.C., only recently opened a Twitter account, perhaps reflecting a studied hesitance about subjecting official Chinese government organs to criticism on foreign platforms outside the reach of China's censors.⁴⁶

Social Media Disinformation Campaign Execution

One Taiwan PLA expert we spoke with said that the PLA follows a standard approach to targeting. It selects the platform best suited for the target demographic. It then collects personal data, maps social networks, cultivates opinion leaders, joins discussion group, and—after building sufficient trust among the group—disseminates disinformation aimed at undermining its adversary.⁴⁷ Not everyone agrees whether such patterns exist. For example, some Taiwan interviewees commented that Beijing uses PTT to reach those younger than 40 years of age; other interviewees said Facebook was the primary vector to reach younger audiences and that LINE was more likely to be used to communicate with older social media users in Taiwan.⁴⁸ Another expert on the online domain commented that LINE is relatively fertile ground for PLA disinformation operations because it is not an open platform, meaning that messages can circulate for some time before the government becomes aware of them and can respond.⁴⁹

⁴⁵ Beauchamp-Mustafaga and Chase, 2019.

⁴⁶ Cui Tiankai, undated.

⁴⁷ Interview with Taiwan cyber expert, interview 9, Taipei, January 2019.

⁴⁸ Interview with Taiwan academic, interview 8; Taipei, January 2019; interview with Taiwan think-tank expert, interview 12D, Taipei, January 2019. The academic commented that one of the standard texts for the PLA's conduct of social media disinformation campaigns appears to be Zeng Huafeng and Shi Haiming, 2014.

⁴⁹ Interview with Taiwan government official, interview 10A, Taipei, January 2019.

Types of Campaigns

China appears to pursue three general types of disinformation campaigns.

The first type is steady-state efforts that are constantly ongoing and designed to deepen social divisions, lower morale, and depress confidence in democracy. These efforts need not be keyed to any specific event and are intended to serve as something like a constant drag on an adversary organization or society. Such efforts are a form of gray-zone warfare or cost imposition that sap resources and are difficult to attribute or respond to; furthermore, engagement in these efforts pose relatively low risk for China. These efforts are generally tied to one-off stories not linked to other news except insofar as they might target the same general adversary (such as the Tsai administration in Taiwan).

A second type of disinformation that China engages in on social media is intended to support goals that are more discrete or time-bounded, such as hampering a trip abroad by the Taiwan president, complicating a regularly scheduled military exercise, or affecting an election outcome over several months. These disinformation efforts try to create a cascade of negative news about a topic in ways that represent a campaign that is more deliberate and resource-intensive. As one Taiwan government official related, these efforts can eat up enormous amounts of senior official time or shape the outcome of local or even presidential electoral contests.⁵⁰

Opportunistic attacks reflect a final type of disinformation operation on social media. “They jump on targets of opportunity a lot,” one Taiwan analyst of information warfare commented.⁵¹ These opportunities can be an adversary’s misstep or an action by someone within an opponent’s society that can be amplified so that it appears to represent a broader degree of resistance to someone or some policy position that China also opposes. In many cases, “China just serves to elevate the profile of unfavorable news that may in fact be true,” an interviewee remarked.⁵² One possible example of this described by an interviewee

⁵⁰ Interview with Taiwan government official, interview 18, Taipei, January 2019.

⁵¹ Interview with Taiwan cyber expert, interview 9, Taipei, January 2019.

⁵² Interview with Taiwan government official, interview 6B, Taipei, January 2019.

involved a case in August 2016 in which an ROC Army tank fell off a bridge and landed upside down in a river, leading to the drowning death of four soldiers.⁵³ China might use social media to amplify the news so as to create an impression of greater military incompetence and to drag down the political support for the government.⁵⁴ In other cases, “some of China’s efforts are just designed to magnify the voices of those who are already dissatisfied,” another interviewee noted.⁵⁵

Intended Targets

Chinese disinformation efforts have targeted a wide variety of actors within Taiwan.⁵⁶ China aims pro-China messages at communities that are already sympathetic to China’s cause; as one Taiwan official noted, “China’s sympathizers play a particularly critical role as facilitators, spreading positive information about China online and generating feedback” for China’s messages.⁵⁷ China also feeds negative information about its adversaries, such as the Tsai administration, to groups that are either already critical or might be receptive to negative information about those adversaries, even if the groups are not pro-China. Countering such disinformation can be extremely challenging, one senior official warned, noting that “[although] media literacy in Taiwan is growing, for those groups who don’t already believe [the government has some degree of credibility], you won’t be able to convince them [that what they’ve been exposed to is disinformation].”⁵⁸ Finally, according to several interviewees, China particularly targets young people, retired

⁵³ Sophia Yang, “Kaohsiung Tank Accident Adds One Dead to Four,” *Taiwan News*, August 19, 2016.

⁵⁴ Interview with U.S. government official, interview 5A, Taipei, January 2019.

⁵⁵ Interview with Taiwan government official, interview 10C, Taipei, January 2019.

⁵⁶ It is worth pointing out that the notion of targeting disinformation in open online forums is a bit of a misnomer, because information, once out in the public, cannot always be discretely delivered to specific recipients. Despite the imperfect nature of targeting for online content delivery, however, some platforms afford more discretion to the content producer whereas other platforms are intended to have broad-scale distribution and effects.

⁵⁷ Interview with Taiwan government official, interview 14, Taipei, January 2019.

⁵⁸ Interview with former Taiwan government official, interview 4A, Taipei, January 2019.

ROC military officers, pensioners, religious groups within Taiwan society, farmers and fishermen, and those deeply attached to one political party or the other (because such highly partisan information consumers can be encouraged to deepen social divisions).⁵⁹

One expert on Chinese military information operations said that there are indications that PLA-linked accounts have sought to develop trusted profiles on social media through the offering of online coupons that can be used to build relationships with people living near base-hosting communities. These online relationships can then be used in tandem with human operators (or “sleeper agents” in place over a long period) to stir up resistance to military operations and foster social divisions over national security and defense affairs.⁶⁰

China also might be shifting away from political issues to more cultural wedge ones. One interviewee said that PRC operations are “no longer conducting targeting by candidates or political parties like the Kuomintang—now, their focus is shifting to issues such as same-sex marriage or what name Taiwan should participate in the Olympics under.”⁶¹ Another interviewee echoed that Chinese operations were shifting from “targeting political parties to targeting of the people of Taiwan.”⁶² One defense and intelligence expert commented that Chinese disinformation operations strive to “identify opinion leaders,” aligning with known PLA writings, such as those discussed in Chapter Two.⁶³ Interviewees argued that prominent Taiwan figures—such as singer/actress Liu Le-Yan, who commented that the Taiwan Strait transit of the PLA Navy aircraft carrier *Liaoning* was unthreatening because it had “come to protect us,”⁶⁴ and master baker Wu Pao-Chun,

⁵⁹ Interview with Taiwan-based think-tank analyst, interview 3, Taipei, January 2019; interview with Taiwan cyber expert, interview 9, Taipei, January 2019.

⁶⁰ Interview with Taiwan cyber expert, interview 9, Taipei, January 2019. It is unclear how much evidence exists to support this claim.

⁶¹ Interview with Taiwan political party activist, interview 13A, Taipei, January 2019.

⁶² Interview with Taiwan politician, interview 7, Taipei, January 2019.

⁶³ Interview with retired Taiwan military officer, interview 4B, Taipei, January 2019.

⁶⁴ Zhang Yu, “Taiwan Actress’s Welcoming Comments on *Liaoning* Put Her Under Scrutiny,” *Global Times*, January 19, 2017.

who has publicly described himself as “a Chinese person who supports the ‘1992 Consensus’”⁶⁵—were examples of the kinds of opinion leaders whom Chinese disinformation operations sought to leverage.⁶⁶

Assuming the adoption of internet-of-things technology creates an environment characterized by even wider proliferation of personalized data that can be harvested for information-targeting, Chinese activity in this arena will likely become more granular. According to one news report, “China is certain to improve the technical sophistication and professionalism of its measures, which would lead to real-time reactions to ongoing events.”⁶⁷ Specifically, the article noted that “China uses metadata, artificial intelligence and other technologies to analyze what content young Taiwan residents consume and exploit the information to cultivate sympathy for Beijing.”⁶⁸ The next section discusses those factors enabling Chinese social media disinformation operations, particularly in Taiwan.

Enablers of Chinese Disinformation Operations

To prosecute a broad-gauge, sophisticated, and effective disinformation campaign, one interviewee noted, “the PLA requires supporting infrastructure.”⁶⁹ This supporting infrastructure features a somewhat

⁶⁵ Lin Zehong [林则宏], “Wu Pao-Chun, Accused of Supporting Taiwan Independence: ‘I Am a Chinese Person Who Supports the ‘1992 Consensus’ [遭指台獨 吳寶春: 我是中國人、支持「九二共識」],” *United Daily News* [聯合報], December 10, 2018. The “1992 Consensus,” a term coined by former Taiwan National Security Advisor Su Chi in 2000, refers to a purported tacit agreement between Taiwan and China following secret meetings in 1992 that each side would agree that the two sides of the Strait both belong to one China and could leave unspecified which “China” they belong to, with Taipei claiming to be the seat of the Republic of China and Beijing claiming that “China” is in reference to the People’s Republic of China.

⁶⁶ Interview with Taiwan political party activist, interview 13A, Taipei, January 2019.

⁶⁷ Aaron Tu and Jonathan Chin, “Beijing Using Emergent Media to Attract Youth,” *Taipei Times*, July 22, 2019.

⁶⁸ Tu and Chin, 2019.

⁶⁹ Interview with retired Taiwan military officer, interview 4B, Taipei, January 2019.

favorable sociopolitical human terrain that is open to some of the messages that China is seeking to spread, a variety of social media platforms that China can gain access to and build credibility on, and an architecture of supplementing tools ranging from diplomacy and economic policy levers to military capabilities and subversive or underground forces that will carry out Beijing’s will. These factors support China’s disinformation efforts; therefore, to the extent that they can be targeted or compromised, they represent vulnerabilities that could be hardened to complicate China’s ability to wage social media disinformation campaigns.

Human Terrain

To spread disinformation, China requires societal fissures that it can readily exploit. In the case of Taiwan, important distinctions exist between (1) those members of society who support the Kuomintang (KMT; Nationalist Party) or other political parties that lean more toward engagement with China and emphasize a shared historical identity and (2) those who lean more toward the Democratic Progressive Party (DPP), which tends to emphasize Taiwan’s unique heritage, identity, and sovereign status. The KMT and other parties that focus on a shared identity with the PRC as part of “China” (however defined) are, in Taiwan’s political lexicon, referred to as the “blue camp” [藍營]; those parties that support a focus on Taiwan’s unique political identity (sometimes referred to casually as “independence-oriented”) are generally grouped under the rubric of the “green camp” [綠營].⁷⁰

Despite China’s distaste for the DPP, Chinese social media disinformation campaigns have sought to undermine the centrist Tsai administration by playing up themes that appeal to “deep blue” and also to “deep green” information recipients. In so doing, they have sought to deepen social divisions and drive Tsai toward the “deep green” camp in the primaries in an effort to undercut her appeal to voters who favor more-moderate policies and politics; as one interviewee commented, “they are attacking the middle, not the ‘deep blue’ or ‘deep green.’”⁷¹

⁷⁰ The two colors refer in part to the main parties’ campaign flag colors.

⁷¹ Interview with retired Taiwan military officer, interview 4B, Taipei, January 2019.

Facilitating China's understanding of Taiwan society has been the dramatic expansion of contacts and exchange across the Strait over roughly the past two decades. Although Taiwan businesses began investing in China in the 1980s, this is a small sample of Taiwan society and not particularly useful either as a vector for influence or as a tool to understand rapidly evolving broader Taiwan public opinion.⁷² The opening up of the *three small links* [小三通]—limited direct postal, shipping, and trade connections between the two sides of the Taiwan Strait in the early 2000s—and the broader *three links* [三通]—shipping, flights, and mail between Taiwan and China in 2008—brought increased access to Taiwan society by Chinese officials, tourists, students, and workers.⁷³ As a consequence, the Chinese government and its associated intelligence organs came into possession of a dramatically expanded amount of information about traditional Taiwan society and politics. Additionally, because Taiwan is an open and online society, China presumably can intercept the enormous volumes of personal communications and personal data transiting through unsecure systems and use that material to develop an increasingly sophisticated picture of its target audience. The UFWD's main responsibility is to understand and exploit Taiwan society for China's ends, so there is likely plenty of expertise and intelligence within the Chinese government if that picture is shared.

Some in Taiwan, including key social media influencers, have proven willing to serve China's ends—or have been compromised or coerced into doing so. Taiwan interviewees also report widespread suspicion that China has, through either cutout organizations or direct hiring, built up a support network of *transponders*, or local Taiwan residents who can be relied on to source key messages from PRC-based “content farms” [内容农场]. Another approach from China is to co-opt people living in Taiwan to amplify CCP messaging. For example, one recent research report found that “Beijing's increased use of emergent media is also evident in the videos on platforms that feature Taiwan

⁷² Murray Scot Tanner, *Chinese Economic Coercion Against Taiwan: A Tricky Weapon to Use*, Santa Monica, Calif.: RAND Corporation, MG-507-OSD, 2007.

⁷³ CEIC, “Taiwan Visitor Arrivals,” webpage, undated.

businesspeople and young people espousing pro-China views.”⁷⁴ Another recent report found that Chinese government agents have paid hotels, restaurants, and bars to keep televisions that broadcast in public areas tuned to pro-PRC media as a way to expose Taiwan media consumers to information that is favorable to China.⁷⁵

A final point on the human terrain is how it interfaces with information consumption patterns. In some countries, such as Singapore, the media is state-owned and thus difficult to manipulate via social media disinformation. In other societies, censorship is widely practiced, making disinformation difficult to transmit. In still other societies, such as Japan, the majority of information consumption is done through traditional print media, television, and radio. In Taiwan, however, China finds the most favorable possible environment: a private sector–dominated media environment in which the state is leery of intervening for fear of being charged with overreach and a society that consumes a substantial amount of its information through online sources. Taiwan government officials repeatedly explained that they were extremely cautious about using policy levers to pull disinformation offline for fear of subverting Taiwan’s democratic values. DPP officials, who struggled against the KMT’s martial law regime, were particularly averse to doing anything that could justify a return to censorship and government control over free speech.⁷⁶

As noted, Taiwan society gets much of its news via social media, making it an environment ripe for Chinese disinformation operations. Facebook, for example, reportedly enjoys an 89-percent penetration rate in Taiwan; other major social media platforms—such as YouTube, LINE, Instagram, WeChat, and other platforms—are also widely

⁷⁴ Tu and Chin, 2019.

⁷⁵ Yimou Lee and I-hwa Cheng, “Paid ‘News’: China Using Taiwan Media to Win Hearts and Minds on Island—Sources,” Reuters, August 9, 2019.

⁷⁶ Interview with Taiwan government official, interview 10C, Taipei, January 2019. This is also a narrative that China and PRC-friendly media sometimes seek to exploit. See, for example, Lawrence Chung, “Taiwan’s Bid to Tackle ‘Fake News’ Raises Fears over Freedom of Speech,” *South China Morning Post*, October 1, 2018.

adopted.⁷⁷ This high degree of interface between the human terrain and the technology landscape facilitates multiple vectors along which China can effect social media disinformation campaigns to reach Taiwan society. The PLA and broader Party-state are actively tracking and researching Taiwan social media, which could improve its targeting of Taiwan social media users and suggests that such targeting is already ongoing.⁷⁸

Information Technology and Media Terrains

Chinese social media disinformation campaigns also benefit from access to both traditional media and information technology terrains that the PRC can access, communicate across, and exploit. As one interviewee pointed out, such “supporting elements are necessary for

⁷⁷ Hootsuite, 2019e. Other surveys have found even higher usage of Facebook in Taiwan. See Ralph Jennings, “Facebook Says It Already Has 97% of Taiwan’s Internet Users, and Now It’s Targeting Businesses,” *Forbes*, October 11, 2018.

⁷⁸ Lai Dongwei [赖东威], 2017; Lou Sijia [娄思佳], 2017; Wang Dapeng [王大鹏], Yue Chunying [岳春颖], and Yan Jie [严洁], “Research on the Use of Social Media in Election Propaganda in Taiwan: An Analysis Based on In-Depth Interview [台湾地区选举宣传中社交媒体的使用研究:一种基于深度访谈的分析],” *Modern Communication*, [现代传播(中国传媒大学学报)], May 2016; Mo Li [莫莉], “Democratic Deliberations Are Still Noisy Self-Talk: The Content of the DPP Candidate Facebook in the 2016 Taiwan Election and the Participation of Netizens [民主的商议还是喧嚣的自语:2016年台湾地区选举中民进党候选人脸谱网内容及网民参与研究],” *Journalism and Mass Communication Monthly* [新闻界], August 2017; Tian Hong [田弘], Lin Gang [林冈], and Fan Zhiqiang [凡志强], “A Study of the Interaction in Facebook Between Public and Mayors of Kaohsiung, Taipei, and New Taipei [台湾地方政府领导人使用社交媒体互动研究——以高雄、台北、新北三市市长Facebook为例],” *Journal of Shanghai* [上海交通大学学报(哲学社会科学版)], February 2018; Li Shiyan [李仕燕] and Li Zhicong [李智], “An Analysis on Cognitive Differences Between Youth of the Chinese Mainland and Taiwan on Social Media—Take the Cancellation of Hosting Rights of Taichung for East Asian Youth Games As an Example [社交媒体中的两岸青年认知差异评析——以台中市“东亚青运”主办权被取消事件为例],” *Modern Taiwan Studies* [现代台湾研究], February 2019; Liu Weichao [刘伟超] and Zhou Jun [周军], “The Analysis of Facebook Users’ Information Behavior in Taiwan: Through the Two Angles of the User and the Media [台湾地区脸书(Facebook)用户信息行为研究——基于用户和媒介的双重视角],” *Taiwan Studies* [台湾研究], March 2019; Le Yuan [乐媛] and Zhou Xiaoqi [周晓琪], “Social Media Mobilization and Inter-Media Agenda-Setting Effects of Social Movement: The Case Study of “Anti-Trade Student Movement” in Taiwan [社会运动中的社交媒体动员与媒介间议程设置效应:以台湾地区“反服贸学运”为例],” *Chinese Journal of Journalism & Communication* [国际新闻界], June 2019.

China’s disinformation campaigns.”⁷⁹ Another expert on Chinese disinformation operations said that “most of the Chinese disinformation that went mainstream in Taiwan did so via traditional media.”⁸⁰ Social media platforms enable China to repeat and amplify messages that it puts out on traditional media.

China’s access to and influence on Taiwan’s traditional print, radio, and television media have grown quite substantially in recent years. The PRC has sought to shape Taiwan’s traditional media by conditioning market access for large conglomerates on their communicating pro-unification messages through their media subsidiaries.⁸¹ China has also provided substantial advertising funds that traditional media require to survive in an increasingly competitive environment, with consequences for editorial line and content.⁸² Finally, Xinhua and other PRC state news content providers offered discounted access to valuable information that media outlets would not otherwise be able to afford, leading to foreign media outlets running Chinese state propaganda as news.⁸³

China has also funded Chinese subsidiaries of some of Taiwan’s major media groups, with Want Want China Times Media Group (hereafter referred to as Want Want), and its head, Tsai Eng-Meng, the leading target for criticism of Chinese influence in the Taiwan traditional media space.⁸⁴ In 2012, concerns that Want Want was gaining too much influence over Taiwan’s information market led to popu-

⁷⁹ Interview with former Taiwan government official, interview 4A, Taipei, January 2019.

⁸⁰ Interview with Taiwan-based think-tank analyst, interview 3, Taipei, January 2019.

⁸¹ Huang Jaw-Nian, “The China Factor in Taiwan’s Media,” *China Perspectives*, March 2017.

⁸² Huang Jaw-Nian, 2017.

⁸³ Emily Feng, “China and the World: How Beijing Spreads the Message,” *Financial Times*, July 12, 2018.

⁸⁴ Sophia Yang, “Taiwan’s Want Want Received NT\$2.8 Billion State Grant from China in 2017,” *Taiwan News*, April 23, 2019b. Tsai Eng-Meng made a fortune selling rice cracker snacks in the China market and has made numerous comments critical of democracy and laudatory of the CCP, including minimizing its responsibility for deaths stemming from the decision to use military force against protestors gathered in and around Tiananmen Square in June 1989.

lar protests and opposition party action that forced the Ma Ying-Jeou administration to block the group's efforts to purchase the Next Media Group.⁸⁵ Frustration with such firms as Want Want—which runs the newspaper *China Times* [中國時報] and the television stations CTV [中國電視公司] and CTiTV [中天電視]—and with television station TVBS [聯利媒體股份有限公司] has boiled over at times, leading popular movements and politicians alike to criticize so-called “red media” and “hatchet men” working for China.⁸⁶ Many in Taiwan see compromised traditional media as willing to shape their coverage to amplify and lend credibility to Chinese disinformation initially spread on social media platforms, serving as “repeater stations,” in the words of one interviewee.⁸⁷ The Taiwan government is investigating China's influence in local media, with President Tsai remarking that a May 2019 meeting hosted by the Chinese government with Taiwan media “proved that Beijing has been pressuring Taiwanese media outlets.”⁸⁸

To insert disinformation into the broader media environment, China often starts by gaining access to local social media or encouraging messages to migrate over to popular Taiwan social media sites from content farms in China. This requires creating social media profiles or recruiting willing participants who can fabricate or import disinformation and put it up on social media platforms, such as Facebook, LINE, or PTT. If the content originates in China, then Taiwan social media users must be alerted to such content and encouraged to upload it; increasingly, however, Taiwan interviewees expressed suspicions that China has recruited Taiwan-based content producers who will fabricate

⁸⁵ Ralph Jennings, “In Taiwan, Proposed Sale of Media Group Prompts Concern,” *Los Angeles Times*, November 29, 2012.

⁸⁶ Keoni Everington, “Taiwan's Foxconn Tycoon Calls Want Want Boss China's ‘Hatchet Man and Lackey,’” *Taiwan News*, June 27, 2019b; Stacy Hsu, “Protestors Gather in Taipei, Asking ‘Red Media’ to Leave Taiwan,” *FocusTaiwan*, June 23, 2019.

⁸⁷ Interview with Taiwan-based think-tank analyst, interview 3, Taipei, January 2019.

⁸⁸ Teng Pei-ju, “Authorities to Monitor Chinese Influence on Taiwanese Media: Tsai,” *Taiwan News*, May 12, 2019. Also see Kathrin Hille, “Taiwan Primaries Highlight Fears over China's Political Influence,” *Financial Times*, July 16, 2019; and Yimou Lee and James Pomfret, “Taiwan Steps Up Probe into Surveillance by Pro-China Media on Island,” *Channel News Asia*, January 18, 2019.

disinformation locally. A Taiwan report by the Institute for National Defense and Security Research reportedly found that “Beijing sends ‘fake news’ to its intermediaries, who then circulate the information on social networks, such as Facebook and the Line messaging app,” noting that “these efforts come in addition to buying Taiwanese-run Facebook pages and hiring local internet celebrities to launch disinformation campaigns.”⁸⁹

Although we found no Chinese military writings discussing the use of intermediaries, at least one article discussed the value of local cooperation. An October 2018 article by engineers at the PLASSF’s psychological warfare base targeting Taiwan explicitly mentions Facebook, Twitter, and LINE—the main social media platforms in Taiwan—and details the role of military-civil fusion and local support in psychological warfare.⁹⁰ The article notes that the PLA could “procure or introduce local . . . technology and equipment,” while ensuring secrecy. Although it is not entirely clear whether this is a reference to Chinese domestic civilian technology or “local” collaborators outside the country, such as Taiwan, this would align well with suspected Chinese efforts. Furthermore, because some social media websites are banned in China, PRC-based actors seeking to execute social media disinformation campaigns on such websites as YouTube and Facebook must circumvent China’s Great Firewall, and would therefore benefit from local agents who can operate on China’s behalf in a freer media environment.

By gaining access to social media sites and spreading disinformation across them, China has been able to get its messages picked up and repeated on traditional media. The effectiveness of these messages is further augmented by the shaping activities that China has undertaken through its diplomatic, economic, subversive penetration, and military activities targeted at Taiwan.

⁸⁹ Chung Li-hua and Jake Chung, “China Using Local ‘Agents’ to Spread Misinformation Online: Institute,” *Taipei Times*, August 4, 2019.

⁹⁰ Liu Huiyan [刘惠燕], Xiong Wu [熊武], Wu Xianliang [吴显亮], and Mei Shunliang [梅顺量], “Several Thoughts on Promoting the Construction of Cognitive Domain Operations Equipment in the Whole Environment [全媒体环境下推进认知域作战装备发展的几点思考],” *Defense Technology Review* [国防科技], October 2018.

Other Policy Tools That Shape PRC Social Media Disinformation Campaigns' Effectiveness

China's cross-strait policy clearly demonstrates that Beijing's intent to design an interlocking policy of compellence designed to send mutually reinforcing messages of enticement and coercion.⁹¹ The diplomatic space offers one example: Since the 2016 elections that put the Tsai administration in office, China has peeled away seven of Taiwan's diplomatic relationships: Burkina Faso, the Dominican Republic, El Salvador, Kiribati, Panama, Sao Tome and Principe, and the Solomon Islands. In the economic arena, China has waged gray-zone economic warfare against Taiwan's global identity, compelling airlines and hotel chains to list Taiwan as "Taiwan, China" if they wish to retain access to the China market. At the same time, Beijing has announced a raft of "31 Measures" designed to lure young talent away from Taiwan and signal to the people of Taiwan that their economic future lies in integration with China.⁹² Finally, the PLA has carried out numerous military exercises intended to intimidate Taiwan, including "island encirclement patrols" that circumnavigate the waters and air space around the main island, flying across the median line in the Taiwan Strait, and practicing decapitation strikes against mock-ups of the Taiwan presidential palace. Although the "31 Measures" arguably have not succeeded, they were certainly intended to reinforce memes that Chinese propagandists have been pushing on social media about Taiwan being a *ghost island* [鬼島] with no future.⁹³

Similarly, China's military exercises around Taiwan—and cross-strait provocations against it—are intended to augment such messages as the faked image of a PLAAF H-6K bomber purportedly flying within visual range of Taiwan's Jade Mountain (i.e., within Taiwan's

⁹¹ Russell Hsiao, "China's Intensifying Pressure Campaign Against Taiwan," *China Brief*, June 19, 2018b.

⁹² Simon Denyer, "Taiwan Battles a Brain Drain as China Strives to Woo Talent," *Washington Post*, April 15, 2018.

⁹³ Sophia Yang, "China's Pro-Unification 31 Measures for Taiwan Have Failed: Academia Sinica Scholar," *Taiwan News*, January 26, 2019a.

sovereign air space), suggesting that the ROC military is too incompetent to detect the PLA and/or too weak to defend against it (Figure 3.1). President Tsai has stated that although the PLA’s operations constitute a “threat,” they have not succeeded at “intimidating” Taiwan, but that is clearly the intention.⁹⁴ This reinforces our belief that any Chinese social media operation will be nested within a broader Chinese information operations campaign.

Service Spotlight: The PLAAF’s Approach to Social Media

The PLAAF is the leading experimenter for the Chinese military’s approach to social media, including for disinformation and targeted

Figure 3.1
Purported Image of Chinese Bomber Flying Near Mountains in Taiwan



SOURCE: PLA photo in “PLA Air Force Releases Apparent H-6K Photographed with Taiwan’s Jade Mountain [解放军空军发布疑似轰-6K与台湾玉山合影],” *Observer* [观察者], December 17, 2016.

⁹⁴ Yimou Lee, “Taiwan President Says Chinese Drills a Threat but Not Intimidated,” *Reuters*, April 15, 2019.

messaging campaigns directed at adversary populations. The PLAAF opened the first PLA account on Weibo and WeChat in October 2015, and now has almost 2.5 million followers on Weibo—more than any other service branch of the PLA.⁹⁵ The PLAAF was also the first to use social media for external messaging when it announced flights over the South China Sea in July 2016 and the first to reportedly engage in disinformation when it released the aforementioned image of an H-6K bomber flying close to a mountain in Taiwan.

The PLAAF's social media strategy was outlined in a speech by its spokesperson, Shen Jinke, in December 2017, when the service received an award for having one of the military's best social media accounts.⁹⁶ Shen said the intent of opening the account was to “improve [the service's] real-time provision of information, broadcasting, influence, and guidance,” which would help the PLAAF seize the “right to speak” [话语权; also translated as “discursive or agenda-setting power”].⁹⁷ Shen went on to say that “in public opinion related to the military, information is power, information is a weapon, information is confidence, information is position, and information is guidance [of public opinion].” Shen then offered three principles for the service's social media strategy, as summarized by one report: “1) seizing the right to speak by controlling the release of information and guiding public opinion through ‘positive energy’; [...] 2) operational security; and 3) promoting appealing content to help with agenda setting.”⁹⁸

The PLAAF's social media accounts generally focus on domestic-facing propaganda. Despite its forward-leaning approach to social media in general, the PLAAF still does not have any publicly identified

⁹⁵ Follower count as of June 15, 2019. See PLAAF, “Air Force Release [空军发布],” Weibo post, undated; and Ministry of National Defense of the People's Republic of China, “China Air Force Weibo, WeChat Public Account Open [中国空军官方微博、微信公众号开通运行],” November 10, 2015.

⁹⁶ Shen Jinke [申进科], “Optimize Information Provision to Lead Online Public Opinion [优化信息供给引领网络舆论],” Xinhua, December 8, 2017. This paragraph draws from Beauchamp-Mustafaga and Chase, 2019.

⁹⁷ Shen Jinke, 2017.

⁹⁸ Beauchamp-Mustafaga and Chase, 2019.

accounts on foreign social media. Much of the PLAAF's content on Weibo might be designed, at least in part, for recruitment purposes.⁹⁹ Moreover, only a few of the PLAAF's posts have any foreign-language content, mostly directed at Taiwan.¹⁰⁰

Social media also serves as a channel for deterrence signaling, especially for efforts to undermine enemy population resolve.¹⁰¹ When the 2016 international ruling on the South China Sea islands challenged China's claims, PLAAF H-6K bombers flew over Scarborough Shoal to signal China's capability and will to defend its maritime claims.¹⁰² The PLAAF released information about its flight through a Weibo post, which was then reposted by the *People's Daily* Online Twitter account.¹⁰³ Generally speaking, the PLAAF is not signaling to the United States directly via Weibo. Instead, the PLAAF uses Chinese social media, such as Weibo and WeChat, to release information mainly for domestic Chinese audiences, and that information is then picked up by Chinese state-run media and reposted to Western social media, such as Facebook and Twitter—thereby facilitating signaling to foreign English-speaking audiences. The PLAAF does not do this signaling particularly well: The State Council Information Office's tweet about the PLAAF's South China Sea flight in July 2016 received only 20 likes and retweets. This lackluster performance reflects a downside of the PLA's lack of official accounts on Western social media; it also reflects the state-run media's role in assisting the military on foreign messaging and highlights that the PLA's reach on social media is far

⁹⁹ Derek Grossman, Nathan Beauchamp-Mustafaga, Logan Ma, and Michael Chase, *China's Long-Range Bomber Flights: Drivers and Implications*, Santa Monica, Calif.: RAND Corporation, RR-2567-AF, November 2018.

¹⁰⁰ Ben Blanchard, "China Air Force Goads Taiwan with Hokkien-Language Video," Reuters, April 20, 2018.

¹⁰¹ For more on H-6K flights as deterrence signaling, see Grossman et al., 2018.

¹⁰² Scarborough Shoal is a disputed territory claimed by China, Taiwan, and the Philippines. Nathan Beauchamp-Mustafaga, Cristina Garafola, Astrid Cevallos, and Arthur Chan, "China Signals Resolve with Bomber Flights over the South China Sea," War on the Rocks, August 2, 2016.

¹⁰³ China State Council Information Office, "And Some Photos Brought by PLA Air Force," Twitter post, July 15, 2016.

greater with domestic audiences than with foreign ones. The PLAAF-published photo of the H-6K bomber flying over Scarborough Shoal reached more than 19 million people on Weibo, compared with a total of 42 users on Twitter.¹⁰⁴

The PLAAF is known to have used social media for disinformation.¹⁰⁵ In December 2016, on the second bomber flight around Taiwan, the PLAAF released an image of an H-6K in front of two mountains.¹⁰⁶ Although the PLAAF did not say where the mountains were, Chinese media speculated they were in Taiwan. After the photos were released, the Taiwan Ministry of Defense denied that the planes flew close enough to actually take such a photo and suggested that it was disinformation,¹⁰⁷ with the statement that, “[The release] is a typical act of propaganda [employed by China], and the [Taiwan] media are helping China in its ‘advertising campaign,’ . . . The goal [of the photograph’s release] is to affect Taiwanese psychologically. There will probably be another picture released tomorrow, as China is thrilled with the reaction of the Taiwanese media.”¹⁰⁸ Sure enough, on February 3, 2019, the PLAAF released a video entitled “Our Fighting Eagles Fly Circles Around Taiwan.”¹⁰⁹

¹⁰⁴These metrics measure different things but clearly indicate a wide disparity in reach. China State Council Information Office, 2016; Shen Jinke [申进科], 2017.

¹⁰⁵Some analysts have claimed that China Central Television has aired old footage of PLA live-fire exercises in an attempt to exaggerate the degree of threat Taiwan is facing. See Rachael Burton, “Disinformation in Taiwan and Cognitive Warfare,” *Global Taiwan Brief*, Vol. 3, No. 22, November 14, 2018.

¹⁰⁶For analysis of flights around Taiwan, see Nathan Beauchamp-Mustafaga, Derek Grossman, and Logan Ma, “Chinese Bomber Flights Around Taiwan: For What Purpose?” *War on the Rocks*, September 13, 2017.

¹⁰⁷Matthew Strong, “Military Denies Yushan in China Bomber Picture: Peak Likely to be Mount Beidawu in Southern Taiwan: Experts,” *Taiwan News*, December 17, 2016.

¹⁰⁸Chen Wei-han, “MND Plays Down China Aircraft Threat,” *Liberty Times*, December 19, 2016.

¹⁰⁹Aaron Tu and William Hetherington, “Defense Bureau to Tackle Propaganda from China,” *Taipei Times*, March 4, 2019.

Conclusion

China, and more specifically the PLA, appears to have been relatively slow to leverage social media for disinformation campaigns. But its activities in this space have been growing over the past three years, in the wake of the 2015 PLA reforms and the 2016 election of Tsai Ing-Wen in Taiwan. As a consequence of shared language, proximity, sociopolitical history, and aspects of the human and media terrains across the Taiwan Strait, China's greatest opportunities to leverage social media disinformation campaigns against an adversary thus far have been in Taiwan. These campaigns are explored in greater depth in the next chapter.

Case Study: Insights from Taiwan's Experience as China's Main Target for Social Media Disinformation

China's disinformation efforts directed at Taiwan generally seek to divide and demoralize Taiwan society, driving up the negative impressions associated with the government of President Tsai and creating an image of an incompetent government. It presents an impression of the Tsai administration as being out of touch with the populace and indifferent to the effects of its (purportedly incorrect) policies, driving Taiwan toward disaster, and betraying Taiwan's economic and territorial interests and its true identity. The disinformation shows the government of Taiwan and its military as weak, corrupt, and incapable of mounting a defense against the PLA; suggests that Taiwan's future is bleak or hopeless (for example, the ghost island meme mentioned in Chapter Three), and imparts a message that democracy is an "ineffective and chaotic" political system (while also judging the Tsai administration against democratic standards and finding it lacking).¹ Some Chinese disinformation is original content; other instances are repostings intended to amplify content originating from within Taiwan society. One interviewee remarked that "a lot of what China's fake news is doing is not changing minds but just reinforcing preexisting divisions and opinions,"² and another noted that "the goal of China's disinformation is to weaken trust in [our] government."³

¹ Interview with Taiwan political party activist, interview 13A, Taipei, January 2019.

² Interview with Taiwan political party activist, interview 13B, Taipei, January 2019.

³ Interview with Taiwan politician, interview 7, Taipei, January 2019.

At the same time, China seeks to convey a twofold image of the PRC to Taiwan on social media. On the one hand, it seeks to reassure those in Taiwan who believe that China is nonthreatening by conveying positive images of China as an attractive place where Taiwan businesses can succeed, jobs and opportunity abound, and Taiwan could even be subsumed as a political entity with no undue need for concern. On the other hand, Chinese information operations also strive to convince target audiences of the inevitability of unification with China. Such information operations might mask, distort, or convey an only partially true impression of China's opportunities and the prospects that Taiwan would enjoy were it to submit to Chinese rule, but they differ substantially from disinformation campaigns of the discrete sort referred to as "fake news." Some, such as the PLAAF's claimed flight near Taiwan's Jade Mountain, have been discussed already; others that are merely intended to highlight China's power and opportunities and cast these factors in a favorable light are not explored further in this report.

According to one interviewee, experts in Taiwan seem to believe that China is attacking Taiwan with as many as 2,400 separate pieces of disinformation every day.⁴ So far as we could discern, no official centralized database is publicly available in Taiwan to track and provide analysis of the content, themes, spread rate and vector, or other relevant data for these attacks. We cannot replicate or attempt to create such a database. However, in this chapter, we explore in greater detail a dozen specific examples of the kind of discrete disinformation attributed to or believed to be associated with China and targeted at Taiwan. Attribution can be difficult or impossible, so these examples should be treated as indicative of PRC propaganda (as seen by Taiwan observers) but not as definitively proven to have originated from Chinese disinformation operations.

With regard to Taiwan, China has been accused of using covert accounts for manipulating the public. For example, in the run-up to Taiwan's 2018 local elections, Taiwan media reported that "China has been creating fake social media accounts to interfere with the Nov. 24 elections as practice for manipulating the 2020 elections

⁴ Interview with Taiwan-based think-tank analyst, interview 3, Taipei, January 2019.

to elect candidates favorable toward Beijing.”⁵ A June 2019 report argued that suspected Chinese accounts were behind a Facebook group supporting Han Kuo-Yu, a Taiwan politician elected mayor of Kaohsiung (the largest city in Southern Taiwan) in 2018.⁶ The author claimed to identify specific Facebook accounts run by Chinese operators that also had fake LinkedIn profiles. Specific planted social media accounts identified on Twitter dated as far back as 2014. One investigation found “scores of fake accounts on Twitter [promoting] Beijing’s line on [Tibet].”⁷ It is difficult to know the details of this isolated incident, but we suspect these might have been sponsored by the Tibetan Autonomous Region’s propaganda department for either tourism or “public opinion warfare.”⁸

Examples of Chinese Social Media Disinformation Against Taiwan

An early example of disinformation, believed to have originated in China around mid-2016, held that the Tsai government was planning to sell out Taiwan’s national sovereignty by leasing its territory—specifically, the island of Itu Aba (also known as Taiping Island [太平島])—to the U.S. Navy for use as a firing range. The Tsai administration denied this

⁵ Chung Li-hua and Hetherington, 2018.

⁶ Chris Horton, “Candidate Seeks Closer China Ties, Shaking Up Taiwan’s Presidential Race,” *New York Times*, June 6, 2019; Paul Huang, “Chinese Cyber-Operatives Boosted Taiwan’s Insurgent Candidate,” *Foreign Policy*, June 26, 2019.

⁷ Kaiman, 2014. According to Kaiman, the human rights NGO Free Tibet “found that the fake accounts had overlapping qualities. Most of their names were comprised of two Western-sounding first names strung together. About 90 of them were also closely intertwined—they followed one another and frequently retweeted each other’s posts, often identical statements and links.” For more recent research, see Gillian Bolsover, “Computational Propaganda in China: An Alternative Model of a Widespread,” Computational Propaganda Research Project, April 2017.

⁸ Tang Dashan, “Tibet Should Build a Major External Propaganda Structure,” *Tibet Daily*, September 14, 2013, p. 3.

on multiple occasions, with former Minister of Defense Feng Shih-Kuan even having to repudiate it in hearings at the Legislative Yuan.⁹

Our second example, from summer 2017, is a rumor, ultimately traced to a PRC content farm, spread on Taiwan's social media platforms that the Tsai administration planned to ban both the burning of traditional "ghost money" and incense and the setting off of firecrackers out of environmental concerns.¹⁰ This ultimately led to an estimated 10,000 people marching in Taipei, protesting the purported ban as a violation of traditional Taoist, Buddhist, or other religious or cultural values, and helped to set an early example of how Beijing might use disinformation to impose costs on and undercut political support for its rival.¹¹

A third example that many Taiwan interviewees remarked on involved a rumor that spread on the PTT bulletin board in May 2018 alleging that the foreign minister of Honduras, a country that has diplomatic relations with Taiwan, was in Beijing to negotiate a switch in recognition. The ROC Foreign Ministry was forced to double-check and even took the extraordinary step of requesting a meeting and a photo with the Honduran foreign minister with Taiwan's ambassador to demonstrate that the rumor was false, wasting precious time and resources to combat a story that had no point other than to play on fears of Taiwan's diplomatic isolation, which were spiking in the weeks after the loss of recognition by Burkina Faso.¹²

A fourth example of Chinese disinformation came in the wake of the Taiwan government's decision to finally undertake long-delayed pension reforms for school teachers, public employees, and the military in summer 2018. In this instance, Chinese disinformation suggested that the cuts to benefits would be even broader (affecting more people)

⁹ "News That US Could Rent Itu Aba Is 'Fake,' Institute Says," *Taipei Times*, July 1, 2018.

¹⁰ Cole, 2017; "Authorities Deny Rumor of Ban . . .," 2017.

¹¹ "Taiwan's Taoists Protest Against Curbs on Incense and Firecrackers," BBC News, July 23, 2017.

¹² Interview with Taiwan government official, interview 15, Taipei, January 2019. Also see Keoni Everington, "Honduras Denies Rumors of Talks with Beijing on Cutting Ties with Taiwan," *Taiwan News*, May 28, 2018a.

and deeper (reducing incomes more steeply) than was actually the case, putting downward pressure on public support for the Tsai administration.¹³ One high-ranking government official even commented that his own mother had initially believed the disinformation and called him, worried about her own pension and economic security.¹⁴

Our fifth example illustrates how China also used disinformation to amplify accusations of inappropriate partisanship on the part of the Taiwan president while she was traveling abroad. When President Tsai stopped in Los Angeles en route to visit Taiwan's diplomatic partners in Latin and South America in August 2018, a false rumor spread that the Taiwan Economic and Cultural Office—Los Angeles had been ordered to ban those greeting the president from waiving the Taiwan flag, instructing them instead to display only the DPP flag.¹⁵ Although not definitively tied back to China, this story might have been deliberately amplified by PRC repostings. Indeed, one Taiwan official commented that officials had been forced to respond to a grand total of seven false stories in a single day during the president's trip, consuming an enormous amount of time and resources on the part of senior government officials.¹⁶

In a sixth example of possible Chinese disinformation, when Typhoon Jebi hit Osaka, Japan, and stranded thousands of tourists at Kansai International Airport, a fabricated story spread on the social media blog PTT that Su Chii-Cherng, the director of the Taipei Economic and Cultural Representative Office (Taiwan's unofficial vehicle for managing bilateral issues), did nothing to help stranded Taiwan citizens, while the PRC consulate in Osaka dispatched buses to rescue the trapped Taiwan citizens. Shortly after the story began circulating, Su came under intense criticism online, ultimately hanging himself. Since his death, there have been conflicting accounts about his motivations: The Ministry of Foreign Affairs claims that his suicide note blamed

¹³ Russell Hsiao, "CCP Propaganda Against Taiwan Enters the Social Age," *China Brief*, Vol. 18, No. 7, April 24, 2018.

¹⁴ Interview with Taiwan government official, interview 16, Taipei, January 2019.

¹⁵ Interview with Taiwan government official, interview 15, Taipei, January 2019.

¹⁶ Interview with Taiwan government official, interview 15, Taipei, January 2019.

the disinformation about his office's incompetence and indifference as the reason for his action; his family said his action was because of criticism he received from the ministry over insufficient assistance to the citizens at the airport.¹⁷ The ministry has denied wrongdoing but has been criticized by some in Taiwan's legislature for its handling of Su and the aftermath.¹⁸ Regardless, the Taiwan government has found no evidence to support the original rumors of Chinese assistance, making this another case of disinformation.¹⁹ The origins of this disinformation, however, highlight the challenges of definitive attribution. In our discussions with Taiwan researchers in January 2019, the prevailing wisdom was that this was a case of Chinese-originated disinformation. However, in December 2019, two Taiwan citizens were charged with creating and spreading the rumor.²⁰ Although China might have played a role in furthering the rumor's spread, that remains unclear as of this report's publication.

Our next two examples indicate that not all Chinese activities on social media are premised on creating fake content. Some serve, instead, to repeat, augment, swamp, and thereby raise the profile of the criticisms against a given person, position, or issue. In 2015, before Tsai Ing-Wen was elected, her Facebook page was "flooded" with PRC-based postings demanding that Taiwan "reunify" with China.²¹ Immediately following Tsai's election, Chinese web users again sought to deluge the

¹⁷ For an early report linking his death to the disinformation, see Ko Tin-yau, "How Fake News Led to Suicide of Taiwan Representative in Osaka," *EJInsight*, September 19, 2018. For the statement from his family, see Joseph Yeh, "Foreign Ministry Denies Reported Plan to Punish Late Diplomat," *Focus Taiwan*, December 21, 2018.

¹⁸ Hsieh Chun-lin, Lu Yi-hsuan, and Jake Chung, "Control Yuan Members Blast Su Report," *Taipei Times*, May 24, 2019.

¹⁹ "Resolution Calls for Hsieh Briefing on Diplomat's Death," *Taipei Times*, December 25, 2018.

²⁰ Keoni Everington, "Slow Yang Charged with Spurring Suicide of Taiwanese Diplomat in Japan with Fake News," *Taiwan News*, December 2, 2019c.

²¹ "Taiwan Opposition Leader Tsai Ing-Wen's Facebook Page Flooded with Posts from the Mainland," Reuters, November 12, 2015.

Taiwan president-elect's Facebook page with similar demands.²² And when the southern Taiwan city of Kaohsiung was literally flooded in October 2018, a man posted two false claims on his Facebook page alleging that Tsai had been accompanied on her damage assessment tour by soldiers with live ammunition, a comment that led to his arrest after the government assessed this as having damaged Tsai's image.²³ Numerous interviewees related that they believed China-linked web-pages and accounts had recirculated this news item so as to elevate its profile and expand its impact.²⁴ Such opportunistic repostings take advantage of domestic discontent or content fabrication—such as a recent discredited story alleging that Premier Su Tseng-Chang had disrespectfully flung away the pencil he used to sign the condolences book at the funeral of a Taiwan policeman²⁵—to make these stories seem more widespread and deep than the circumstances actually are.

A ninth instance of social media manipulation involves widespread suspicions that China funded and promoted the election of Kaohsiung Mayor Han Kuo-Yu in November 2018. These suspicions have recently been given added credibility thanks to reports identifying PRC-linked accounts that sought to create an impression of an insurgent wave of support.²⁶ Han subsequently became one of the leading candidates for the KMT's nomination for the presidency in 2020, and allegations that China might have manipulated underground political betting markets to create an impression of momentum and inevitability have also circulated.²⁷ In the run-up to the 2018 Kaohsiung may-

²² "Chinese Flood Taiwan President-Elect's Facebook, Demanding Return to China," Reuters, January 21, 2016.

²³ Matthew Strong, "Taiwan Police Detain Man for Spreading Fake News About President," *Taiwan News*, October 6, 2018.

²⁴ Interview with Taiwan-based think-tank analyst, interview 3, Taipei, January 2019.

²⁵ Matthew Strong, "Taiwan Police Find Author of Fake Video about Premier Su Tseng-Chang," *Taiwan News*, July 10, 2019.

²⁶ Interview with Taiwan-based think-tank analyst, interview 3, Taipei, January 2019 (we also heard this in other interviews); Keoni Everington, "Chinese Cybergroup Behind Kaohsiung Mayor's Win Uncovered," *Taiwan News*, June 27, 2019a; Huang, 2019.

²⁷ Interview with Taiwan-based think-tank analyst, interview 3, Taipei, January 2019.

oral election (and in the months since then), Han received heavy and favorable coverage in PRC media sources, many of which are available in Taiwan and/or circulated via social media—and, therefore, can help shape impressions of the candidate among Taiwan voters.²⁸

The Kaohsiung mayoral contest also gave rise to our tenth example: disinformation intended to damage the prospects of the incumbent mayoral candidate, Chen Chi-Mai, who was accused first on PTT and later on *Apple Daily* of having worn an earpiece during the public debates.²⁹ In October 2018, Chen's lawyers informed reporters that they "had evidence that misinformation defaming Mr. Chen that had spread widely on Taiwan social media had originated from overseas accounts."³⁰ Although not necessarily a direct consequence of such disinformation alone, Chen went on to lose the election to Han Kuo-Yu, who on July 15, 2019, went on to be named the KMT's 2020 presidential candidate.

An eleventh instance of media manipulation involves stories circulated on PTT that the Tsai administration had not effectively handled an outbreak of African swine fever in China because its cross-strait policy led Beijing to isolate it from the World Health Assembly and other medical and health information exchange fora. Taiwan pig farmers were extremely concerned when a dead pig infected with the disease washed up on the shore of Kinmen Island in late 2018, leading to fears that Taiwan's 5.39 million hogs could share the fate of 600,000 of their fellow swine across the Taiwan Strait that had to be culled in China in 2018.³¹ Taiwan has subsequently raised the fines for bringing pork products into the country from China, but the anxiety levels of

²⁸ Interview with Taiwan-based think-tank analyst, interview 3, Taipei, January 2019.

²⁹ J. Michael Cole, "That's What 'Fake News' Looks Like and What It Does to Democracy," *Taiwan Sentinel*, November 12, 2018.

³⁰ Horton, 2018.

³¹ I-fan Lin, "Taiwan's Battle Against Swine Fever Gets Political on PTT," *The News Lens*, January 11, 2019.

local farmers purportedly remained high, and fear of disinformation related to animal diseases remains a concern.³²

Our final example stems from March 2019, when CTiTV reported a case of disinformation that some of our interviewees suspected might have originated with Chinese disinformation. During an interview with a farmer in Tainan (one of the main cities in southern Taiwan), CTiTV reported as true a claim by the farmer that one consequence of the Tsai administration's refusal to acknowledge the "1992 Consensus"³³ was that Beijing refused access to some Taiwan agricultural produce, leading prices for pomelos (a type of tropical fruit akin to a sweet grapefruit) to drop so low that local farmers had opted to dump more than 2 million tons of the fruit into a local reservoir to rot rather than try to sell their products elsewhere. The story aired just ahead of a local by-election in which the DPP, traditionally the dominant party in Tainan, barely retained the seat, leading to speculation that the news was intended to affect the outcome of the electoral contest.³⁴

Conclusion

Overall, the themes that come out of these dozen instances of disinformation are highly political in nature. Indeed, with the exceptions of the instances of the PLAAF flight purporting to occur within visual range of Jade Mountain and the possible reposting of the ROC Army tank disaster noted in the previous chapter, our interlocutors were unable to identify specific instances in which China had targeted the ROC armed forces with disinformation. As one interviewee commented, "the PLA is

³² Central News Agency, "Sharers of Fake News About Animal Diseases Face Fines in Taiwan," *Taiwan News*, June 27, 2019.

³³ The "1992 Consensus," refers to the tacit agreement between Taiwan and China that the two sides of the Strait both belong to one China, leaving unspecified which "China" they belong to.

³⁴ Shelley Shan, "CtiTV Penalized Another NT\$1M for Pomelo Story," *Taipei Times*, April 11, 2019.

attacking our military through our population.”³⁵ Another defense official agreed, stating that “the PLA is mostly carrying out cyberattacks on [our military] in tandem with more-conventional military operations and psychological warfare. This is because the ROC armed forces are not allowed to use social media while on base.”³⁶

The vagueness and ambiguity surrounding the origins of online information also feeds an impression that China might be behind any or even every instance of disinformation. This has two effects. First, it can magnify China’s apparent power, further adding to the sense that Taiwan is besieged and outmatched. On the other hand, China is not necessarily behind every instance of disinformation online in Taiwan, but this impression can provide those who are more favorable toward engagement with China—or those who are deliberately seeking to muddy the waters on China’s behalf so as to complicate attribution—an opportunity to paint those who think China is involved as conspiracy theorists or as biased against China.

Similar to efforts to parse Russia’s social media activities, it is difficult to precisely identify the actual impact and effectiveness of China’s campaign on social media, and it is especially difficult to disaggregate the social media sphere from China’s broader information campaign and even overall influence operations. China has clearly targeted President Tsai’s popularity in Taiwan, but Chinese disinformation campaigns are only one factor affecting Tsai’s approval ratings.³⁷ China’s purported disinformation efforts have generated some real-life protests in Taiwan, such as the 2017 rumor about banning ghost money bringing 10,000 people into the streets.³⁸ Perhaps the most important impact, however, is much like that of Russian activities—simply questioning the veracity of news and political statements could lower overall trust in Taiwan society and aggravate sociopolitical divisions.

³⁵ Interview with Taiwan government official, interview 18, Taipei, January 2019.

³⁶ Interview with Taiwan think-tank analyst, interview 2A, Taipei, January 2019.

³⁷ “Polls Show Taiwanese Public Indifferent to Tsai: Poll Expert Michael You,” *Taiwan News*, May 25, 2019.

³⁸ “Taiwan’s Taoists Protest . . .,” 2017.

In response to this Chinese activity, the Taiwan government and broader society have adopted several steps against disinformation, but the effect has yet to be truly tested. First, the government has sought to quickly identify and respond to suspected disinformation.³⁹ Second, it has encouraged greater public awareness and media literacy, in part through a greater willingness to attribute at least the problem of disinformation (though perhaps not specific instances of online disinformation activity) to China.⁴⁰ Third, it has increased prosecutions under relevant existing legislation and has proposed further expanding them, and the Taiwan legislature passed a finalized bill in December 2019 in the run-up to the January 2020 presidential election.⁴¹ Fourth, it has considered banning some Chinese-owned applications, such as iQiyi and Tencent Video, though it is unclear whether a final decision has been reached.⁴² Some legislators have proposed increasing the existing penalties for spreading disinformation online and proposed various new bills, such as the Digital Communications Act, that might place some responsibility with tech companies, but much of this legislation is opposed by other lawmakers, some Taiwan journalists, and the platforms themselves.⁴³

Taiwan civil society has also been an important contributor. Two fact-checking groups, CoFact and the Taiwan FactCheck Center, pro-

³⁹ For an interview with Taiwan's digital minister on how Taiwan is responding, see Steven Butler and Iris Hsu, "Q&A: Taiwan's Digital Minister on Combatting Disinformation Without Censorship," Committee to Protect Journalists, blog post, May 23, 2019.

⁴⁰ For example, see Lawrence Chung, "Taiwan 'at the Front Line of Threats' from Beijing, Tsai Ing-Wen Tells US Think Tanks," *South China Morning Post*, April 9, 2019a.

⁴¹ Lawrence Chung, "Taiwan Gets Tough over Fake News Blamed on Beijing 'Disrupting Its Democracy,'" *South China Morning Post*, July 27, 2019; Ralph Jennings, "Taiwan Seeks to Rein In Freewheeling Media with Tougher Anti-Fake News Laws," *Voice of America*, April 22, 2019b; Yimou Lee and Fabian Hamacher, "Taiwan Passes Law to Combat Chinese Influence on Politics," Reuters, December 31, 2019.

⁴² Edward White, "Taiwan Warns of 'Rampant' Fake News amid China Interference Fears," *Financial Times*, April 2, 2019.

⁴³ Jane Rickards, "The Battle Against Disinformation," *Taiwan Business Topics*, American Chamber of Commerce in Taipei, August 21, 2019; Tseng Wei-Chen, "Lawmaker Seeks Detention for Spreading Fake News," *Taipei Times*, June 10, 2018.

vide neutral third-party analysis for citizens independent of the government. Chinese disinformation has also been politicized in Taiwan; so far, it has mostly been seen to support KMT candidates and disadvantage the DPP. This has made legislative solutions more difficult but not impossible. As for tech companies, Taiwan interlocutors relayed that they have received minimal support so far in addressing what they view as a crisis that is impossible to solve without an integral role played by the platforms themselves.⁴⁴

Having explored the themes that can be derived from the Taiwan case, we next turn to an examination of whether China appears to be actively employing disinformation campaigns against other countries in the Indo-Pacific, focusing specifically on the cases of Singapore, the Philippines, and Japan.

⁴⁴ Interviews with Taiwan government officials, interviews 10A, 10B, and 10C, Taipei, January 2019.

Regional Experiences and Responses to Chinese Disinformation

China's efforts to spread disinformation in Taiwan appear widespread. Are these efforts unique to Taiwan? How active is China in other parts of the Indo-Pacific? How have other countries responded? To answer this, we looked at countries with alliances or close partnerships with the United States, focusing on Singapore, the Philippines, and Japan. In addition to being in close relationships with the United States, each either currently hosts USAF platforms in the Indo-Pacific or might be asked to permit transit and overflight, refueling and reprovisioning, or facility access at some point in the future.¹ Singapore and the Philippines are also multiethnic nations; Japan and the Philippines are liberal democracies; and all three nations possess some potentially exploitable vulnerability that could provide fertile ground to Chinese disinformation campaigns on social media. We conducted field research in all three countries, speaking to more than two dozen officials, scholars, representatives from the tech community, and journalists.² Our objec-

¹ For broader though short surveys of other Asian countries' responses to the issue of disinformation, see Daniel Funke and Daniela Flamini, "A Guide to Anti-Misinformation Actions Around the World," Poynter, August 2019; Ralph Jennings, "In the Name of 'Fake News,' Asian Governments Tighten Control on Social Media," *Los Angeles Times*, February 8, 2019; and Ishan Joshi, "Fighting Fake News in Asia," Asia News Network, August 28, 2019.

² Field research in Japan was conducted in Tokyo in January 2019 and via email correspondence. Field research in Singapore and the Philippines was conducted in May 2019. All interviews were conducted anonymously to protect the identity of our interlocutors. Although government officials are referred to as such, all other interviewees are referred to as *political/defense analysts*.

tive was to determine to what extent, if any, China was engaged in spreading disinformation via social media.

We did not find much evidence that China is engaged in propagating or spreading disinformation on social media or digital platforms in these three countries the way it appears to be doing in Taiwan. Disinformation operations exist in all three countries, but evidence suggests that these are largely domestic in origin and done for political purposes. This is not to say that China is not attempting to increase its influence in these countries; quite the contrary, China appears to be active in all three countries but is engaging in influence operations through other methods. In Singapore, there are rumors of Chinese agents of influence and sympathizers presenting in different parts of society, and it is believed that Beijing is attempting to play up ethnic Chinese sentiments to sway public opinion. In the Philippines, China is not only attempting economic penetration and suspected of influencing traditional media, it is also focused on cultivating a positive image via diplomatic and political means and elite capture.³ In Japan, there is little evidence of Chinese activity, but there are rumors of penetration in legitimate businesses. In all three countries, there is evidence of UFDW proxy groups at work.

This chapter is organized by country with three sections for each. In each country's first section, we examine potential exploitable vulnerabilities. In the second section, we address evidence of disinformation campaigns and whether they are connected to Chinese efforts. In the last section, we examine how these countries are responding to the perceived threat of disinformation. We then conclude with some findings.

Singapore

Possible Vulnerability: Multiculturalism

Prior to independence, Singapore was colonized by the United Kingdom (1819–1942; 1946–1963) and Japan (1942–1945); later, it was

³ *Elite capture* can be defined as efforts by China to “buy” local officials’ support through development or business deals that directly benefit that officials’ community or even bribes.

part of the Federation with Malaysia (1963–1965). Throughout this time, the major ethnic groups were segregated, each assigned its own area in which to live and work.⁴ This segregation came to a head as poor living conditions and high unemployment led to ethnic tensions that erupted into race riots in 1964. The riots, in which ethnic Chinese and Malays clashed, began July 21 and ended August 2, during which time 3,568 people were arrested, 23 people were killed, and 454 were injured.⁵ A shorter riot occurred on September 3, when 1,439 people were arrested, 13 were killed, and 106 were injured.⁶

These riots played a contributing factor to Singapore's separation from Malaysia in June 1965. Singapore's new government, led by Lee Kuan Yew, wanted to avoid similar problems. The new independent Singapore "was a disoriented mess fraught with racial tensions between the Chinese and Malay, with no common cause for unity and had little sense of its own history."⁷ The solution was to create a new identity that could pacify the underlying racial tensions. Lee's government took multiculturalism as the new state's guiding mantra. On the day of Singapore's founding, Lee declared, "This is not a Malay nation; this is not a Chinese nation; this is not an Indian nation. Everyone will have his place: equal language, culture, religion."⁸ This was built into Singapore's constitution, where Article 152 states that the government has a responsibility to constantly "care for the interests of the racial and religious minorities in Singapore."⁹ Lee and his successors have all strived to build and protect "a multicultural, secular, meritocratic

⁴ Public Service Division (Singapore), "Cultivating a Harmonious Society, Becoming One People," Prime Minister's Office, undated.

⁵ Jamie Han, "Communal Riots of 1964," Singapore Infopedia, undated.

⁶ Han, undated.

⁷ "Bella," "The Myth of Multiculturalism in Singapore," *Medium*, June 3, 2017.

⁸ Walter Sim, "The Race Issue: How Far Has Singapore Come?" *Straits Times*, November 8, 2015.

⁹ Constitution of the Republic of Singapore, Article 152, August 9, 1965.

nation in which all Singaporeans are equal before the law regardless of race, language or religion.”¹⁰

Today, multiculturalism is ingrained in the Singaporean psyche. As of June 2018, Singapore’s population comprised three main ethnicities plus a host of smaller ones. Ethnic Chinese make up the largest, at 74.3 percent of the population, with ethnic Malays at 13.4 percent, Indians at 9 percent, and other ethnicities making up the remaining 3.2 percent.¹¹ The largest of those other groups is Eurasian, which makes up less than 1 percent of the population.¹² Given that ethnic differences were a source of societal instability before, including small riots in 1969 and 2013, multiculturalism could prove problematic again. Singaporean leadership is aware of this danger: Prime Minister Lee Hsien Loong said in 2015 that, regardless of the progress that Singapore has made, it would be “complacent and dangerous” to be lulled into a false sense that racial and religious matters are not the divisive issues they once were.¹³ Striking a similar note, a Singaporean official we interviewed said, “We are aware this peace is fragile and anything could set it off again.”¹⁴

Singaporean officials are concerned that ethnic differences will be manipulated by an external actor for purposes of stoking instability. The purpose of such actions could be to “undermine the Republic’s values such as multiracialism and multiculturalism,”¹⁵ or to “prey on racist sentiments.”¹⁶ Ethnic Chinese make up a large percentage of the Singaporean population and, unlike other ethnic groupings, they are organized into clan associations. These conditions could provide fertile

¹⁰ Public Service Division, undated.

¹¹ Department of Statistics (Singapore), *Population Trends 2018*, Ministry of Trade and Industry, September 2018, p. 5.

¹² “Faces of Singapore,” VisitSingapore.com, undated.

¹³ Sim, 2015.

¹⁴ Interview with Singapore government official, Singapore, May 14, 2019.

¹⁵ Kelly Ng, “The Big Read: In an Era of Fake News, the Truth May Not Always Be out There,” *Today*, June 2, 2017.

¹⁶ Rachel Au-Yong, “Facing Up to Fake News: Why We Should Be Worried,” *Straits Times*, December 4, 2016.

ground for China to exert influence via the spread of disinformation—for example, by spreading messages in Mandarin that appeal to those with Chinese ethnicity. Disinformation campaigns could be designed to cause societal chaos and make Singapore ungovernable, thereby making it difficult for the United States to operate from there.

Evidence of External Activity Lacking

Facebook and WhatsApp are the largest social media platforms in Singapore. But the Singaporean government did not pay close attention to the issue of disinformation until 2016,¹⁷ when two events changed that focus. The first was the U.S. presidential election. For Singapore, this effect of disinformation was worrisome because the general view was, “if it can happen in the U.S., . . . it could happen anywhere,” including in Singapore.¹⁸ The second event was an incident that began on November 23, 2016, when a Singapore-bound cargo ship carrying nine Singapore Armed Forces armored Terrex Infantry Carrier Vehicles was seized by Chinese customs officials in Hong Kong on its journey back from a military training exercise in Taiwan.¹⁹ Accused of not having the proper license, the Terrex vehicles were detained by customs officials and not released until January 2017.²⁰ Following the seizure, China’s Foreign Ministry demanded that Singapore “stick to the One China principle” and voiced its opposition to “any forms of official interaction” with Taiwan, including military exchanges and cooperation.²¹ What raised concerns about the spread of disinformation, however, was the fact that,

¹⁷ For an overview of China’s broader influence operations in Singapore, see Russel Hsiao, “A Preliminary Survey of CCP Influence Operations in Singapore,” *China Brief*, Vol. 19, No. 13, July 16, 2019b.

¹⁸ Interview with Singapore government official, Singapore, May 2019.

¹⁹ Alan Chong and David Han, “Foreign Policy Lessons from the Terrex Episode,” *RSIS Commentary*, No. 22, February 2, 2017; “Terrex: Hong Kong to Return Singapore Army Vehicles,” BBC, January 25, 2017.

²⁰ Bernard F. W. Loo, “Making Sense of the Terrex Incident,” *Today*, December 6, 2016; Royston Sim, “Hong Kong to Return 9 SAF Terrex Vehicles to Singapore: Ministry of Foreign Affairs,” *Straits Times*, January 24, 2017.

²¹ “Foreign Ministry Spokesperson Geng Shuang’s Regular Press Conference,” Ministry of Foreign Affairs (China), November 28, 2016.

shortly after this seizure, Singaporean authorities noticed an uptick in negative online activity regarding Singapore—largely on Chinese-language platforms. This included an increase in Chinese-language op-eds that both expressed negative views about Singapore and questioned Singapore’s relationship with Taiwan.²² This online commentary featured subtle discussions about making sure Singapore was “making right decisions” about its relationships.²³ A *Global Times* article, for example, warned that Beijing could adjust its policies toward Singapore, which might “profoundly impact Singapore’s economy.”²⁴

Shortly after the Terrex seizure, and extending through February 2017, a series of YouTube videos were posted online. The high-quality videos, posted in both simplified and traditional Chinese-language characters, questioned whether the Singapore government has a correct understanding of Singapore-China relations.²⁵ Because these videos were only in Chinese (and because no other videos were ever created that were in English or targeted other ethnic groups or religions), it is believed they were meant to target Singapore’s clan associations.²⁶ Because of the large volume of videos released, Singapore officials’ main concern was whether these videos were spreading in closed social groups and having an effect on trust in both the government and military.²⁷

There have not been many cases of deliberate disinformation activity in Singapore. One of the best known involved a hoax photograph that showed a collapsed roof at a housing complex that led to the immediate dispatch of Singaporean responders.²⁸ Others involved false reports of Lee Kuan Yew’s death, a collision between two trains, on-

²² Interview with Singapore political/defense analyst, Singapore, May 2019; interview with Singapore government official, Singapore, May 2019.

²³ Interview with Singapore political/defense analyst, Singapore, May 2019.

²⁴ Ai Jun, “Singapore’s Hypocrisy Exposed by Seized Military Vehicles,” *Global Times*, November 27, 2016.

²⁵ Interview with Singapore government official, Singapore, May 2019.

²⁶ Interview with Singapore political/defense analyst, Singapore, May 2019.

²⁷ Interview with Singapore government official, Singapore, May 2019.

²⁸ Au-Yong, 2016.

the-spot cash fines for traffic summons, and fines at local restaurants for leaving used tissues in food bowls.²⁹ All of these are believed to be domestic in origin and to be attempts to discredit the government. Similarly, several websites have been known proliferators of disinformation, such as *The Real Singapore*, *States Times Review*, and *All Singapore Stuff*. *The Real Singapore*—now shut down after its executives were found guilty on sedition charges—“thrived on fabricated articles, some of which attempted to sow discord between Singaporeans and foreigners.”³⁰ Similarly, *States Times Review*—run by a Singaporean political activist based in Australia—posted inflammatory posts on Facebook about Lee Hsien Loong.³¹ Although articles occasionally claim that foreign state actors are responsible for spreading disinformation in Singapore, there is no evidence to support these claims.³² This is largely because the media environment is overseen by the Singaporean government.

Response to Perceived Disinformation

Singapore has several laws that aim to prevent the incitement of racial and religious discord and other laws that deal with libel and defamation. But these regulations were insufficient to check the speed and ease with which disinformation spreads across social media platforms. Concerned about the impact that this spread could have on Singapore’s racial harmony and social stability, the government initiated proceedings to combat disinformation activities. In September 2018, the Select Committee on Deliberate Online Falsehoods made 22 recommendations that were meant to fulfill five primary aims:

²⁹ For a good list of other, less reported disinformation, see Kuan Yung Teng, “10 ‘Fake News’ Hoaxes That Went Viral In Singapore,” Must Share News, April 19, 2017.

³⁰ Au-Yong, 2016.

³¹ Casandra Wong, “Singapore Cannot Count on Social Media Platforms to Protect It from Fake News: Edwin Tong,” Yahoo News, November 20, 2018.

³² For example, see Jonathan Head, “Outlaw or Ignore? How Asia is Fighting ‘Fake News,’” BBC, April 4, 2018.

1. Nurture an informed public through education and accurate journalism.
2. Reinforce social cohesion and trust by providing timely clarifications and information.
3. Promote speedy fact-checking.
4. Disrupt online falsehoods through legislation and through more proactive efforts by technology and social media companies.
5. Deal with threats to national security and sovereignty against state-sponsored disinformation operations.³³

The recommendation focused on legislative responses proved the most controversial. Passed in May 2019, the Protection from Online Falsehoods and Manipulation Law gives the government the ability to request that online platforms (i.e., not individual users)—whether they are traditional media or social media—either (1) post corrections of statements that the government deems to be demonstrably false and against the public interest or (2) remove those posts, should corrections not be issued.³⁴ If the platform refuses to take either step, the government can block the website or take it to court.³⁵ The law is meant to cover statements of facts, not academic discourse, opinions, criticism, satire, or parody.³⁶ The law also bans the use of fake online accounts and bots. Failure to comply could bring fines and imprisonment, but these apply only in cases of deliberate intent—i.e., knowing the content

³³ Royston Sim, “Select Committee Releases 22 Proposals to Combat Fake News,” *Straits Times*, September 21, 2018.

³⁴ Parliament (Singapore), Protection from Online Falsehoods and Manipulation, Bill Number 10/2019, April 1, 2019; interview with Singapore defense/political analyst, Singapore, May 2019. For a good summary of the key points of the bill that eventually became law, see Lim Min Zhang, “Fighting Fake News Here with Legislation,” *Straits Times*, May 13, 2019.

³⁵ Author email correspondence with Singapore government official, June 2019.

³⁶ Cara Wan, “No Need to Be Overly Worried About Fake News Laws, Says Ong Ye Kung,” *Straits Times*, April 29, 2019. Our field research found examples that the government gave as applicable under the new law to be debatable as opinions rather than facts (for example, op-eds or posts that complain about emergency room waiting times being too long).

that was shared was false.³⁷ It is even legally applicable to closed platforms, including online chat groups (such as LINE) and social media groups that feature applications with end-to-end encryption (such as WhatsApp).³⁸ The law was widely criticized by Singapore-based academics, journalists, and tech companies, who declared it to be unnecessary, at best, or, worse, a tool giving the government an enormous amount of power to decide what information is true or false and thus what gets taken down, blocked, or corrected, thereby stifling freedom of speech and expression.³⁹

In addition to this, the government runs an information literacy campaign called S.U.R.E. (Source, Understand, Research, and Evaluate) that aims to educate primary and secondary school students about how to evaluate content trustworthiness.⁴⁰ Begun in 2013, the campaign

³⁷ Interview with Singapore political/defense analyst, Singapore, May 2019; author email correspondence with Singapore government official, June 2019.

³⁸ Although applicable, the government cannot enforce the law in these private groupings because of the inability to monitor these discussions. If, however, something deliberately fake was shared publicly and the individual knew it was fake, then the government could enforce the law, including prosecution of the individual. Interview with Singapore government official, Singapore, May 2019; interview with Singapore political/defense analyst, Singapore, May 2019.

³⁹ Kirsten Han, "Why Singapore's Moves to Curb 'Fake News' May Backfire," *Washington Post*, March 5, 2018; Hillary Leung, "Singapore Is the Latest Country to Propose Tough Legislation Against Fake News," *Time*, April 2, 2019; "Singapore Fake News Law a 'Disaster' for Freedom of Speech, Says Rights Group," *The Guardian*, May 9, 2019; Michelle Toh, "Google Says Singapore Risks Hurting Innovation with Fake News Law," CNN, May 9, 2019; Tessa Wong, "Singapore Fake News Law Polices Chats and Online Platforms, BBC," May 9, 2019.

⁴⁰ S.U.R.E. Campaign, "About Us," National Library Board, undated. The program focuses on four concepts:

Source: Look at its origins. Are they trustworthy? Make sure that the source of information is credible and reliable.

Understand: Know what you're reading. Search for clarity. Look for facts rather than opinions. Question personal biases.

Research: Dig deeper. Go beyond the initial source. Investigate thoroughly before making a conclusion. Check and compare with multiple sources.

Evaluate: Find the balance. Exercise fair judgement. Look from different angles. There are at least two sides to every story.

today includes training in how to recognize disinformation.⁴¹ The government has also set up a website, called *Factually*, that aims to clarify widespread or common misperceptions of policies or other matters of public concern.⁴² The Singapore Police Force also manages an inoculation campaign meant to make people more-critical consumers of online content. Finally, there are various nongovernmental literacy efforts. The Media Literacy Council—an organization that works with industry, educators, parents, and the government on public education and awareness programs related to media literacy and cyber wellness—runs an annual campaign to educate internet users about how to identify and resist fake content and disinformation.⁴³ An alliance of regional media companies, including the *Straits Times*, attempts to raise awareness about disinformation and help people become better-informed consumers of online content.⁴⁴ Despite the fear of disinformation efforts to exploit Singapore’s multiculturalism, none of the examples we encountered in our research appeared to originate with China, nor did any target Singapore’s multicultural nature and interethnic communal relations. They did, however, carry the potential to affect Singapore’s governability. Singapore worries about its people’s “trust” in government; if trust is lost, one Singaporean government official we spoke with said, “governance hurts.”⁴⁵ The disinformation cases skirt the edges of this trust issue, calling into question situations that might collectively reduce citizens’ faith in their government. Still, the lack of widespread disinformation campaigns and with Singapore’s proactive efforts on this front suggest that the government wants “to be ahead of the curve.”⁴⁶ Although the existing examples of disinformation do not target ethnic seams, they could affect social trust. On the government side, one official we interviewed said that trust is important

⁴¹ National Library Board (Singapore), “Fact-Checking Using Multiple Sources,” webpage, undated.

⁴² Government of Singapore, *Factually*, website, undated; Ng, 2017.

⁴³ Ng, 2017.

⁴⁴ Shefali Rekhi, “ST to Share Insights from Fight Against Fake News,” *Straits Times*, October 26, 2017.

⁴⁵ Interview with Singapore government official, Singapore, May 2019.

⁴⁶ Interview with Singapore government official, Singapore, May 2019.

“to maintain social cohesion.”⁴⁷ Government efforts, particularly the legislative measures, are “meant to be preventative steps put in place before the threats get really problematic to harmony in Singapore.”⁴⁸

The absence of Chinese disinformation activity does not mean that China is not seeking influence in Singaporean society. Although the government has not detected direct connections in Singapore’s clan associations with the Chinese government or its agents of influence, a report published by the Jamestown Foundation argues that Beijing is using clan associations—as well as business associations, youth programs and Chinese-language media outlets—to sway public opinion and policy in Singapore into alignment with the interests of the CCP.⁴⁹ Furthermore, there is a proliferation of UFDW proxy groups,⁵⁰ such as the China Council for the Promotion of Peaceful National Reunification (CCPPNR), Chinese People’s Association for Friendship with Foreign Countries (CPAFFC), China Overseas Friendship Association (COFA), and the China Zhi Gong Party (CZG).⁵¹ We also found information suggesting that China targets naturalized Singaporeans who were formerly PRC nationals in chatrooms.⁵² Some analysts commented that the East Asian Institute at the National University of Singapore is widely believed to be “compromised” by China.⁵³ Chinese agents of influence and sympathizers are believed to be present at these organizations and others.⁵⁴ For example, in August 2017, Singapore revoked the permanent resident status of a China-born professor at the

⁴⁷ Interview with Singapore government official, Singapore May 2019.

⁴⁸ Interview with Singapore political/defense analyst, Singapore, May 2019.

⁴⁹ Hsiao, 2019b.

⁵⁰ Interview with Singapore government official, Singapore, May 2019.

⁵¹ Amy E. Searight, “Chinese Influence Activities with U.S. Allies and Partners in Southeast Asia,” testimony before the U.S.-China Economic and Security Review Commission, April 5, 2018, pp. 5–6.

⁵² Interview with Singapore political/defense analyst, Singapore, May 2019.

⁵³ Interview with Singapore political/defense analyst, Singapore, May 2019; interview with Singapore political/defense analyst, Singapore, May 2019.

⁵⁴ Interview with Singapore political/defense analyst, Singapore, May 2019.

Lee Kuan Yew School of Public Policy. He was expelled from Singapore and accused of being an “agent of influence” for an unnamed foreign country who knowingly worked with the intelligence organizations and agents of that country to attempt to influence Singapore’s foreign policy and public opinion.⁵⁵ Local media reported that the country for which he was accused of acting was believed to be China.

Philippines

Possible Vulnerability: Tensions in the Alliance with the United States

Tensions have always existed in U.S.–Philippines alliance, even when relations were good. One of the most prominent sources of strain has been Washington’s refusal to commit to protect Manila’s claims in the South China Sea.⁵⁶ In recent years, this tension increased after China took Scarborough Shoal in 2012 despite a U.S. effort to negotiate a return to the status quo ante. Although political ties between Manila and Washington remained strong during the presidencies of Barack Obama and Benigno Aquino III—including the signing of a ten-year Enhanced Defense Cooperation Agreement—the Scarborough episode “loomed large in the mind of the security sector as an example of abandonment.”⁵⁷ China’s growing aggression has cast doubt on the Mutual Defense Treaty (MDT)’s deterrent effects, reinforced by “the more inward-looking and transactional U.S. leadership of President Donald Trump.”⁵⁸

⁵⁵ “Singapore Bans Chinese-American Scholar as Foreign Agent,” AP News, August 4, 2017; “Huang Jing, Chinese-American Academic Expelled by Singapore, Is Working in Beijing and Has ‘No Hard Feelings,’” *Today*, June 18, 2019.

⁵⁶ For a brief overview of some of this history, see Jay L. Batongbacal, “How to Reinvalidate the US-Philippine Alliance,” *The Diplomat*, May 1, 2019.

⁵⁷ Batongbacal, 2019.

⁵⁸ Lucio Blanco Pitlo III, “Ambiguity and Changing Times Compel Review of the Philippine-U.S. Mutual Defense Treaty,” Asia Maritime Transparency Initiative, February 8, 2019.

Much of the recent political instability in U.S.-Philippines relations is tied directly to Philippine President Rodrigo Duterte, who is notorious for bashing the United States (once even telling Obama to “go to hell” after he criticized Duterte’s war on drugs).⁵⁹ More troubling were Duterte’s suggestions of pursuing closer relations with China and making the Philippines less dependent on the United States for security. Under the slogan of pursuing an “independent foreign policy,” Duterte has distanced the Philippines from the United States and soft-pedaled Manila’s position on the South China Sea dispute.⁶⁰ He has also called for all U.S. special forces to leave,⁶¹ suspended joint military exercises, ruled out joint navy patrols, and announced the Philippines’ intent to terminate the Visiting Forces Agreement that facilitates U.S. military operations in the Philippines, before later suspending that abrogation.⁶² After declaring he had reached a “point of no return” with the United States, Duterte said he wanted “open alliances” with Russia and China.⁶³

Some analysts have written off these types of statements as rhetoric, but there are growing examples of this rhetoric in the Philippines government policy. For example, in March 2017, Manila canceled Enhanced Defense Cooperation Agreement construction plans at Antonio Bautista Air Base, the closest base to Scarborough Shoal.⁶⁴

⁵⁹ “Philippines’ Duterte Tells Obama to ‘Go to Hell,’” BBC, October 4, 2016.

⁶⁰ “Factbox: Duterte Distances Philippines from Ally U.S.,” Reuters, October 21, 2016; Cliff Venzon, “Duterte Soft Pedals on ‘Sensitive’ China Issues,” *Nikkei Asian Review*, December 20, 2016.

⁶¹ Manuel Mogato, “Duterte Says He Wants U.S. Special Forces out of Southern Philippines,” Reuters, September 12, 2016.

⁶² Jim Gomez, “Philippines Suspends Abrogation of Defense Pact with US,” Associated Press via *Washington Post*, June 2, 2020; Karen Lema, Martin Petty, and Phil Stewart, “Duterte Terminates Philippines Troop Pact, U.S. Calls Move ‘Unfortunate,’” Reuters, February 11, 2020; Martin Petty, “As Philippines’ Duterte Visits Vietnam, U.S. Jibes Hang over New Partnership,” Reuters, September 29, 2016.

⁶³ Pia Ranada, “Duterte to Russia: I’m About to ‘Cross Rubicon’ with US,” Rappler, September 28, 2016.

⁶⁴ Carmela Fonbuena, “Duterte Gov’t Rejects U.S. Plans to Construct in Palawan Air Base,” Rappler, March 6, 2017.

In November 2018, Manila and Beijing signed 29 agreements during Duterte's visit to China, including a memorandum of understanding to cooperate on oil and gas development in the South China Sea.⁶⁵ One month later, Philippine Defense Secretary Delfin Lorenzana initiated a review of the MDT to see whether it was "still valid or still relevant" to the Philippines' "national interest."⁶⁶ Despite a visit from U.S. Secretary of State Mike Pompeo during which he sought to reassure Manila of U.S. commitment, Lorenzana reiterated the need to review the MDT out of fear of being sucked into a "war that we do not seek and do not want."⁶⁷ Finally, the Chinese ambassador is said to have "24-hour access" to Duterte; the U.S. ambassador does not.⁶⁸

This stands in sharp contrast to Duterte's approach to China. Under an economic strategy called "Build Build Build" (BBB), Duterte hopes "to dramatically boost Chinese companies' investments in the Philippines," including infrastructure projects,⁶⁹ and the Philippines has welcomed Chinese investments. China promised it would provide \$24 billion in 2016 but had only provided approximately \$150 million as of July 2018.⁷⁰ Still, it appears that things are changing. As of November 2018, China was set to provide funding for 34 of the 75 flagship infrastructure projects under the BBB program (although the dollar amount of these projects is unclear),⁷¹ including projects located on or near former U.S. bases (Clark Air Base and Subic Bay Naval

⁶⁵ Pia Ranada, "LIST: Deals Signed During Xi Jinping's Trip to Philippines," Rappler, November 20, 2018.

⁶⁶ Jelly Musico, "Lorenzana Orders Review of 67-Year-Old US-PH Military Pact, Philippine News Agency, December 28, 2018.

⁶⁷ Guy Taylor, "Philippine Defense Official Review of 1951 Mutual Defense Treaty," *Washington Times*, March 5, 2019.

⁶⁸ Interview with Philippine political/defense analyst, Manila, May 20, 2019.

⁶⁹ Joshua Kurlantzick, "How Much Damage Can Duterte Do to the U.S.-Philippine Relationship?" *World Politics Review*, October 7, 2016.

⁷⁰ Jason Koutsoukis and Cecilia Yap, "China Hasn't Delivered on Its \$24 Billion Philippines Promise," Bloomberg, July 25, 2018; Jenny Lei Ravelo, "Japan, China Battle for ODA Influence in the Philippines," *Devex*, November 20, 2018.

⁷¹ "Diokno: PH Not in Risk over China Loans," CNN Philippines, November 19, 2018.

Base).⁷² Chinese investment has also expanded into the digital realm: The leading wireless provider in the Philippines, Globe Telecom, is on track to launch its Huawei-backed 5G service, and Huawei is the winning contractor for the Safe Philippines project, in which 12,000 state-of-the-art mass surveillance security cameras will be piloted in several cities.⁷³ China Telecom won a telecommunications license at the personal behest of Duterte.⁷⁴

Officials say Duterte is interested in balancing ties with China and Washington as a way to provide the Philippines with more options. The rhetoric and actions by his administration have opened opportunities to exploit potential gaps, given that messaging from Manila suggests the Philippines feels it is being abandoned, taken for granted, or undersupported by the United States. Given the welcoming of greater Chinese involvement and investments and Manila's friendlier relations with Beijing, disinformation could be used to further inflame negative views of the United States and the MDT. This is particularly worrisome if, as some have described, there is decades-long pent-up dissatisfaction with the United States stemming from the legacy of U.S. cultural colonialism in the Philippines.⁷⁵ As one Filipino interviewee explained, this has left remnants of anti-Americanism in the Philippines.⁷⁶ Therefore, the Philippines might provide fertile ground for disinformation campaigns designed to turn the local population further against the United States.

⁷² Timothy McLaughlin, "A U.S. Ally Is Turning to China to 'Build, Build, Build,'" *The Atlantic*, May 8, 2019.

⁷³ Mark Manantan, "Commentary: What the Huawei Espionage Controversy Means to the Philippines," *Philstar*, March 25, 2019; Cliff Venzon, "Philippines' Wireless Leader Pushes on with Huawei 5G Launch," *Nikkei Asian Review*, February 12, 2019.

⁷⁴ Neil Jerome Morales and Karen Lema, "China Telecom, Local Tycoon Team up to Win Philippine Telco License," *Reuters*, November 6, 2018.

⁷⁵ Mark Valencia, "Whither the US-Philippines Alliance? Analysis," *Eurasia Review*, March 12, 2019.

⁷⁶ Interview with Philippine political/defense analyst, Manila, May 18, 2019.

Evidence of External Activity Lacking

Disinformation is rampant in the Philippines, particularly on Facebook, but there is no evidence of Chinese involvement.⁷⁷ Instead, evidence points to domestic sources. In large part, Filipinos' high social media usage stems from the fact that the two large local telecom companies have a policy of automatically setting up Facebook accounts for new internet subscribers,⁷⁸ meaning that internet access is roughly equal to Facebook accounts. The heavy reliance on Facebook is important because, according to some thinking, Duterte's supporters, and possibly Duterte himself, have deliberately used social media platforms "to twist public opinion and silence dissent."⁷⁹ According to one Filipino interviewee, Facebook "is the primary venue" for spreading disinformation in the Philippines.⁸⁰

Researchers and news organizations (such as Rappler and VERA Files) track both the social media and traditional media spaces for disinformation and work in partnership with Facebook as third-party fact-checkers.⁸¹ These actors have detected and tracked what they say is the undeniable usage of automated bots and fake social media accounts that are overwhelmingly pro-Duterte. Many of these social media sites appear to be "linked in some way"—they often have "coordinated, similar messaging" that tends "to all shift together."⁸² For example, Rappler uncovered 26 accounts that spread nearly the same messaging and followed more groups than they had friends, which is a red flag in identifying fake accounts.⁸³ Looking deeper into these accounts, Rappler found that many of the links being posted were by accounts run by supporters of Duterte. There is also evidence of trolling groups spread-

⁷⁷ Interview with Philippine government official, Manila, May 2019.

⁷⁸ Interview with Philippine political/defense analyst, Manila, May 2019.

⁷⁹ Head, 2018.

⁸⁰ Interview with Philippine political/defense analyst, Manila, May 2019.

⁸¹ "VERA Files Joins Facebook's Third-Party Fact-Checking Program in PH," VERA Files, April 13, 2018.

⁸² Interview with Philippine political/defense analysts, Manila, May 2019.

⁸³ Interview with Philippine political/defense analyst, Manila, May 2019.

ing disinformation. These groups comprise real people who buy old Facebook accounts to disguise their efforts and get paid per post.⁸⁴

The messages on these pro-Duterte platforms are clear in their support of him and in their targeting of his opponents. Many political opponents of Duterte are targeted with “a lot of hate mongering” messages.⁸⁵ It does not stop there. These groups have also attacked traditional media, accusing some journalists of being foreign agents and pressuring organizations and individual journalists with threats, lawsuits, and warnings that the government might not renew the franchise licenses of companies if they do not change the way they cover the news. This has been the case against outlets critical of the Duterte administration, such as Rappler.⁸⁶ The Philippines’ Department of Justice has said it could indict both Rappler and its founder, Maria Ressa, for tax evasion and failure to file tax returns.⁸⁷ Accused of libel and violating foreign ownership laws, Ressa has spent time in and out of prison. Both Ressa and the cofounder of VERA Files, Ellen Tordesillas, have been accused of an elaborate plot orchestrated by the U.S. Central Intelligence Agency to oust Duterte from office.⁸⁸ In addition to online trolling, administration critics have also received death threats.⁸⁹

Since the 2012 Scarborough incident, there has been a growing narrative in the Philippines questioning the credibility of U.S. security commitments. Duterte’s presidency brought an uptick in anti-U.S., antiliberal democracy messaging, leading one Filipino observer to note

⁸⁴ Interview with Philippine political/defense analyst, Manila, May 2019.

⁸⁵ Interview with Philippine political/defense analyst, Manila, May 2019.

⁸⁶ Neil Jerome Morales, “Philippine Regulator Revokes News Site’s License over Ownership Rules, Media Outraged,” Reuters, January 15, 2018.

⁸⁷ Alexandra Stevenson, “Soldiers in Facebook’s War on Fake News Are Feeling Overrun,” *New York Times*, October 9, 2018.

⁸⁸ Shawn W. Crispin, “Rappler-CIA Plot Claim Is Attempt to Cut Funding, Philippine Journalists Say,” Committee to Protect Journalists, May 21, 2019; Camille Elemia, “‘False, Garbage’: Maria Ressa, Ellen Tordesillas, PCIJ on Duterte ‘Ouster Plot,’” Rappler, April 22, 2019.

⁸⁹ Daniel Funke, “These Fact-Checkers Were Attacked Online After Partnering with Facebook,” Poynter, September 10, 2018.

that “we see a rewriting of what we know of our history.”⁹⁰ Filipinos have traditionally been strong supporters of the United States, and almost all of our Filipino interviewees reiterated that Filipinos remain this way by nature; blatant anti-U.S. messaging is something that has only arisen since Duterte became president. Much of this messaging is subtle, focusing on distrust of the United States, complaints about the MDT, or an inability to depend on the United States.⁹¹ Some of the messages are less subtle, such as saying the Philippines should not be aligned with the United States.⁹² Nevertheless, the frequency of such messaging carries the potential of “fueling skepticism in the alliance.”⁹³ One recent example of Duterte’s shift in policy was the country’s embrace of China’s telecom companies despite U.S. warnings.⁹⁴

There is no question that much of this activity is organized by real people who support Duterte. There is even evidence of military personnel becoming more active on social media.⁹⁵ This is not surprising, according to one analyst, given that military members and reservists tend to see Duterte as promilitary.⁹⁶ And despite the overwhelming evidence of disinformation spreading on social and traditional media, there is no evidence of foreign involvement—but there are hints of foreign techniques.⁹⁷ For example, although disinformation existed before Duterte became president, “fake accounts” have become much more sophisticated since that time, making it more difficult to trace and check them and, consequently, also making it harder to debunk disin-

⁹⁰ Interview with Philippine political/defense analyst, Manila, May 2019.

⁹¹ Interview with Philippine political/defense analysts, Manila, May 2019.

⁹² Interview with Philippine political/defense analyst, Manila, May 2019.

⁹³ Interview with Philippine political/defense analyst, Manila, May 2019.

⁹⁴ Niharika Mandhana, “In Global Tech Battle, a Balky U.S. Ally Chooses China,” *Wall Street Journal*, July 15, 2019.

⁹⁵ One analyst cited the following groups as examples: Defense of the Republic of the Philippines, RHK111, and Philippines Defense Forces. Interview with Philippine political/defense analyst, Manila, May 2019.

⁹⁶ Interview with Philippine political/defense analyst, Manila, May 2019.

⁹⁷ Interview with Philippine political/defense analyst, Manila, May 2019.

formation.⁹⁸ The operations are now more professional, more systematic, and more deliberate in their targeting and messaging.⁹⁹ Postings of disinformation on Facebook also appear to adjust more quickly to that platform's algorithm to avoid flagging.¹⁰⁰

There are some questions about whether Duterte has sought help from abroad for disinformation techniques. In 2017, Manila and Moscow inked several deals on such issues as agriculture, transportation, and defense cooperation.¹⁰¹ One of these included a memorandum of cooperation between the Philippines' Presidential Communications Operations Office (PCOO) and the Russian Ministry of Telecom and Mass Communications.¹⁰² The purpose of the partnership was to focus on "state information dissemination," which included "intensive media and management training" of PCOO staffers in Russia at the RT TV Headquarters, Russian news agency TASS, and the Ministry of Telecom and Mass Media.¹⁰³ Although the details of this training were never announced, the fact that these officials are in charge of external communications, including social media, raised concerns that Philippine officials are learning Russian disinformation techniques.

The lack of evidence directly connecting China to the Philippines' disinformation activity does not necessarily mean that China is not active. Like Singapore, UFWO proxy groups, such as the CCPNR, CPAFFC, COFA, and the CZG, are active.¹⁰⁴ There is also suspicion of Chinese influence in traditional media. For example, the World News "serves as a mouthpiece for pro-CCP sentiments as the

⁹⁸ Interview with Philippine political/defense analyst, Manila, May 2019.

⁹⁹ Interview with Philippine political/defense analyst, Manila, May 2019.

¹⁰⁰ Interview with Philippine political/defense analyst, Manila, May 2019.

¹⁰¹ Pia Ranada, "PH, Russia Sign Defense Agreement, 9 Other Deals," Rappler, May 25, 2017a; Pia Ranada, "PH, Russia Sign 8 Agreements, Including Extradition Treaty," Rappler, November 14, 2017.

¹⁰² The Russian ministry is now called the Ministry of Digital Development, Communications and Mass Media of the Russian Federation.

¹⁰³ "PH, Russia Communication Offices to Partner in Info Dissemination," *Interaksyon*, May 30, 2017.

¹⁰⁴ Searight, 2018, pp. 5–6.

country's largest Chinese-language newspaper in terms of circulation" and "its leadership maintains strong ties to pro-China organizations in the Philippines."¹⁰⁵ Another example is the *Manila Times*, which has similarly been accused of accepting Chinese funding to keep afloat in return for pro-China coverage.¹⁰⁶ Evidence is lacking so far, however, and there are virtually no pro-China articles or social media groupings in the Philippines; news about China is generally quite negative.

This is because Filipinos tend to be anti-China, a refrain voiced almost unanimously during our field research.¹⁰⁷ One interviewee characterized it that Filipinos simply see China as having "different values," while another argued that Filipinos "don't trust China."¹⁰⁸ This negative view is reinforced by the influx of Chinese that follow Chinese investments.¹⁰⁹ According to the Bureau of Immigration, 3.12 million Chinese tourists entered the Philippines from January 2016 to May 2018.¹¹⁰ Although it is unclear how many were workers, there has been an increase in the issuance of worker permits to Chinese.¹¹¹ There are also believed to be approximately 400,000 illegal Chinese workers in the country.¹¹² Although there is no evidence that these Chinese arrivals are working under any sort of guidance from Beijing, Filipinos view the influx negatively.¹¹³ This is particularly true of the workers, who are

¹⁰⁵Searight, "2018, p. 5.

¹⁰⁶Interview with Philippine political/defense analyst, Manila, May 18, 2019; interview with Philippine political/defense analyst, Manila, May 20, 2019.

¹⁰⁷Nick Aspinwall, "'We Are Filipinos, and We Hate China': China's Influence in the Philippines, and Backlash Against Tsinoys," *SupChina*, June 6, 2019.

¹⁰⁸Interview with Philippine political/defense analyst, Manila, May 2019; interview with Philippine government official, Manila, May 2019.

¹⁰⁹Panos Mourdoukoutas, "Filipinos Are Beginning to See the Ugly Side of Chinese Investments," *Forbes*, March 21, 2019.

¹¹⁰Ian Nicolas Cigaral, "More Than 3 Million Chinese Allowed Entry into Philippines Since 2016—Immigration Data," *Philstar*, June 9, 2018.

¹¹¹Ronald U. Mendoza and Miann S. Banaag, "Is the Philippines' Pro-China Policy Working?" *The Diplomat*, November 14, 2018.

¹¹²Manantan, 2019.

¹¹³Interview with Philippine government official, Manila, May 20, 2019.

seen as taking jobs away from Filipinos and causing real estate prices to rise by buying up properties.¹¹⁴ Behavior by some Chinese visitors reinforces the negative perceptions, such as a February 2019 incident in which a Chinese student, when told she had to finish her dessert before entering a train station, instead threw her pudding at a Filipino police officer.¹¹⁵ For many Filipinos, the incident reflected a widely held view that Chinese hold the Philippines in low regard.¹¹⁶ One interviewee went as far as to say that Filipinos hold racist views about Chinese.¹¹⁷ Even if China is engaged in disinformation campaigns to propagate positive images about China, these campaigns are likely to have minimal impact because they are not likely to resonate.

Still, this is not to suggest such campaigns would not have any impact. Chinese disinformation campaigns could help inflame negative Filipino views of the United States or increase Filipinos' mistrust in liberal democracy.¹¹⁸ Although our research found no evidence of pent-up dissatisfaction with the United States, numerous Filipino interviewees observed that, despite traditionally pro-U.S. views among Filipinos, trends indicate an increasing willingness to question U.S. reliability since Duterte became president. According to a 2017 public opinion poll by the Pew Research Center, the gap between Filipinos' favorable views of the United States and of China closed over the 2015–2017 period mainly because of a decline in support for the United States.¹¹⁹ The percentage of Filipinos with a favorable view of the United States

¹¹⁴ “Chinese ‘Invasion’ Triggers Property Surge in Manila,” *Business Mirror*, May 5, 2018; Mendoza and Banaag, 2018.

¹¹⁵ “Chinese Student Charged for Throwing Soybean Pudding at Filipino Officer,” BBC, February 14, 2019.

¹¹⁶ Raul Dancel, “Chinese Student in Pudding-Throwing Tantrum ‘Really, Really Sorry’, but Still Faces Deportation from Philippines,” *Straits Times*, February 12, 2019.

¹¹⁷ Interview with Philippine political/defense analyst, Manila, May 2019.

¹¹⁸ Such disinformation could be specifically targeted at Filipinos of ethnic Chinese heritage who might be easier for China to reach via such social media platforms as WeChat. Our study, however, did not uncover evidence of China targeting ethnic Chinese Filipinos specifically.

¹¹⁹ Jacob Poushter and Caldwell Bishop, “People in the Philippines Still Favor U.S. over China, but Gap Is Narrowing,” Pew Research Center, September 21, 2017.

fell from 92 percent to 78 percent over that time, and confidence in U.S. leaders “to do the right thing regarding world affairs” similarly fell from 94 percent to 69 percent between the Obama and Trump administrations; China’s favorability only rose 1 point, to 55 percent, and confidence in Xi Jinping rose 2 points, to 53 percent. One interviewee noted that Filipinos’ distrust of the United States was much less under Duterte’s predecessor Aquino.¹²⁰ Some worried that the rise of disinformation was effectively normalizing the argument that the Philippines and the United States are not really well aligned in terms of security goals.¹²¹ These feelings are matched by a subtle reduction of frustration vis-à-vis China. These two trends combined suggest that disinformation messaging might be having some effect on Filipinos, but it is impossible to disaggregate this empirically from the change in political leadership in both countries.

There is some anecdotal evidence that indirectly ties China to the disinformation problem in the Philippines. In 2016, the Philippine Amusement and Gaming Corporation issued rules to regulate operations of the Philippine Offshore Gaming Operators, which are entities that offer online gaming services to foreign players. More than 50 offshore gaming companies that cater to Chinese clients were given permits to operate in the Philippines.¹²² There is evidence to suggest that some of these companies are also being used for more-nefarious domestic purposes. Some of these offshore gaming companies, along with former Philippine business call centers, have been converted into troll farms or “click factories” used by pro-Duterte actors.¹²³ These entities offer low-paying positions in which people increase clicks for specific

¹²⁰Interview with Philippine political/defense analyst, Manila, May 2019.

¹²¹Interview with Philippine political/defense analyst, Manila, May 2019.

¹²²“Chinese ‘Invasion’ Triggers . . .,” 2018.

¹²³These are for-hire private-sector businesses that hire workers to put out a great deal of disinformation; in this case, for President Duterte. Interview with Philippine political/defense analysts, Manila, May 18 and May 19, 2019. For one academic study on artificial social media activity in the Philippines, see Samantha Bradshaw and Philip N. Howard, *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*, Oxford, UK: Computational Propaganda Research Project, December 2017.

websites or open and operate fake Facebook or Twitter accounts.¹²⁴ These are for-hire operations that are believed to be funded by Duterte and his supporters to push pro-Duterte messages and to attack the media and his political opponents.¹²⁵ One of these former call centers in Duterte's hometown of Davao City, which was believed to be a troll farm, burned down. In addition to a quick response from Manila, China provided aid to families of those who died, leading to speculation it was a China-operated troll farm.¹²⁶

China appears to be most active in traditional influence operations. In addition to economic penetration focused on gaining a foothold in strategic locations and key industries,¹²⁷ China has focused on cultivating a positive image in the Philippines through three avenues: diplomatic, political, and elite capture.¹²⁸ China is trying to build its diplomatic image in the Philippines through its infrastructure projects and other various development projects—and to remind Filipinos of who funds these projects, China has sponsored newspaper ads in the Philippines that run in English and describe the progress China has made in the region.¹²⁹

Politically, China has cultivated a close relationship with Duterte to encourage Manila to be more pliable, including easing off its South China Sea claims. Evidence of success here is seen in Duterte's changed approach to some issues. For example, Duterte began restricting officials from visiting Taiwan for training purposes in 2018.¹³⁰ He also has allowed Chinese shows on state-run PTV and Chinese military aircraft to fly through Philippines airspace and land in his hometown of Davao

¹²⁴Head, 2018.

¹²⁵Interview with Philippine political/defense analyst, Manila, May 2019.

¹²⁶Interview with Philippine political/defense analyst, Manila, May 2019.

¹²⁷Richard Javad Heydarian, "China's Economic Cabbage Strategy," Asia Maritime Transparency Initiative, March 11, 2019.

¹²⁸Interview with Southeast Asia political/defense analyst, Singapore, May 16, 2019.

¹²⁹Interview with Philippine political/defense analyst, Manila, May 18, 2019.

¹³⁰Interview with Philippine political/defense analyst, Manila, May 20, 2019.

City.¹³¹ One public incident was Duterte's feud with Supreme Court Senior Associate Justice Antonio Carpio. Contrary to Carpio's calls to be more assertive in defending Manila's sovereign rights in the South China Sea, Duterte sometimes mirrors Beijing talking points by saying that standing up to China would mean certain war and is therefore not in the Philippines' interest.¹³²

Finally, some analysts said that China is engaged in attempts at elite capture to improve its influence.¹³³ Although not believed to be widespread at the federal level, Chinese officials are cultivating relationships with local government officials (such as governors or mayors) who are in need of financial resources and thus might be more susceptible to foreign influence; Chinese officials are also courting heads of big business conglomerates who are eager for business with China. Because of anti-Chinese views among Filipinos, however, it is not uncommon for local leaders to take the money but not adopt positive views of China.¹³⁴

Response to Perceived Disinformation

Although disinformation is rampant, the government is not actively working to counter it or to promote education campaigns to increase information literacy. Duterte and his supporters attack the media as peddling disinformation and deny accusations of fake accounts and use of bots.¹³⁵ Nor has the government pursued any legislation in the way that Singapore has. Hearings at the Philippine Senate, for example, concluded that legislation regarding disinformation "was unrec-

¹³¹Patricia Lourdes Viray, "Senate Minority Wants Probe into Chinese Planes in Davao, Chinese Shows on PTV," *Philstar*, July 9, 2018.

¹³²Barbara Marchadesch, "Duterte Blasts Carpio over South China Sea Stance," *MSN*, November 28, 2018.

¹³³Interview with Philippine political/defense analyst, Manila, May 19, 2019; interview with Philippine political/defense analyst, Manila, May 20, 2019.

¹³⁴Interview with Philippine political/defense analyst, Manila, May 20, 2019.

¹³⁵Ruth Abbey Gita, "Duterte 'Nothing to Do' with Banned Facebook Account," *Sunstar*, April 1, 2019.

essary, and possibly counterproductive.”¹³⁶ Although the government has a cyber unit that investigates disinformation, it tends to go after people critical of the president.¹³⁷ In addition to the deals with Huawei and China Telecom, the Philippines’ Department of Information and Communications Technology signed a memorandum of understanding with Russian company BiZone Limited Liability Company to conduct joint research and development on cybersecurity technologies and to exchange information on cybersecurity policies, threats, and technologies.¹³⁸ Combined, these raise concerns that Philippine information technology systems might be compromised in the near future, if they are not already.

Therefore, much of the effort to combat disinformation has fallen to private actors. Rappler and VERA Files, for example, fact-check sites and links suspected of being fake. (No one checks foreign-language sources, meaning that communications in Chinese go unchecked.¹³⁹) If Rappler or VERA Files confirm that an article is fake, Facebook, because of its partnerships with those outlets, downgrades the material in its own newsfeed but does not delete or block that material. If someone clicks on the link, a bubble pops up saying it was flagged for content along with a link explaining why the news is regarded as fake. Rappler and VERA Files also teamed up with nine other news organizations and three universities to launch a fact-checking website for the 2019 elections.¹⁴⁰

¹³⁶Head, 2018.

¹³⁷Interview with Philippine political/defense analyst, Manila, May 2019.

¹³⁸Consuelo Marquez, “DICT Signs MOU with Russian Firm to Boost Cybersecurity,” *Inquirer.Net*, September 25, 2018.

¹³⁹Interview with Philippine political/defense analyst, Manila, May 2019.

¹⁴⁰Tsek.ph, homepage, undated.

Japan

Possible Vulnerability: Anti-Base Sentiment in Okinawa

The U.S.–Japan alliance enjoys widespread and deep support among Japan’s political leaders. Since Abe Shinzō returned to office in 2012, his administration has passed a series of laws that strengthen and expand Japan’s role in the security domain.¹⁴¹ In 2015, his administration signed revised Guidelines for U.S.–Japan Defense Cooperation that better defined—and in some ways expanded—the roles and missions of Japan within the alliance. Abe’s government has advocated that Japan make “proactive contributions to peace” with the goal of a “free and open Indo-Pacific.” Some of these efforts have led Japan to take a larger role in standing up to China in the region.¹⁴²

Abe’s support for the United States has created problems for him with the leadership or people of Okinawa because of his strong support for continued hosting of U.S. bases on the island. Although Okinawa makes up 0.6 percent of Japan’s territory, it is home to about 25,843 U.S. military personnel, accounting for 70.4 percent of the total area exclusively used for U.S. military facilities in Japan.¹⁴³ Critics of Abe and of the U.S. presence in Okinawa argue that the majority of Okinawans are opposed to continued hosting of the U.S. presence,¹⁴⁴ and polls tend to support this.¹⁴⁵ Regardless of whether Okinawans under-

¹⁴¹ Jeffrey W. Hornung, “Japan’s 2015 Security Legislation: Changed Rooted Firmly in Continuity,” in Mary McCarthy, ed., *Routledge Handbook of Japanese Foreign Policy*, New York: Routledge, 2018.

¹⁴² Jeffrey Reeves, Jeffrey W. Hornung, and Kerry Lynn Nankivell, *Vying for Influence: How Competition Between China and Japan Is Shaping the Asia-Pacific’s Regional Security*, New York: Routledge, 2017.

¹⁴³ Okinawa Prefectural Government, *What Okinawa Wants You to Understand About the U.S. Military Bases*, Naha, Japan, March 2018, pp. 2, 6.

¹⁴⁴ Jeff Kingston, “Understanding Anti-Base Sentiment in Okinawa,” *Japan Times*, May 28, 2016.

¹⁴⁵ An April 2017 NHK poll showed that 77 percent of Okinawa residents wanted either a complete removal or a reduction of U.S. bases. Kei Kōno, “Okinawa and Nationwide Awareness Regarding U.S. Military Bases in Okinawa: April 2017 ‘Okinawa at 45 Years Since Reversion’ Poll [沖縄米軍基地をめぐる意識 沖縄と全国 ～2017年4月「復帰45年の沖縄」調査～],” *NHK*, August 2017. Similarly, a February 2019 Asahi poll found 88 per-

stand the national security need for U.S. forces, “they do not understand why Okinawa has to have such a large proportion of the U.S. bases.”¹⁴⁶

Resentment of the U.S. presence in Okinawa is not new. Okinawans have pointed to the 1995 abduction and gang rape of a 12-year-old girl by three servicemen; the murder of a 20-year-old woman in 2016; traffic accidents; poor behavior by drunken military personnel; accidents stemming from malfunctions of U.S. equipment; and concerns over noise, pollution, and environmental effects as sources of frustration.¹⁴⁷ The public anger tied to such events is undeniable, but it is also only one facet of the overall experience that Okinawans have of the U.S. presence. U.S. service personnel are engaged in the local communities, contribute to the local economy, and even give their lives in unfortunate accidents that anti-base activists tend to ignore but that most Okinawans are cognizant of.¹⁴⁸

The focal point of public opposition is the Marines Corps Air Station Futenma. Following the 1995 gang rape, Tokyo and Washington moved quickly to relocate Futenma’s personnel and functions out of Ginowan in central Okinawa. Under a 1996 agreement, the air station would close, its functions would be distributed throughout

cent of residents in Okinawa felt that, compared with mainland Japan, the burden of hosting U.S. forces was too much. “88% Okinawa Base Burden ‘Too Big,’ Asahi Newspaper Prefectural Survey [沖縄の基地負担「大きすぎ」88% 朝日新聞社県民調査],” *Asahi Shimbun*, February 19, 2019.

¹⁴⁶Tim Daiss, “Anti-U.S. Sentiment in Japan Grows amid Former Marine’s Alleged Murder,” *Forbes*, July 4, 2016.

¹⁴⁷Individual events and the public backlash that follows are well documented in media reports and statements from the Okinawa Governor. An official document published by the Okinawa Prefectural Government regarding U.S. presence on the island states that

The incidents, accidents, noise pollution, environmental issues, and other problems that have arisen from these sprawling bases have had a significant impact on the lives of people residing in Okinawa, and just the presence of these bases is the biggest factor inhibiting Okinawa’s economic development. (Okinawa Prefectural Government, 2018, p. 3)

¹⁴⁸U.S. military personnel have lost their lives performing work for the public good on Okinawa. For example, in 2009, a U.S. Marine was killed and two others were seriously injured when a World War II-era shell that they were preparing for disposal exploded. David Allen, “Marine Killed by Blast on Okinawa Is ID’d,” *Stars and Stripes*, March 27, 2009.

Japan, and the facility's land would revert to the prefecture "after adequate replacement facilities are completed and operational."¹⁴⁹ Opponents pushed for the Futenma Replacement Facility to be moved off Okinawa entirely and were given hope in 2009 when Prime Minister Hatoyama Yukio advocated as much. Hatoyama, however, eventually conceded that there was no viable alternative to the chosen site, leading to his resignation as premier.¹⁵⁰ His successor quickly reverted to supporting the original position, which every subsequent prime minister has also upheld.

In Okinawa, however, Hatoyama's actions gave new energy to the base opposition. Even after Tokyo's reversion to its traditional position, consecutive Okinawa governors have opposed the plan. Current governor Tamaki Denny is no different. Tamaki became governor on September 30, 2018, running on an agenda of closing down Futenma and relocating it out of the prefecture. Tamaki has urged Tokyo to work with Washington to move Futenma's functions and personnel off Okinawa. Shortly after he became governor, the Okinawa prefectural assembly approved an ordinance for a public referendum on whether residents of Okinawa support the land reclamation of Henoko.¹⁵¹ On November 27, Tamaki announced his intention to hold the referendum.¹⁵²

The referendum, held on February 24, 2019, gave voters three choices: favor the relocation plan, oppose the relocation plan, or have

¹⁴⁹ *The SACO Final Report on Futenma Air Station (an Integral Part of the SACO Final Report)*, Ministry of Foreign Affairs (Japan), December 2, 1996.

¹⁵⁰ "Japanese PM Yukio Hatoyama Resigns amid Okinawa Row," BBC, June 2, 2010; Louisa Lim and Lucy Craft, "Japan's Prime Minister Resigns over U.S. Base," NPR, June 2, 2010.

¹⁵¹ Civic groups had lobbied for a referendum by collecting more than 90,000 signatures. Kazuyuki Ito, "Okinawa Decides to Hold Feb. 24 Referendum on U.S. Base Issue," *Asahi Shimbun*, November 27, 2018.

¹⁵² "Governor Tamaki, 'An Important Opportunity to Directly Reflect the Prefectural Public's Will,' Okinawa Prefecture Announces February 24 for Holding Prefectural Referendum [沖縄県が県民投票2月24日実施を発表 玉城知事「県民の意思を直接反映させる重要な機会」]," *Ryūkyū Shimpō*, November 27, 2018.

no opinion.¹⁵³ The result was a powerful vote opposing relocation at 72.2 percent, with 19.1 percent supporting it and 8.7 percent not having an opinion.¹⁵⁴ Although legally nonbinding, turnout was 52.48 percent of eligible voters, providing legitimacy to the referendum and viewed as representative of local sentiment.¹⁵⁵ Despite this, and despite the ongoing opposition by the governor and local groups, Tokyo has been continuing its land reclamation work off the coast of Henoko as part of the Futenma Replacement Facility project.¹⁵⁶

The referendum is believed to have further emboldened Okinawan sentiment opposing U.S. basing, and herein lies Okinawa's potential exploitable vulnerability. Understanding that there is a segment of the local population unhappy with Tokyo and with Washington for having to host a large percentage of U.S. military bases could provide fertile ground for disinformation campaigns that, if successful, could drive further wedges between the prefecture and Tokyo or further foment anti-U.S. sentiment.

Evidence of External Activity Lacking

Compared with the Philippines, disinformation does not appear to be much of a problem in Japan.¹⁵⁷ One of the best-known examples occurred in 2005 when a fake Yahoo News site reported that Chinese forces invaded Okinawa.¹⁵⁸ More recently, a few fake stories have

¹⁵³Initially, the third option was not included. It was only after five cities in Okinawa indicated that they would not participate in the referendum unless the third option of "neither" was included that the option appeared.

¹⁵⁴Eric Johnston, "More Than 70% in Okinawa Vote No to Relocation of U.S. Futenma Base to Henoko," *Japan Times*, February 24, 2019.

¹⁵⁵Johnston, 2019.

¹⁵⁶The same February 2019 Asahi poll referenced above found 68 percent of Okinawa residents opposed to the relocation of Futenma to Henoko. "88% Okinawa Base Burden . . ." 2019.

¹⁵⁷For a broader overview of Chinese influence operations in Japan, see Hsiao, 2019a.

¹⁵⁸Loren Baker, "Fake Yahoo News Site Reports Chinese Troops Attack Okinawa," *Search Engine Journal*, October 19, 2005.

come to light, but none is believed to be the work of China.¹⁵⁹ Instead, they are believed to be domestic in origin and to stem primarily from Japan's right wing. For example, the Japanese Culture Channel Sakura, a right-wing news blog, was blamed for a story circulating in 2014 that claimed Naha's then-Mayor Onaga Takeshi was shown favoritism by Chinese authorities, having sent his daughter to study in China.¹⁶⁰ Onaga attempted to debunk the story, but Tamogami Toshio, a former chief of staff of the Air Self-Defense Force who lost his job over a historical revisionist essay, circulated the same story in April 2015 on Twitter as an explanation for why Onaga was against the Futenma Replacement Facility plan.¹⁶¹ In the 2018 Okinawa gubernatorial election, there were 60 incidents believed to be disinformation, two of which were confirmed as such.¹⁶² One was a tweet that, along with criticizing Tamaki for believing he can talk easily to Americans just because he is half-American, also falsely claimed that former-Governor Onaga had never been able to meet U.S. officials or enter U.S. bases on Okinawa.¹⁶³

Onaga, who died in 2018, was a frequent target, but disinformation campaigns also target base opponents. For example, a January 2017 edition of Tokyo MXTV's "News Joshi" included a segment on protesters trying to stop the construction of U.S. military helipads in Okinawa. The reporter never engaged the protestors; instead, he reported

¹⁵⁹ Author email correspondence with Japan political/defense analyst, November 14, 2018; interview with Japan government official, Tokyo, January 16, 2019; interview with Japan political/defense analyst, Tokyo, January 16, 2019.

¹⁶⁰ "Okinawa Gov.'s 'China Connection' Nothing but 'Fake News,' But Spreads Via Internet," *Mainichi*, June 18, 2017.

¹⁶¹ "Okinawa Gov.'s 'China Connection' . . .," 2017.

¹⁶² "Originator of Fake News: I Can't Stand It That the Public Will Can Bend by Biased News [フェイクニュースの発信者「偏った情報で民意が歪められるの耐えられない」]," *Okinawa Times*, February 2, 2019.

¹⁶³ "Originator of Fake News . . .," 2019; "Verifying Disinformation in the Okinawa Gubernatorial Election: Fake 'Even When Communist Party Candidate Onaga Visited America, He Couldn't Meet Any U.S. Government Official' [沖縄県知事選で偽情報検証: フェイク「共産党出馬の翁長知事が訪米しても政府関係者の誰にも会えなかった」]," *Okinawa Times*, September 27, 2018.

that the elderly protesters were dangerous and “being paid by ‘a radical group’ in Tokyo headed by someone with a Korean name.”¹⁶⁴ The segment was sharply criticized as heavily biased and poorly reported. A group mentioned by name in the segment, Norikoe Net, even filed a complaint with Japan’s Broadcasting Ethics and Program Improvement Organization for slander by “fake information.” This included claims that people are being paid to struggle against U.S. bases in Okinawa; that the people struggling against the bases are not Okinawan locals but extremists and activists from Japan’s main islands; that the anti-base struggle receives support from China and North Korea; and that secret agents of China, South Korea, and North Korea are leading the struggle in Okinawa.¹⁶⁵

Although some suspect Chinese involvement in these incidents, there is no evidence to support it in any conclusive way.¹⁶⁶ There is evidence, however, that China might be engaged in traditional influence operations in Okinawa. Much of this is anecdotal; if real, it could prove corrosive to Japan’s security and the U.S.-Japan alliance. The base protests provide one example. The Marine Corps on Okinawa and U.S. Forces Japan said that local anti-military sentiment among Okinawans is not as widespread as it appears. Rather, “large protests are often organized and manned by outsiders and professional groups, such as teachers’ unions and workers groups who fly in from the Tokyo area.”¹⁶⁷ This claim is not without some support. One Japanese academic sympathetic with the anti-base protestors notes,

Protest activities are organized and led by people in Okinawa However, local activists urge people outside Okinawa to join them, and ask for their support. There is, indeed, a con-

¹⁶⁴Philip Brator, “Japan Enters the Post-Truth Age with Distorted MXTV Report on Okinawa Protests,” *Japan Times*, February 4, 2017.

¹⁶⁵Shin Sugok, “The Recent Merging of Anti-Okinawa and Anti-Korean Hate in the Japanese Mass Media,” *Asia-Pacific Journal: Japan Focus*, Vol. 17, No. 1, January 15, 2019.

¹⁶⁶Interview with Japan government official, Tokyo, January 16, 2019.

¹⁶⁷Travis Tritten and Chiyomi Sumida, “Protests on Okinawa Aren’t Always What They Appear to Be,” *Stars and Stripes*, May 23, 2013.

stant flow of visitors. [Peace activist Yuichi] Kamoshita maintains that about 30 percent of those who sit in front of the gates of Camp Schwab are those from other parts of Japan, and more people from outside participate in other protest activities.”¹⁶⁸

There is even “transnational support” of the protests by “international visitors.”¹⁶⁹

These claims are important because there are those who believe that China is involved in these efforts. For example, some claim that Beijing is funneling cash to Chinese student associations in Okinawa and even supporting Okinawans who oppose U.S. basing.¹⁷⁰ Officials admit that there is no evidence to support the idea that China is directly funding anti-base protestors, but there is uncertainty regarding how and where the left-wing groups that fund the protestors get their money.¹⁷¹ Others claim that the protestors are guided from Beijing. One anecdote claiming that South Koreans were involved in anti-base protests in Ginowan in May 2012 included the assertion that one of the main sponsors was a New Left group called Communists Alliance (Unification Committee). This group, according to the claim, “is generally friendly with the Chinese Communist Party, and they tend to tailor their activism to fit the global strategies of the CCP.”¹⁷²

Some have drawn direct connections between the anti-base movement and Beijing. The only known official report on the issue comes

¹⁶⁸Maki Kimura, “The Anti-US Military Base Struggle in Okinawa, Japan,” *Open Democracy*, February 13, 2016.

¹⁶⁹Kimura, 2016.

¹⁷⁰Gordon Chang, “Now China Wants Okinawa, Site of U.S. Bases in Japan,” *Daily Beast*, June 26, 2017. China frequently uses Chinese students and scholars associations worldwide to carry out monitoring and surveillance of overseas students, engage in influence operations, and support the work of its diplomatic missions in demonstrating adulation for visiting top leaders or presenting a unified front in challenging positions that China opposes. For an example, see Bethany Allen-Ebrahmanian, “China’s Long Arm Reaches into American Campuses,” *Foreign Policy*, March 7, 2018.

¹⁷¹Interview with Japan government official, Tokyo, January 16, 2019.

¹⁷²Michio Ezaki, “Kick out US Bases from Okinawa and Jeju, and China Will Build Their Own,” *Japan Forward*, June 13, 2017.

from Japan's Public Security Intelligence Agency in the 2016 iteration of *Review and Prospects of Internal and External Situation*, which states that China has attempted "to form public opinion in Okinawa in its favor, by approaching 'groups for Ryūkyū independence' which were calling for 'removal of all bases from the Ryukyus.'"¹⁷³ Murai Tomohide, a professor at Japan's National Defense Academy, claims that Beijing seeks to divide Japan and prompt pro-China sentiment from Okinawans.¹⁷⁴ Accordingly, one would expect to see Chinese attempts to undermine Japanese rule on Okinawa. In the past, Chinese officials' statements or articles on platforms closely tied to Beijing have either challenged Japan's sovereignty of the Ryūkyū Island chain (of which Okinawa is a part) or failed to affirm Japanese sovereignty.¹⁷⁵ One Japanese analyst said China sends its officials to Okinawa to contact these groups and promote independence, which could undermine the U.S. defense posture in the prefecture.¹⁷⁶ The Public Security Intelligence Agency report supports this, stating that Chinese universities and think tanks play a leading role in promoting academic exchanges and deepening ties with groups and organizations in Japan promoting independence of the Ryūkyūs as a way "to form a favorable public opinion in Okinawa and to attempt [to foster or exploit] division[s] in Japan."¹⁷⁷

China's influence activities in Okinawa are difficult to gauge, but anecdotal reporting suggests they do exist.¹⁷⁸ It does not have a large ethnic Chinese population or clan associations that could be vulnerable to Chinese influence. Local elites are also not eager for Chinese investment funds that would make them vulnerable to elite capture. Similarly, there is no widespread presence of UFWD proxy groups.

¹⁷³Public Security Intelligence Agency (Japan), *Annual Report 2016: Review and Prospects of Internal and External Situations*, Tokyo, Japan, January 2017.

¹⁷⁴Tritten and Chiyomi Sumida, 2013.

¹⁷⁵For examples, see Chang, 2017.

¹⁷⁶Interview with Japan political/defense analyst, Tokyo, January 16, 2019.

¹⁷⁷Public Security Intelligence Agency, 2017, p. 23.

¹⁷⁸Russell Hsiao, "A Preliminary Survey of CCP Influence Operations in Japan," *China Brief*, Vol. 19, No. 12, June 26, 2019a.

Japan has only one counterpart office for CPAFFC in Tokyo and a branch of CCPNR and no confirmed presence of COFA or CZG.¹⁷⁹ Similar to the situation in the Philippines, although Okinawa has a sizable anti-base population, these people are not pro-China.¹⁸⁰ Moreover, polls show that people in Okinawa can both oppose U.S. basing but support a U.S. alliance.¹⁸¹

Also similar to the case in the Philippines, anecdotes of attempts at more-direct Chinese activity exist but are not conclusive. For example, one interviewee noted that questions have surrounded a particular Japanese construction company in Okinawa that worked on runway construction at Naha Airport.¹⁸² Another example cited by interviewees notes the possibility that Chinese buyers might have taken ownership of an apartment complex overlooking the Japan Air-Self Defense Force base in Naha.¹⁸³ These are anecdotes, however, with little concrete supporting evidence.

Response to Perceived Disinformation

Although Japan is not nearly as proactive as Singapore, Tokyo is working to address possible disinformation. Prior to the 2018 Okinawa public referendum, LINE worked to fact-check news.¹⁸⁴ Similar fact-checking was done by Okinawa's local dailies before the September 2018 gubernatorial election.¹⁸⁵ The national government was involved

¹⁷⁹ Author email correspondence with Japan government official, June 2019.

¹⁸⁰ Interview with Japan political/defense analyst, Tokyo, January 16, 2019.

¹⁸¹ An April 2017 poll conducted by NHK found that, compared with 48 percent of Okinawans feeling U.S. bases are not needed or dangerous, 65 percent feel that the U.S.-Japan security treaty is necessary. Kōno, 2017.

¹⁸² Interview with Japan government official, Tokyo, January 16, 2019.

¹⁸³ Interview with Japan political/defense analyst, Tokyo, January 16, 2019.

¹⁸⁴ "(Recruiting at LINE@) Information and Opinions on Fake News in the Okinawa Public Referendum [【LINE@で募集中】沖縄県民投票のフェイクニュース情報 意見]," *Okinawa Times*, January 7, 2019.

¹⁸⁵ "Okinawa Dailies Fact-Check, Debunk Rumors Spread During Gubernatorial Race," *Mainichi*, October 1, 2018; "Why Is Hate Speech and Fake News Against Okinawa Spreading? Is There Hope for the Internet Era? 'Fact Check' Discussion (2)

with the December 2018 *National Defense Program Guidelines*, noting that “manipulating foreign country’s public opinion by exploiting social media” is a threat to undermining one’s sovereignty.¹⁸⁶ Reports in January 2019 said Tokyo had plans to come up “with a set of measures aimed at preventing the spread of false online information . . . particularly during elections and disasters.”¹⁸⁷ This plan, still in formulation as of this writing, “may include requesting that major U.S. technology companies and other information providers voluntarily formulate a code of conduct” and calling on Japan-based tech companies—such as LINE Corp. (owned by a South Korean company) and Yahoo Japan Corp. (owned by a Japanese company)—to improve measures that combat the spread of misinformation on their platforms.¹⁸⁸

Simply put, battling possible disinformation does not rise to a priority level of concern in Japan. A prominent reason is that Japan sees China’s task at penetrating Japan as too difficult.¹⁸⁹ This perception stems from several factors, such as Japan still relying heavily on traditional media (including print media and the state-owned NHK), the Japanese language being seen as too difficult a barrier, and anti-Chinese sentiment among the public that results in consumers immediately disbelieving anything appearing even remotely friendly to China.¹⁹⁰ Japan’s real concern, voiced by defense specialists and included

[なぜ沖縄に対するフェイク情報、ヘイト言説が流れるのか? ネットの時代に希望はあるのか? 「ファクトチェック」座談会【2】],” *Ryūkyū Shimpō*, May 24, 2019.

¹⁸⁶Government of Japan, *National Defense Program Guidelines for FY 2019 and Beyond*, Ministry of Defense (Japan), December 18, 2018, p. 3.

¹⁸⁷Kyodo, “Japan Plans to Take Steps Against ‘Fake News’ by June,” *Japan Times*, January 14, 2019.

¹⁸⁸Kyodo, 2019.

¹⁸⁹Anne-Marie Brady, in personal communications with the authors, warns that this might be too rosy an assessment, noting that much of China’s influence in Japan stems from long-standing united front work. Such works often consists of “friendly exchanges” between Chinese academics and legislators and their Japanese counterparts and “Chinese people’s organizations” that can bring Japanese students and business people to China for visits where they can be wooed and cultivated.

¹⁹⁰Interview with a Japanese government official, Tokyo, January 16, 2019; interview with a Japan political/defense analyst, Tokyo, January 16, 2019.

in Japan's strategic documents (such as the 2018 *National Defense Program Guidelines*), is potential cyber activity targeting Japan.¹⁹¹ This activity is considered much more dangerous and is suspected of already being employed against Japan.¹⁹²

Conclusion

The three cases suggest that China is not engaged in actively spreading disinformation on social media or any digital platform in Singapore, the Philippines, or Japan, as is the case in Taiwan. Disinformation operations exist in all three countries, but evidence suggests they are largely domestic in origin and undertaken for domestic political purposes. Still, China is not forgoing attempts to increase its influence in these countries; quite the contrary. Understanding that much of the evidence found in this research is anecdotal and suspected but not confirmed, we tentatively conclude that China is likely attempting to build influence in these countries but via more-traditional influence operations rather than via social media. There are four possible hypotheses that could explain the apparent lack of Chinese disinformation activity in these three countries.

Taiwan Is Unique

The first hypothesis is that China's disinformation campaigns focusing on Taiwan are unique. China views Taiwan as an inherent part of China; the two share the same language and history and have similar cultural identities; and there exists a pro-unification population in Taiwan itself. This political dynamic does not exist anywhere else in the Indo-Pacific region, so it is doubtful that China could succeed in disinformation campaigns elsewhere even if it wanted to, particu-

¹⁹¹ The focus on cyber is one of three new domains that the Japanese government laid out in the 2018 iteration of the strategic document. The other two are space and the electromagnetic domain. See Government of Japan, 2018.

¹⁹² Interview with a Japanese government official, Tokyo, January 16, 2019; interview with a Japan political/defense analyst, Tokyo, January 16, 2019.

larly when large segments of regional populations hold anti-Chinese sentiment.

Taiwan Is Where China Is Field-Testing Its Social Media Disinformation Capabilities

A second hypothesis is that China is perfecting its capabilities in Taiwan for later use elsewhere in the region. Accordingly, although there are no evident Chinese disinformation campaigns in the three countries we examined in this chapter, China is learning what works and what does not work from its experiences in Taiwan and will be better positioned to employ these tactics, once perfected, more broadly throughout the region. Indeed, as this study was wrapping up in August 2019, early indications began to emerge that suggested China had initiated a widespread disinformation campaign against Hong Kong in response to societal protests over the erosion of the city's legal autonomy, incompetence on the part of Chief Executive Carrie Lam, widespread police violence, and allegations of police cooperation with organized crime groups.¹⁹³ Evidence has also emerged that China might be actively engaging in social media manipulation in Australia, mostly targeting the ethnic Chinese community there.¹⁹⁴ It is not yet clear how effective such a disinformation campaign might be, nor is it certain that such campaigns have China's official sanction, but they will merit watching and comparing with the campaigns that China has launched against Taiwan in the past several years.

China Finds Other Tools Better Suited to Its Goals in These Other Cases

A third hypothesis is that China is not conducting disinformation campaigns in these countries because doing so would work against its interests. China has the technical capabilities to conduct these operations, as the situation in Taiwan demonstrates. Unlike Russia, China

¹⁹³Laurie Chen, "China Troll Army's Battle Expeditions Leap Great Firewall to Target Hong Kong Anti-Government Protests," *South China Morning Post*, August 8, 2019.

¹⁹⁴Steve Cannane and Echo Hui, "Federal Election 2019: Anti-Labor Scare Campaign Targets Chinese-Australians," ABC Australia, May 2, 2019.

does not seek simply to disrupt the internal affairs of large numbers of other countries to cause chaos; China seeks influence; it seeks to counteract or neutralize threats and to pave the way for its rise in the region. Disinformation campaigns are geared more toward generating instability, which is not conducive to generating influence, particularly because instability is difficult to control. Accordingly, China dedicates time and resources to building influence in regional countries via such programs as the Belt and Road Initiative. If China's intention is to project an image as a benevolent power, discovery of a disinformation campaign would ruin this image and thus negate diplomatic and economic outreach.¹⁹⁵

Substantial Chinese Disinformation Is Going Undetected

A final possibility is that a large volume of disinformation is going unrecognized for what it is or being misattributed to other actors, whether local or foreign. Although this is logically possible, the fact that Chinese disinformation appears to have been fairly quickly identified in the case of Taiwan (and in the case of attacks on the Hong Kong protest movement) suggests that this is a less probable, perhaps impossible, explanation. Furthermore, Singaporean counterintelligence and policing authorities are alert to the risk of Chinese influence operations more generally, are widely able to read Chinese-language sources, and are particularly concerned about disinformation circulating on social media—therefore, such an explanation seems even more implausible. In Japan, where another highly capable domestic intelligence service has been on alert for Chinese influence operations in Okinawa and elsewhere and where the ability to read Chinese is partly facilitated by the shared nature of characters as part of the Japanese language, this

¹⁹⁵ Anne-Marie Brady points out in a communication with the authors that Chinese diplomats under Xi Jinping also engage in “undiplomatic diplomacy,” attacking foreign governments, activists, and the media in an effort to enhance in-group identification among domestic and overseas Chinese audiences. Although some comments along these lines are reported in foreign-language media outlets, many others are not; consequently, China is often able to show both a soft/attractive side and a hard/frightening aspect without having to choose between the two or pay overly high costs for frequent efforts to intimidate adversaries and warn fence-sitters.

explanation seems similarly difficult to credit. Only in the Philippines, where the state counterintelligence apparatus is weak and there are relatively lower levels of familiarity with Chinese languages, does such an explanation seem potentially plausible—although, again, disinformation campaigns were also identified in the case of the Philippines, even if they seemed to originate from the country’s own political circles and not advance goals that China would likely see as attractive.

It is difficult to conclude with certainty which hypothesis is most likely. One of the main reasons is temporal; the nonexistence of disinformation campaigns might not hold true in the future. If, for example, the YouTube videos incident in Singapore is of Chinese origin, then China is already testing its techniques outside Taiwan and might do so again. Therefore, one cannot falsify Hypothesis 2. Similarly, there are large populations of ethnic Chinese throughout the region. Although the existence of a diaspora population of ethnic Chinese is by no means synonymous with a community defined by pro-China sentiment, we believe that China will focus its targeting on ethnic Chinese first because Beijing regards ethnic Chinese as more likely to be receptive to its messages.¹⁹⁶ Therefore, one cannot falsify Hypothesis 1, particularly if parts of the Chinese diaspora community prove receptive to Chinese messaging. That said, given the deep anti-China sentiment in Japan and the Philippines, it is hard to imagine pro-China messaging resonating in these countries.

Hypothesis 3 stands as the most likely, but even this is not without problems. Although the cases show that China is operating to gain influence via traditional means—aid, investment, and diplomacy—in the Philippines and Singapore, there is not much activity in Japan. Where we do see Chinese disinformation operations, the messages and means are adaptive, but the objective appears to be framing China as a nonaggressive, normal country that others can trust. This might be difficult, however, given the presence of anti-Chinese views in some parts of these countries where Chinese are regarded as unwelcome

¹⁹⁶Anne-Marie Brady points out, in a personal communication with the authors, that Chinese influence campaigns differentiate between foreign target nations with large overseas Chinese populations and those with small diaspora communities.

guests, a cause of societal ills, and/or potential fifth columnists for Beijing. Still, as one Filipino official framed it, even if China's efforts are not successful at converting local populations, these efforts could still succeed over time by reducing anti-Chinese sentiment, even by a little.¹⁹⁷ This approach becomes more detrimental when it accompanies messaging that questions a country's reliance on the United States—or, worse, that actively plays up rumors of negative behavior by the United States or U.S. citizens to shape a distorted narrative about the United States. As noted above, Hypothesis 4 seems the least likely for a variety of reasons.

Although disinformation campaigns exist, we have shown in this chapter that such campaigns are predominantly domestic in origin in Singapore, the Philippines, and Japan. These campaigns largely use publicly accessible social media, such as Facebook, and traditional media platforms. Of the three countries examined, only the Philippines appears to be experiencing a constant disinformation campaign, including activity prior to elections, and the techniques in this campaign appear to be improving. The campaigns in Singapore and Japan largely appear to be opportunistic and adhere to no obvious pattern, though it is possible that they are merely extremely well disguised or not the main focus of efforts in those countries.¹⁹⁸ Although it is impossible to judge the level of activity in closed messaging boards, none of the interviewees we spoke with said that they believed this to be an important vector of Chinese influence on social media, even anecdotally. Importantly, there is no evidence of social media disinformation campaigns targeting the military in the three countries.

Perhaps the most important finding is that, although little evidence ties disinformation campaigns in these three countries to China, there is evidence of Russian ties to the Philippines and possible trans-

¹⁹⁷Interview with Philippine government official, Manila, May 2019.

¹⁹⁸Anne-Marie Brady, in personal communication with the authors, points out that Chinese influence operations are usually highly tailored to the societies being targeted, and thus might look quite different from one country to another, making it more difficult than might otherwise be expected to divine any "pattern." Influence operations, if they vary from one country to another, might logically adopt differentiated approaches to the employment of social media disinformation campaigns within the overall influence effort.

mission of disinformation techniques. Furthermore, depending on the Philippines' reliance on Huawei or China Telecom, there could emerge a real possibility of China increasingly (1) engaging in espionage and surveillance of users using the network and (2) leveraging its access in malicious ways, such as backdoor intelligence-gathering. For now, although China has a growing capacity to influence the Philippines, there is no evidence to support the argument that China is directly involved in spreading disinformation on social media in that country.

Conclusion and Recommendations

The results of our study indicate that China is using Taiwan as a test bed for developing attack vectors using disinformation on social media. To date, in the case of Taiwan, China's use of disinformation has achieved mixed and somewhat limited results that are primarily in the political domain, not the military operational one. We found no evidence that China has carried out substantial disinformation operations against other U.S. allies or partners, including Singapore, the Philippines, or Japan. Nonetheless, Chinese disinformation campaigns could be directed against the United States in the event of a crisis or conflict. In this chapter, we turn to the challenging task of trying to draw insights from the preceding chapters to provide informed speculation about how China might use social media disinformation campaigns against USAF in advance of and during a military confrontation. We conclude with recommendations and some thoughts on future trends that might tip the balance.

Notional PRC Employment of Social Media Disinformation to Target the U.S. Military

Unlike Western military thought that has tended to distinguish between peacetime and wartime, CCP thinking about the nature of international affairs and armed conflict elides any easy distinction between preconflict and conflict. Western thinking about conflict can be rather legalistic and dichotomous (either peacetime or wartime, akin to a light switch that is either on or off), but Chinese Commu-

nist writings and practice tend to reflect a more continuous, sliding scale perspective on conflict (analogous to a rheostat). Additionally, the CCP's view is that it is on the defensive, and the PLA's doctrine of *active defense* [积极防御] gives it full license to respond, even preemptively, to the threats posed by external actors, or *hostile foreign forces* [敌对势力].¹

This is not to say that the distinction between peacetime and wartime is entirely absent in Chinese thinking; as one Taiwan PLA watcher commented, "In peacetime, the PLA's focus is on Taiwan's society and economy, but in wartime [we expect] they will focus on the ROC's armed forces."² Nonetheless, and especially in light of the experiences of Taiwan described in this report, it makes sense to examine the prospect that Chinese uses of disinformation to target USAF or the U.S. military more broadly might be ongoing during what is nominally peacetime.

As China moves to incorporate social media further into its military operations, it will increasingly engage in some level of shaping operations during what Western observers would consider the "preconflict" stage. Should outright kinetic exchanges appear imminent or actually occur, an elevated level of disinformation should be expected, accompanied by messages aimed at such key groups as senior political and military leaders, service members and their families, and base hosting communities. Given China's control over the Chinese-language social media platform WeChat and a general belief among PRC authors that the global ethnic Chinese diaspora is a favorable vector of influence for Beijing to leverage, China will likely seek to communicate directly with Chinese-American military officers and personnel and their families, attempting to turn them against any U.S. policies or operations that China finds objectionable. Chinese disinformation efforts also will likely seek to introduce information that is difficult for the United States to definitively refute, either because doing so would require revealing classified

¹ Fravel, 2019.

² Interview with Taiwan think-tank analyst, interview 12B, Taipei, January 2019.

information or because it is impossible to disprove a negative. These issues are explored in this chapter.

Preconflict Operations

For China, “the goal is not a knock-out. . . . [I]t’s to weaken and increase distrust in the government,” one Taiwan official commented, adding that “this is an approach of ‘death by a thousand cuts.’ In peacetime, China seeks to erode trust; in wartime, they seek to leverage the experience with social media they’ve gathered during peacetime.”³ The 2013 *Science of Military Strategy* explained that the PLA should “create a favorable posture for the initiative prior to combat,” which includes “flexibly applying psychological warfare means to shake the opponent, and split up and disintegrate the opponent’s war foundation” using the “synthetic application of political, economic, diplomatic, legal, and public opinion means.”⁴ Applied to the United States, this would presumably mean efforts to weaken the supporting infrastructure that the United States needs to conduct military operations.

As noted, the U.S.-Japan alliance and U.S. access to bases, air stations, facilities, and supporting infrastructure in Japan are critical to U.S. military operations in the Indo-Pacific. Given the sensitivities associated with the U.S. presence and history in Okinawa, China might seek to play on such issues as crime, noise, pollution, environmental damage, or operational accidents and mishaps—issues that other studies have noted are already serious preexisting sources of tension in the relationships between the U.S. forces and Japan, the U.S. forces and the Okinawa community, and Tokyo’s own domestic relationship with Okinawa.⁵ In light of this, Chinese social media disinformation could seek to further undermine support for U.S. base presence in and opera-

³ Interview with Taiwan politician, interview 7, Taipei, January 2019.

⁴ People’s Liberation Army Academy of Military Science Military Strategy Department, 2013, p. 129.

⁵ Dennis Blair and James Kendall, *U.S. Bases in Okinawa: What Must Be Done, and Quickly*, Washington, D.C.: Sasakawa Peace Foundation, 2015; Emma Chanlett-Avery and Ian Rinehart, *The U.S. Military Presence in Okinawa and the Futenma Base Controversy*, Washington, D.C.: Congressional Research Service, 2016.

tions out of Okinawa by spreading rumors about another rape or other criminal action by U.S. military personnel or contractors, or by doctoring imagery of a U.S. military platform to suggest that there had been an accident.⁶ Although these activities would represent an uptick in Chinese targeting of the U.S. military via social media, they could be somewhat deniable and might even allege that the United States was involved in a cover-up as a way to explain the absence of credible and definitive supporting evidence to back up the alleged crimes or disasters. Similarly—and linked to both Okinawan resentment and broader Japanese public opinion that opposes the introduction of nuclear weapons into Japanese territory (something the United States had previously done under secret agreements with Japan during the 1960s and 1970s as part of the Okinawa reversion agreement⁷)—Chinese disinformation might allege that any USAF B-2 and B-52 bombers rotating through or transiting Japan on strategic deterrent missions were armed with nuclear weapons. Such claims would be difficult or impossible to disprove despite being untrue and, if skillfully executed, could inflame Japanese public opinion against the alliance.

Separately, in a period of heightened tensions between China and the United States or its allies and partners, China might seek to induce doubt about U.S. reliability. Chinese content farms and clandestine accounts could hint that the United States has given Beijing private assurances that it does not want conflict and will not intervene in the event of a clash between the PLA and the ROC armed forces (Taiwan) or over Chinese claims to the Senkakus (Japan) or various features in the South China Sea (the Philippines). Such promises would purportedly be secret agreements, perhaps described as part of a quid pro quo on some other issue of substance to the United States,

⁶ Regular U.S. military operations out of Okinawa have experienced a series of accidents and near disasters that have raised concerns among the local population over the past decade, most notably over the issue of rotary-wing airframes operating over densely populated areas. There have been a small number of crashes, hard or forced landings, and parts that have fallen off U.S. airframes. In particular, the MV-22 *Osprey* has attracted substantial concern over its safety record.

⁷ “Japan Officially Gave U.S. Consent to Bring in Nuclear Weapons Ahead of Okinawa Reversion Accord: Document,” *Japan Times*, August 14, 2017.

such as trade deficits, or countering North Korean or Iranian proliferation. U.S. disavowal of such claims might not succeed in convincing worried Taiwan, Japanese, or Filipino audiences that Washington truly intended to support those countries in the event of a conflict with China, perhaps even making central governments more prone to compromise or seek accommodation on Chinese terms. Past and/or current instances of real or perceived U.S. unreliability—such as the failure to intervene in the 1956 Hungarian uprising, the 1961 Bay of Pigs invasion in Cuba, the 1968 Prague Spring in Czechoslovakia, the 1991 flight of Shi'a and Marsh Arabs of Southern Iraq from Saddam Hussein, or the 2019 betrayal of the Kurds of Northern Syria—might be cited by Chinese propagandists seeking to sow doubts about U.S. intent to betray an ally.

A separate type of disinformation campaign might seek to influence USAF operations during an imminent or ongoing kinetic exchange.

Social Media Disinformation Operations During a Conflict

Were China and the United States to come into open conflict over some issue—most likely Taiwan, but possibly a Chinese effort to seize the Senkakus from Japan, a disputed feature in the South China Sea, a North Korea contingency, or a China-India border clash—China might seek to leverage social media disinformation campaigns as part of a broader collection of tools used to complicate, hamper, degrade, or defeat U.S. military operations. At least five possible Chinese approaches are worth considering.

First, China might seek to encourage ethnic Chinese-American officers and service members not to follow orders or to disbelieve the reasons for the conflict by presenting information that seeks to (1) position Chinese-American military personnel as owing their loyalty to China, and (2) present China's case as reasonable and worthy of support—as one Taiwan official commented, China “targeting [ethnic] Chinese communities in Canada, Australia, and the United States.”⁸ Communicating in Chinese language on Chinese government–dominated social and tra-

⁸ Interview with Taiwan politician, interview 7, Taipei, January 2019.

ditional media platforms (many of which are accessible in the United States and overseas), China would likely attempt to induce doubt about the wisdom of U.S. policy, lower morale, spur opposition to confronting China militarily, and (in the most ambitious “reach” goal) encourage defections. None of this is intended in any way to say that Chinese-Americans would respond to such PRC disinformation campaigns as China would hope, but it is certainly the case that the CCP regards the global Chinese diaspora as a vector of influence.

Second, if the United States were to come to the aid of Taiwan during a conflict, China might seek to complicate coordination among Taipei, Washington, and Tokyo by hinting that Japan had received a quid pro quo for permitting the U.S. military to conduct operations out of bases in Japan in support of Taiwan. The most plausible rumor that Chinese disinformation could seek to sow would be a variant of the rumor that the Tsai administration was going to lease Taiping Island to the United States. That might take the form of disinformation suggesting that Washington had secretly promised Tokyo that it would formally recognize Japan’s territorial claims to the Senkaku Islands (claimed by Taipei as the Diaoyutai [釣魚台]). Indeed, the islands have been a source of tension between Taipei and Tokyo as far back as the mid- to late 1960s and as recently as mid-2018.⁹ Such a rumor could wrong-foot Washington, put pressure on Taipei, and lead Tokyo to be more cautious.

Third, China might try to spread rumors that create an impression that the United States had conducted a strike that unintentionally killed U.S. allies or Chinese civilians. In other contexts, the Taliban has routinely engaged in disinformation intended to suggest that U.S. airstrikes had gone astray, killing innocent civilians. In an attempt to turn public opinion against the U.S. war effort, Chinese disinformation might claim that the United States had hit and sunk a civilian ship from Taiwan, or that the United States had committed war crimes by targeting Chinese civilians inside the PRC. Fake content created by Chinese agents could also seek to shake or reshape U.S. support for the

⁹ Shin Kawashima, “The Origins of the Senkaku/Diaoyu Islands Issue,” *Asia-Pacific Review*, Vol. 20, No. 2, 2013; Stacy Hsu, “Taiwan Asserts Sovereignty over Diaoyutai,” *Taipei Times*, July 19, 2018.

continuation of combat operations against China by alleging that the United States had lost a major exchange, suffered a catastrophic accident, and/or lost the initiative.

Fourth, PRC disinformation teams might seek to degrade unit morale in the wake of a kinetic exchange by claiming that one or more commanders or unit leads had deserted or defected. Such disinformation is not likely to reach U.S. forces directly during the heat of battle because social media access during such a contingency would likely be highly restricted—or perhaps completely shut off—for U.S. forces. However, in keeping with the comment by one former high-ranking Taiwan defense official that China is “attacking our military through our population,” such information might be intended to filter back to the fielded force through comments that China delivers to families of military personnel or the general public.

Finally, China could attempt to target base-hosting communities in the United States and especially overseas. Here, efforts could be made to convince populations surrounding key nodes from which the United States operates that, if they do not speak out against the war, the consequences of the conflict will affect them shortly in the form of PRC attacks. The goal here would be to encourage a country—such as Japan or the Philippines—to deny the United States the use of basing and facilities or to sway local U.S. communities to speak up and act out in ways that might constrain (or entirely prevent) use of base facilities by USAF personnel and platforms.

Unlike kinetic strikes or cyber operations that can achieve results in hours, minutes, or even seconds, social media disinformation operations often take a substantial period of time—days, weeks, or even longer—to achieve their effects, though in some cases the effects can be quite rapid and potentially achieve wider effects than a localized kinetic weapon. Additionally, unlike kinetic activities (but more akin to cyberattacks), conducting the equivalent of battle damage assessments in the aftermath of a social media disinformation campaign is in many cases quite challenging. It is rare that the results of a given piece of disinformation are as directly visible as the 10,000 people who gathered in Taipei to protest against the Tsai government’s alleged plans to ban the burning of ghost money and firecrackers. For these reasons, China is likely to use

such operations only as a small part of its overall effort during an actual conflict. As one former Taiwan defense official stated, Chinese social media disinformation campaigns are best conceived of as a “quasimilitary approach—[to succeed,] they need to be incorporated into a conventional, symmetric, linear [set of military operations].”¹⁰ Another Taiwan defense expert concurred, commenting that disinformation operations are part of China’s overall “technical reconnaissance and three warfares” and that these are always “embedded in a broader effort.”¹¹

Still, if included as part of a well-designed strategic messaging and psychological warfare operation and executed in tandem with other lines of effort designed to complicate, degrade, or defeat U.S. military operations, such disinformation campaigns on social media can be, as one Taiwan interviewee commented, “as powerful as a missile.”¹² Another interviewee made similar comments, remarking that “fake news *is* war . . . and information war can be [more effective] than missiles.”¹³ This reflects perceptions among Taiwan residents about the impact of social media disinformation, especially the potential to shape public perceptions without the use of force.

Although China has targeted Taiwan with disinformation, there is little evidence that China has targeted the United States or the U.S. military with the types of disinformation campaigns on social media seen in the cases of Taiwan or Hong Kong.¹⁴ This could change if China were to assess that the likelihood of an armed confrontation with the United States was rising and/or imminent. Next, we discuss some current and possible trends in Chinese uses of disinformation on social media; policy options for the United States; and recommendations.

¹⁰ Interview with retired Taiwan military officer, interview 4B, Taipei, January 2019.

¹¹ Interview with Taiwan cyber expert, interview 9, Taipei, January 2019.

¹² Interview with Taiwan academic, interview 8, Taipei, January 2019.

¹³ Interview with Taiwan government official, interview 10B, Taipei, January 2019.

¹⁴ Alyza Sebenius, “Facebook, Twitter Can’t Find China Election Meddling Trump Claims,” Bloomberg, October 24, 2018.

Policy Options and Recommendations

To respond effectively, the case study of Taiwan suggests that defense against social media disinformation should be treated akin to ballistic missile defense, with “multilayered defenses required—these should be whole of military, whole of government, and whole of society.”¹⁵ Although China does not appear to have employed social media disinformation campaigns against the United States or its military to date, it behooves the United States to prepare for the likelihood that the PRC (with its belief in the importance of information as the ultimate high ground and psychological warfare as an integral component to modern conflict) might use these tools in a crisis or contingency involving the United States. Preparing USAF, the joint force, DoD, the interagency (efforts that extend across DoD and other U.S. departments), and the U.S. government to defeat Chinese social media disinformation will, therefore, require a multifaceted approach (Table 6.1).

Recommendations for Air Force Special Operations Command and the Joint Force

Consider Incorporating Adversary Social Media Disinformation into Red-Teaming or Wargaming, Possibly with an Eye Toward Future Incorporation into Training and Exercises

In this report, we have largely focused on issues of policy during peacetime and crisis, but DoD—and, specifically, USAF—are ultimately required to prepare for the possibility of an outbreak of armed conflict requiring a response involving the use of military force. Training and exercising, both alone and in tandem with allies and partner nations, are essential components of maintaining readiness, operational effectiveness, and preparedness. For DoD and USAF, it might prove valuable to consider incorporating disinformation operations into future service-specific, joint, and partner-focused military training and exercises, at both the command post and field levels. Although our research

¹⁵ Interview with Taiwan civil society activist, interview 1A, Taipei, January 2019.

Table 6.1
Summary of Recommendations

Recommendation	AFSOC/ Joint Force	DoD	Interagency	U.S. Government
Incorporate adversary social media disinformation into red-teaming and wargames	X			
Engage base communities	X			
Raise awareness of Chinese malign activities on social media	X			
Train the joint force and DoD personnel to recognize and resist foreign media disinformation campaigns		X		
Explore the cost and benefit of passive vs. active, technological vs. human responses to defeating disinformation campaigns		X		
Establish a trusted online presence			X	
Consider establishing a presence on Chinese platforms			X	
Protect and reach out to build, increase and preserve trust with Chinese-Americans and Taiwanese-Americans				X
Build a database of examples of Chinese social media disinformation				X
Engage allies and partners				X
Balance global counter-influence efforts				X

did not identify how best to include disinformation operations into U.S. military planning and exercises, it did suggest that doing so now would be advantageous as a way to think through how China might seek to target the U.S. military during a crisis or contingency, and how best to defeat such a disinformation campaign. It is worth noting that Taiwan has recently moved to incorporate Chinese disinformation into its annual *Han Kuang* military exercises as a way to explore how such situations might unfold and affect military operations and effectiveness.¹⁶

¹⁶ Duncan DeAeth, "Taiwan Military Holds First-Ever Simulated 'Anti-Fake News' Exercises," *Taiwan News*, April 22, 2019.

With respect to countering Chinese disinformation campaigns on social media, the emphasis for Air Force Special Operations Command, and USAF more broadly, should be on service members in the Indo-Pacific Command region. Beyond exercises, day-to-day instruction on what constitutes disinformation and important indicators for such activity would be useful for troops and their families. Equally, asking service members to identify, flag, and collect disinformation observed in the local community would help in building a database of Chinese disinformation (discussed in a later section).

Engage Base Communities

Improving awareness of foreign manipulation—and resilience against it—among U.S. service members on social media will not be sufficient if local communities in host nations fall victim to the same disinformation, thus undermining support for U.S. presence and operations. All U.S. service members should be looking for evidence of activities aimed at base communities. Peacetime engagement to build familiarity and trust can also help improve ties and local resilience for when Chinese activities escalate. These efforts should focus especially on the families of U.S. service members who come from local communities and can serve as a bridge both for disinformation into USAF but also for counter-disinformation efforts to the host nation.

Raise Awareness of Chinese Malign Activity on Social Media

Members of the joint force might benefit from being better informed about the themes that China seeks to convey via overt propaganda accounts, such as Xinhua and China Daily. In educating the joint force about PRC propaganda more generally, DoD might find it beneficial to alert service members more specifically to China's view of information as a domain of warfare and its increasingly active use of disinformation, including material conveyed via social media, to achieve strategic and tactical aims in undercutting the morale and unity of PRC adversaries. More specifically, it might be useful to occasionally brief selected service members working in the Indo-Pacific theater on overview information about the local social media platforms adopted in their countries or areas of responsibility (such as PTT and LINE in Taiwan).

Recommendations for DoD

Train the Joint Force and the Broader DoD Workforce to Recognize and Resist Foreign Disinformation Campaigns

A key focus of any effort to degrade or defeat disinformation campaigns must be to prepare U.S. military personnel to recognize and resist disinformation and prepare proper, effective responses. This will require sensitizing the force to the vectors, patterns, themes, and goals of foreign (and in this case, specifically Chinese) adversaries who seek to target the United States military on-line. Occasional briefings about themes in Chinese disinformation that may be employed to target the force could be helpful and cost-efficient.

Explore Costs and Benefits of Passive vs. Active and Technological vs. Human Responses to Adversary Disinformation Campaigns

As a first step, DoD and USAF should, if they have not already, begin thinking about whether and how to respond to the rise of social media disinformation campaigns, including whether passive or active responses are better and whether, if active responses are preferred, these are better advanced through technology and human operators.¹⁷ As shown by the cases of Taiwan, Singapore, the Philippines, and Japan, different countries are adopting a variety of possible responses to the rise of social media disinformation campaigns. These range from relatively passive responses that favor a broad “marketplace of ideas” defense to a more top-down reaction intended to leverage the strength of the state and the legal system. Some broad decisions will lie with Congress, the executive branch, and the judiciary. Others might fall more appropriately within DoD’s or the Services’ prerogatives to set policy for staff and service members.

In Taiwan, an extremely small number of civil society groups with minimal funding have been somewhat effective in identifying

¹⁷ Other elements of a response could be legal measures mandating take-down and penalizing deliberate and harmful disinformation; partnering with civil society; broader efforts to raise consciousness and media literacy in U.S. society or in societies where DoD and USAF specifically require basing access, support, or overflight; eliciting support from private sector social media firms; or other steps.

and discrediting Chinese disinformation operations. For example, Taiwan's CoFacts (with roughly ten part-time volunteer editors) and the Taiwan Fact Check Center (with just four full-time staff) have already played key roles in raising consciousness, initiating discussions of policy options for responding, and exploring technology solutions for flagging and processing information of concern.¹⁸ With substantially greater resources and the ability to task trained, full-time, professional defense and military personnel to respond to a Chinese social media disinformation threat during a crisis or contingency, DoD might be better positioned to counter this threat than Taiwan. Additionally, through DoD's abilities to direct resources to the Defense Advanced Research Projects Agency, commission research and development by private-sector technology firms, and engage in contracted direct support, it should be possible to improve substantially on Taiwan's ability to counter Chinese disinformation.

Recommendations for the Interagency

Establish Trusted Online Presence for Credible Communication

Efforts to counter Chinese social media disinformation are broader than simply those involving DoD. Other departments and agencies will have important roles to play, though DoD could be an integral part of any effort to respond to Chinese disinformation in a crisis. To play a full role, DoD should develop a trusted online presence so that it has a voice and an ability to push back should the PRC launch a disinformation campaign on social media, including on platforms popular in Asia. U.S. law, DoD policy, and USAF service guidelines regulate the types of accounts, content of messages, rules governing transparency, requirements for preservation, and other aspects of online accounts and platforms on which DoD and USAF operate.¹⁹

¹⁸ Interviews with Taiwan civil society activists, interviews 1A and 1B, Taipei, January 2019; interview with Taiwan civil society activist, interview 11, Taipei, January 2019.

¹⁹ Chief Information Officer, "Web and Social Media Policies," webpage, undated. USAF policy sets mandatory public communications policy on public release of information.

For its part, the U.S. Department of State operates on several social media platforms for worldwide communications, such as Dip-Note Blog, Facebook, Flickr, Instagram, LinkedIn, Medium, Snapchat, Twitter, and YouTube.²⁰ USAF, at least as of 2013, had established official accounts on Facebook, Flickr, Twitter, Vine, and YouTube, and the Air Force Live Blog.²¹

Consider Establishing a Presence on Chinese Platforms

A final possibility to consider further would be for military and civilian disinformation operators to establish accounts on Chinese-language social media now, building up trusted profiles that could be leveraged in the event of a crisis or conflict. To do that, disinformation teams will need accounts, followers, a familiarity with censorship practices, and fluency in the world of online social media communications in Chinese. These things are not easily acquired, so it might be worth investing in acquiring them now for potential future use.

The U.S. military should explore opening accounts on Weibo and WeChat, especially if the Chinese military opens an account on Twitter or other major U.S.-based social media platforms. Some U.S. government organizations have accounts on Chinese social media, such as the U.S. embassy in Beijing, though these are subject to Chinese censorship. Nevertheless, more U.S. accounts would expand the reach of U.S. messaging in peacetime and provide some semblance of reciprocity for Chinese state-run media presence on Western social media.

USAF, Policy Directive 35-1, March 8, 2018.

²⁰ U.S. Department of State, "Global Social Media Presence," webpage, undated.

²¹ USAF, *Air Force Social Media Guide*, 4th ed., 2013.

Recommendations for U.S. Government

Engage Chinese-Americans and Taiwanese-Americans to Resist Hostile Social Media Campaigns

As we have noted, Chinese writings and practice both suggest that the PRC approach to disinformation is most likely to target ethnic Chinese abroad by leveraging China's control over and influence on global Chinese-language media platforms, including social media giant WeChat. For this reason, Chinese-American military personnel and DoD officials and their families might merit particular attention in preparing to identify and resist PRC disinformation operations on social media. Indeed, Chinese-Americans and Taiwanese-Americans serving in U.S. government positions might constitute something akin to first responders in medical emergencies or instances of terrorism—first on the scene and best positioned to recognize and assist others in identifying and reacting to an instance of PRC disinformation. PRC disinformation is not guaranteed to always be crafted in Chinese language or distributed across Chinese social media platforms, and DoD will have to guard against assuming that the only threat vectors are those that would be in Chinese on Chinese social media. Still, it seems likely that Chinese-Americans and Taiwanese-Americans will be at least as well and perhaps better positioned than their non-Chinese-speaking colleagues to detect and identify Chinese disinformation campaigns.

Additionally, as the Taiwan case shows, even the families of high-ranking Taiwan government officials proved vulnerable to PRC disinformation (in the case of disinformation about the breadth, depth, and timing of pension reform). This suggests that the families of Chinese-American and Taiwanese-American defense officials and military personnel are also likely to be exposed to Chinese disinformation—perhaps even more likely than those serving in government or military positions. These family members could constitute vectors by which information is spread but could also be seen as force multipliers, additional sensors, and intelligence collectors whose linguistic competencies and understanding of both cultural nuances and political realities in China, Taiwan, or elsewhere in the Indo-Pacific are likely to vastly

surpass those of most DoD and USAF personnel. Families are not under any official obligation to assist DoD or USAF in identifying or responding to Chinese disinformation campaigns, but early and regular outreach to Chinese-American and Taiwanese-American officials and service members might help build additional channels of trust, respect, and feedback that can prove useful in helping their families resist PRC efforts to use them as influence channels.

Build a Database of Chinese Disinformation on Social Media

Interviewees suggested that China might have targeted Taiwan with as many as tens to hundreds of thousands of individual instances of disinformation over the past three years.²² At present, however, it does not appear that any comprehensive database of Chinese disinformation campaigns or messages exists; compilation of such a database could prove a valuable resource for any effort to identify signature indicators and warnings and/or to improve the abilities of those targeted by Chinese disinformation to recognize and resist such campaigns.

Engage Allies and Partners to Learn and Share Best Practices

China does not have to effectively target U.S. citizens to have an impact on U.S. operations in Asia. U.S. access to allies' military bases and facilities plays a critical role in U.S. power projection around the world, including in Asia, so a successful campaign to undermine allied general public and/or elite support for U.S. military access can indirectly, but quite concretely, affect U.S. operations for an Asia contingency.

Many U.S. government organizations can be involved in the effort to track, analyze, and counter Chinese disinformation campaigns. The Department of State's Global Engagement Center is already carrying out some of this work. The Intelligence Community should also engage with U.S. allies and partners. DoD can engage regional militaries to discuss how to counter adversary disinformation on social media plat-

²² Various interviews, Taipei, January 2019. An additional complicating factor is definitional: whether an instance of fake news is (1) the creation of the false information and posting it to the web or (2) the accessing of such disinformation. In this study, we have opted to define an instance of *disinformation* as the fake news story itself; determining the number of unique hits and/or the reception of content by those accessing it is inordinately difficult.

forms based in allied and partner nations, such as Kakao Talk, LINE, and others. This discussion could clarify the legal authorities held by regional governments and the requirements that such governments would have of any information (intelligence) the U.S. government might want to provide to generate action against suspected adversary actors. U.S. allies and partners in Asia (Australia, Japan, New Zealand, the Republic of Korea, Singapore, and Taiwan), Europe, and Canada, among others, would likely all have valuable insights to contribute in developing a shared understanding of Chinese influence and interference operations.

Continually Reassess Where Best to Expend Resources to Counter Chinese Global Influence Efforts

Despite clear evidence of Chinese social media manipulation against Taiwan, there is less evidence of similar activity in other countries of the region. China is using many other tools to accomplish its influence campaign in those places, including traditional media, political lobbying, and economic coercion. Although it is imperative to acknowledge the risk of greater Chinese social media manipulation in the future, especially in the event of a crisis or contingency, the absence of Chinese efforts to target the United States in this way to date suggests that the United States might be best off preparing initial steps to guard against the possibility of competition with China in this area and, given limited U.S. government resources, reserving its greatest efforts for countering Chinese influence and interference operations in other areas. We would recommend that any efforts focused on social media first address Chinese-owned platforms, such as WeChat and Weibo, which are clearly conduits for Chinese information operations abroad. Still, should the U.S. Intelligence Community, DoD, or USAF detect evidence that the PLA is moving to employ social media disinformation against the United States, the lessons and recommendations in this report provide insights regarding how such a campaign might evolve and a prospective road map of how to counter it effectively.

Future Trends

Going forward, two key trends are worth noting in regard to disinformation operations conducted via social media, one of which is general and one of which is specific to China today.

First, disinformation campaigns benefit from the relative anonymity and ambiguity associated with cyberspace and social media postings. Social media and the online domain are not static, unchanging mediums, however; as technology evolves, artificial intelligence can be leveraged to identify an instance of disinformation as soon as it is posted or circulated. On the other hand, many observers warn that increasingly advanced artificial intelligence could make social media disinformation easier, cheaper, and more believable—leveraging voice capture, facial mimicking, the internet of things, and geotracking to present increasingly plausible misrepresentations of reality. In such a world, the “offense-advantaged” environment could evolve toward an “offense-dominant” situation in which discerning falsehood from truth becomes increasingly problematic.

Separate from these theoretical speculations, Taiwan interviewees described China’s disinformation operations as becoming increasingly sophisticated. “Two years ago it was easy to tell content from China,” said one official, “but today they’re getting better.”²³ Another commentator agreed, stating that “China’s disinformation is getting better at sounding authentically Taiwanese. They are either learning or hiring people on the ground in Taiwan [or both].”²⁴ Another Taiwan defense expert agreed, stating that although “most Chinese disinformation efforts over the past few years [were] pretty awkward and ineffective . . . due to the sloppiness and cockiness of the PLA . . . the content has been improving [recently].”²⁵ And a fourth observer characterized China as “nativizing” its messaging and content terms in ways that more accurately mimic how people in Taiwan communicate.²⁶ In the past, Chinese postings would

²³ Interview with Taiwan government official, interview 6A, Taipei, January 2019.

²⁴ Interview with Taiwan politician, interview 7, Taipei, January 2019.

²⁵ Interview with Taiwan think-tank analyst, interview 2A, Taipei, January 2019.

²⁶ Interview with Taiwan academic, interview 8, Taipei, January 2019.

sometimes use simplified characters or expressions found only in China; today, content is increasingly expressed in traditional characters and in ways that echo how people from Taiwan express themselves.

At the same time, China's disinformation campaigns are in a race against time with Taiwan society, where younger social media users are savvier and the whole of society is gaining in media literacy and awareness that the threat of PRC-originated fake content is growing. The Taiwan government is also improving its response time and leveraging legal and policy tools to encourage social media platforms to take down false content sooner. As one Taiwan defense expert commented, "we're only concerned about the first 24–48 hours of an instance of disinformation; after that time frame, it has either gone viral or gotten trapped in the bubble [of closed-circle communications online]."²⁷ A Taiwan official noted that "48 hours is too long to wait to take down a piece of disinformation; six hours is the time frame that the media in Taiwan works on," meaning that the government must be extremely quick to respond if it detects an instance of hostile social media disinformation.²⁸

Final Thoughts

China's growing facility with disinformation campaigns conducted via social media is part of its broader pattern of employing technical reconnaissance and psychological, legal, and public opinion warfare (the three warfares) as part of its information operations in a strategic support role for its military objectives. The reorganization of the PLA since 2015, including the establishment of the PLASSF, appears to have strengthened Chinese interest in and ability to execute disinformation campaigns. Additionally, the 2016 election of Tsai Ing-Wen has incentivized the PLA and broader Chinese Party-state apparatus to explore ways to target Taiwan with disinformation, a trend that appears to have further strengthened through the island's 2018

²⁷ Interview with Taiwan think-tank analyst, interview 2A, Taipei, January 2019.

²⁸ Interview with Taiwan government official, interview 10A, Taipei, January 2019.

midterm elections.²⁹ As research on China's influence operations has shown, it is possible to disaggregate, analyze, and understand Chinese thinking and practice of disinformation, including issues of C2, targeting, required supporting infrastructures and conditions, themes, and implications. Although other Asian nations do not appear to have been targeted by Chinese disinformation campaigns to date, the experiences of Taiwan can be particularly useful in understanding the threat posed by China's disinformation operations.³⁰

An effective response to such threats requires studying adversary capabilities and preparing a multilayered set of defenses. Many interviewees we spoke with stated that, in important ways, such defenses are analogous to ballistic missile defense, with no single defense sufficient but many active and passive defenses collectively working to blunt the effect of such campaigns. This report is intended as a first step to aid efforts focused on blunting and defeating inbound Chinese disinformation campaign threats on social media.

²⁹ Jessica Drun, "Taiwan's Social Media Landscape: Ripe for Election Interference?" Center for Advanced China Research, blog post, November 13, 2018; Kathrin Hille, "China's 'Sharp Power' Play in Taiwan," *Financial Times*, November 21, 2018.

³⁰ For a discussion of the Taiwan case, see Rong-I Wu, Russell Hsiao, J. Michael Cole, William Stanton, Mark Stokes, and Stephen M. Young, *The Global Taiwan Brief*, Vol. 3, No. 24, December 12, 2018.

Potential Chinese Vulnerabilities to Social Media–Based Information Operations

If China were to commence a campaign of social media disinformation intended to target and compromise the U.S. military’s ability to gain reliable access to the Indo-Pacific and/or operate effectively in and around that region, several options would be available to the United States. Among these would be to attempt deterrence through denial; i.e., the United States would take steps to harden itself and defeat such disinformation efforts (as explored in the preceding chapters), making it undesirable for China to continue such a campaign by rendering it a waste of effort (or perceived waste of effort). An alternative approach would be to attempt deterrence by punishment; i.e., the United States would threaten to impose unacceptably high costs on China if the latter continued to direct disinformation campaigns against U.S. interests.¹

The latter approach would pose several challenges, among them clarity of communication and credibility, an ability to commit to termination, and questions about legality and commensurateness with U.S. values; still, it might not be impossible and U.S. policymakers pondering how to respond to the Chinese disinformation threat might wish to at least consider deterrence by punishment rather than dismiss it outright.²

¹ Marcus Weisgerber, “U.S. Military Should Add Deception to Its Playbook, Pacific Air Forces General Says,” *Defense One*, December 18, 2019.

² Such considerations could affect the effectiveness of any such campaign were the United States to conduct it purely clandestinely (i.e., undetected) as opposed to covertly (or with plausible deniability), because a key feature of deterrence by punishment is usually considered to be the clear and credible signaling of a consequence (here, the United States sowing

Adoption of such an approach by the United States could involve use of a wide variety of cross-domain policy tools, such as diplomatic signaling and pressure, information and disinformation operations, military responses, or economic sanctions. A comprehensive description of the possible ways that the United States might engage in deterrence through punishment of Chinese disinformation campaigns lies outside the scope of this study, but we can provide a limited examination of the possibility of engaging in an information operations version of what is referred to in the cyber community as *hack-back*, an in-kind, same-domain response to an adversary intended to halt provoking actions that initiated the tit-for-tat exchange.

In this appendix, we consider some of the possible ways that the U.S. military could target China with disinformation. Researching this topic presents a substantial methodological challenge; for the most part, Chinese authors do not write about the attacks that U.S. disinformation campaigns could best leverage to inflict damage on the PLA or on China more broadly, nor is it possible to elicit information regarding such questions through direct engagement with PLA officers or Chinese state officials. Therefore, this chapter's findings are necessarily somewhat speculative and rely in substantial measure on evaluations of China's history of military conflicts and accidents, broader knowledge of PLA and CCP vulnerabilities and concerns, and possible future weaknesses. Any decision by the U.S. military to actually adopt deterrence by punishment through disinformation campaigns would warrant a more thoroughgoing assessment of the costs, risks, and benefits that might be associated with such an approach; the following analysis constitutes simply an initial sketch of what such an approach might involve.

disinformation about China) if the adversary does not cease its hostile actions (PRC disinformation targeting the United States). Further research on the requirements for and possible ramifications of such an approach would be merited.

Anxieties About Social Media–Based Information Operations

Chinese leadership has made clear that it is deeply concerned by the potential of “dangerous” outside information to “infiltrate” China, fearing it would disrupt domestic social stability and even undermine the CCP’s rule. In 2013, Xi Jinping warned darkly that “Western forces hostile to China and dissidents within the country are still constantly infiltrating the ideological sphere,” and told the Party to “strengthen guidance of public opinion on the Internet [and] purify the environment of public opinion on the Internet.”³ For the PLA, social media is considered first as a threat and only second as an opportunity. This trend echoes China’s overall view of the phenomenon as noted by other authors looking at the issue, who have noted that China first identified key influencers online and brought them under control or shut them down, only later turned to social media as a means of spreading disinformation and extending its control.⁴ The 2009 social media–fueled protests in Iran appear to have brought the risks of this new form of communication to the attention of the PLA, especially in relation to its fundamental mission of keeping the CCP in power.⁵ The 2015 version of the *Science of Military Strategy* reflects the PLA’s early concerns, before it transitioned to offensive applications:

Since the beginning of the 21st century, cyberspace has been used by some countries to launch ‘color revolutions’ against other countries. The political turmoil that has erupted in the Middle East and North Africa in recent years is often dominated by behind-the-scenes operations using social networking sites such as Twitter and Facebook as the engine, from manufacturing network public opinion to inciting social unrest. As a result, national

³ Chris Buckley, “China Takes Aim at Western Ideas,” *New York Times*, August 19, 2013; “Document 9: A ChinaFile Translation,” ChinaFile, November 8, 2013.

⁴ Elizabeth C. Economy, *The Third Revolution: Xi Jinping and the New Chinese State*, New York: Oxford University Press, 2018.

⁵ Chi Yannian [迟延年], “Cyber Subversion: Security Threats That Must Not Be Taken Lightly [网络颠覆: 不容小觑的安全威胁],” *China Defense News*, August 6, 2009, p. 3.

governments lacking the strategic means for cyberspace military struggle have continued to collapse.⁶

There are characteristics of the Chinese military and CCP system that might represent vectors by which these institutions could be targeted, such as the PLA's widespread corruption and factional division, the risk of Chinese casualties in a conflict (including, in part, the PLA's growing reliance on the private sector for maintenance and repair and for support services and maritime intelligence, surveillance, and reconnaissance), and perceptions that the PLA is serving the interests of the CCP and not the nation (drawing contrast between a party vs. national army).

Military Corruption Wastes Citizens' Money

Chinese leaders, and the leaders of the PLA specifically, know that corruption is a major institutional and political problem. Former President Hu Jintao even warned in 2012 that corruption “could prove fatal to the party and even cause the collapse of the party and the fall of the state.”⁷ Similarly, around the same time, General Liu Yuan said in a speech, “No one can defeat China [. . .] Only our own corruption can destroy us and cause our armed forces to be defeated without fighting.”⁸ These problems went beyond simple corruption, however: “They physically attack loyal and upstanding officials, kidnap and blackmail party leaders, and drag in their superiors to act as human shields. They deploy all of the tricks of the mafia trade within the army itself.”⁹ Since assuming the leadership of the Party, the state, and the PLA in 2012–2013, Xi Jinping has launched a wide-ranging and persistent campaign against corruption that has netted numerous senior Chinese military officers, including both vice chairmen of the Central Military Commission who served with Xi from 2007 to 2012 (Gen-

⁶ Xiao Tianliang [肖天亮], 2015.

⁷ Tania Branigan, “China’s Hu Jintao Warns Congress Corruption Could Cause Fall of State,” *The Guardian*, November 8, 2012.

⁸ John Garnaut, “Rotting from Within,” *Foreign Policy*, April 16, 2012.

⁹ Garnaut, 2012.

eral Guo Boxiong and General Xu Caihou) and the PLA Chief of the General Staff from 2012 to 2017 (General Fang Fenghui).¹⁰ Although their total illicit gains are unknown, they were publicly accused of embezzling millions—meaning the number is very likely significantly higher. In 2013, Xi’s anticorruption campaign netted former Politburo Standing Committee member Zhou Yongkang, the former Secretary of the Political and Legal Affairs Commission responsible for the overall management of the regime’s internal security apparatus.¹¹ Xi’s anti-corruption drive has also led to the arrest of hundreds of lower-ranking state officials (including intelligence officers), military personnel, state-owned enterprise leaders, and even think-tank experts and academics. The CCP’s sensitivity to accusations—and evidence—of corruption by senior leadership is evident in its decision to censor and completely block the *New York Times* and Bloomberg from China for reporting on the immense wealth held by the families of former premier Wen Jiabao and Xi Jinping.¹²

A key element to understand about the anticorruption campaign is how it fits in with the factional struggle between Xi Jinping and his predecessors (Hu Jintao and—especially—Jiang Zemin) and their networks of supporters and beneficiaries, including their ties to the PLA.¹³ Not only is this corruption and factionalism a widely recognized weakness of the PLA (even seen as such by PLA authors themselves), it is also a persistent source of potential broader political instability.¹⁴ A central argument of much of the literature on changes in the PLA since 2015

¹⁰ Charles Clover, “Xi Takes Aim at Military in Anti-Graft Drive,” *Financial Times*, February 11, 2018.

¹¹ Michael Forsythe, “Zhou Yongkang, Ex-Security Chief in China, Gets Life Sentence for Graft,” *New York Times*, June 11, 2015.

¹² David Barboza, “Billions in Hidden Riches for Family of Chinese Leader,” *New York Times*, October 25, 2012; Barbara Demick, “The *Times*, Bloomberg News, and the Richest Man in China,” *New Yorker*, May 5, 2015; “Xi Jinping Millionaire Relations Reveal Fortunes of Elite,” Bloomberg, June 29, 2012.

¹³ Bo Zhiyue, “Guo Boxiong, Jiang Zemin, and the Corruption of the Chinese Military,” *The Diplomat*, July 31, 2015.

¹⁴ Michael S. Chase, Jeffrey Engstrom, Tai Ming Cheung, Kristen Gunness, Scott W. Harold, Susan Puska, and Samuel K. Berkowitz, *China’s Incomplete Military Transformation:*

has been that these changes are driven by Xi Jinping's need to establish a firm grip on the PLA as a way of dealing with the threats that corruption and factionalism pose to his personal rule and the PLA's operational effectiveness.¹⁵ Therefore, any social media messages that reveal true corruption and factional intrigue or that create perceptions of high-level corruption hampering the common soldier's ability to fight and backroom dealing between rival military factions might give senior leadership pause in pursuing a war in the face of divided command. Such messages also might generate a lack of support among the general public stemming from troops not being well served by their commanders.

Other possible themes are corruption among military-linked industrial concerns, such as Aviation Industry Corporation of China Heavy Machinery Co., the Poly Group, or other firms;¹⁶ among Chinese united front organizations, such as the China Energy Fund Committee;¹⁷ or in contracts associated with the Belt and Road Initiative.¹⁸

Chinese Casualties Are Unacceptable

Although China has the world's largest population, its birth rate has been slowing since it implemented the One China Policy in the late

Assessing the Weaknesses of the Chinese People's Liberation Army (PLA), Santa Monica, Calif.: RAND Corporation, RR-893-USCC, 2015.

¹⁵ Phillip C. Saunders and Joel Wuthnow, "China's Goldwater-Nichols? Assessing PLA Organizational Reforms," *INSS Strategic Forum*, April 2016; Joel Wuthnow and Phillip C. Saunders, *Chinese Military Reforms in the Age of Xi Jinping: Drivers, Challenges, and Implications*, Washington, D.C.: National Defense University Press, 2017.

¹⁶ An Baijie, "Oversight of Military Firms on Rise," *China Daily*, June 5, 2014; Sam Cooper and Doug Quan, "How a Murky Company with Ties to the People's Liberation Army Set Up Shop in B.C.," *Vancouver Sun*, August 26, 2017.

¹⁷ U.S. Attorney's Office Southern District of New York, U.S. Department of Justice, "Patrick Ho, Former Head of Organization Backed by Chinese Energy Conglomerate, Sentenced to 3 Years in Prison for International Bribery and Money Laundering Offenses," March 25, 2019.

¹⁸ Will Doig, "The Belt and Road Initiative Is a Corruption Bonanza," *Foreign Policy*, January 15, 2019.

1970s and has continued to slow even as this policy has been relaxed to allow two children for all families under President Xi. Two generations of only children have created an immense cultural focus on the value and importance of children for supporting parents and older relatives as the country's average age increases. Therefore, it might be possible for the U.S. military to erode PLA morale and broader PRC support for any conflict by playing up the theme of unacceptable losses for the Chinese population, focusing particularly on Chinese families.

As China has sought to develop additional military effectiveness, it has increasingly focused on the need to leverage support services from the Chinese private sector. China also often engages in political-military contests with its neighbors using a gray-zone approach centered on involving nonuniformed combatants, such as its purportedly commercial fishing fleet. (Many of these sailors are themselves members of the maritime militia.¹⁹) Under certain circumstances, the PLA's ability to achieve desired effects might be complicated by these approaches to supporting, maintaining, and repairing military hardware or escalating tensions with neighbors while trying to remain below a given threshold that would elicit a reaction. China's dependence on people who are not military professionals, whose levels of discipline and training might be less than military grade, and who might not have signed up for combat with the world's foremost military power might open the PLA to levels of vulnerability, including in the information space, that it has underappreciated. For example, if maintenance and repair personnel from firms that manufacture China's military hardware or communications technologies are convinced that they are being asked to risk their lives to carry out repairs, or if they are exposed to information that suggests the PLA suspects them of engaging in sabotage, they might simply decline to report for duty when called. Similarly, if members of China's fishing fleet are exposed to rumors that the United States has begun sinking Chinese fishing vessels operating in areas where the PLA is also present, they might be less willing to put to sea.

¹⁹ On the Chinese maritime militia, see Andrew S. Erickson, "The China Maritime Militia Bookshelf: Complete with Latest Recommendations & Fact Sheet," webpage, May 21, 2019.

Although U.S. military policy likely would not permit the targeting of civilians in ordinary circumstances, China's deliberate blurring of the lines between civilian and military actors might change that, especially if supported by an announcement that the United States had observed and would target "illegal combatants." A well-timed reference to the 2018 U.S. targeting of Russian mercenaries in Syria could reinforce a message that the gloves had come off and induce greater caution in Chinese forces and their supporting elements.²⁰

PLA Does Not Represent or Fight for China's National Interests

The PLA's status as the armed wing of the CCP, not a national military, opens it to accusations that it does not represent the interests of the Chinese nation and Chinese people. At various times in the past, most notably in the Tiananmen Square massacre of June 3–4, 1989, the PLA has damaged its reputation with the Chinese public by following orders that benefited the Party over the people, and this represents a continuing source of concern for PLA and CCP leaders. CCP and PLA elites are sensitive to suggestions that the Chinese military should become a national military.²¹ Consistent exhortations for loyalty to the Party and public statements by senior officials against "nationalization"—especially at important anniversaries, such as Tiananmen Square in 2009, or leadership transitions, such as from Hu to Xi in 2012—suggest that this is an issue of deep concern for the PLA.²² Therefore, Chinese propaganda frequently strives to portray the PLA as one with the Chinese nation, presenting the "dream of a strong military" [强军梦] as the logical cor-

²⁰ Thomas Gibbons-Neff, "How a Four-Hour Battle Between Russian Mercenaries and U.S. Commandos Unfolded in Syria," *New York Times*, May 24, 2018.

²¹ Minnie Chan, "The Tiananmen Crackdown Ignited a Decade of Debate on the Chinese Military's Role, and Where Its Loyalties Should Lie," *South China Morning Post*, December 7, 2018b.

²² Ben Blanchard, "China General Tells Troops Party Trumps State," Reuters, April 1, 2009; Liz Carter, "Whom Should the Chinese Army Serve—the Party or the State?" *The Atlantic*, October 25, 2012; Michael Chase, "Army Day Coverage Stresses PLA's Contributions and Party Control," *China Brief*, Vol. 12, No. 16, August 17, 2012; Huang Jingjing, "A More Loyal PLA Rebuffs the Heresy of Separating the Party and Military," *Global Times*, June 9, 2017.

ollary to Xi Jinping's "China dream" [中国梦] of national rejuvenation. Creating doubts about the accuracy of this narrative might strike a chord with some of the Chinese public and/or service members, and might be especially useful for messaging as deterrence by punishment.

Will to Fight and the Horrors of War

The PLA's lack of combat experience since 1979 means that, despite impressive military hardware and China's military buildup over three-plus decades, one of the biggest looming questions is how the human component of the military will perform in a conflict. Just as there are concerns that the PLA might trick military personnel in Taiwan or other countries into believing that other units are abandoning their posts or that the general lack of a will to fight means individual resistance to a Chinese invasion is futile, similar doubts could be created on the Chinese side. PLA officials publicly address the troops' "peace disease" and the need to cultivate "courage," especially among the younger generation, which is often perceived as weaker and less willing or even able to struggle through adversity.²³ Creating or amplifying operational-level units' concerns about the horrors of war and their colleagues' willingness to fight could affect personnel morale and suggest to PLA leadership that its lack of fighting force means a war is unwinnable.

Lack of Chinese Public Support for War

Although China is an authoritarian state ruled by the CCP, the CCP is acutely aware of public opinion and takes great effort to ensure Party support, or at least tolerance, by the wider population. With only 80 million Party members among 1.4 billion citizens, the Party's effort to maintain at least the façade of public support is perhaps most visible in the great expenses the CCP incurs to guide, control, and censor public discussion online as part of its broader domestic propaganda apparatus. In wartime, the CCP will certainly take great effort to rally the population around the flag for the cause of the war. Creating or

²³ Ryan D. Martinson, "The Courage to Fight and Win: The PLA Cultivates Xuexing for the Wars of the Future," *China Brief*, Vol. 16, No. 9, June 1, 2016.

amplifying public opinion online that opposes the war—for whatever reason—might generate enough opposition to have an actual impact on Chinese military operations (such as starting protests), or it could lead the Chinese leadership to reconsider its calculus about going to war under the perception of lacking public support.

Exposing Chinese Misdeeds

The Chinese military is always careful to frame its actions in terms of defensive responses to foreign aggression, so discrediting this idea could have an impact on the lower ranks of the Chinese military and on public support for the war. The United States could track, name, shame, and indict Chinese disinformation practitioners, whether uniformed or operating in support of the Chinese Party-state or military. In 2014, the United States indicted five uniformed PLA officers for cyber intrusions against U.S. commercial and private-sector entities, an event that appeared to catch China off guard and represented an instance of strategic surprise.²⁴ Subsequently, the United States also targeted Russian disinformation actors, indicted North Korean hackers, and revealed personal details about operational cyber actors in China.²⁵ Such actions might impose discrete costs on specific elements of the PLA and, in so doing, affect Chinese disinformation employment.

Intelligence Exploitation

The Chinese military is well aware that social media has turned every soldier into a potential walking transmitter of open-source information, and military leaders have sought to tighten control over soldiers' access to and use of smartphones and social media.²⁶ Concerns over the use of

²⁴ Michael S. Schmidt and David E. Sanger, "5 in China Army Face U.S. Charges of Cyberattacks," *New York Times*, May 19, 2014.

²⁵ Christopher Bing and Sarah N. Lynch, "U.S. Charges N. Korean Hacker in Sony, Wanna-Cry Cyberattacks," Reuters, September 6, 2018; Josh Chin, "Cyber Sleuths Track Hacker to China's Military," *Wall Street Journal*, September 23, 2015; Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, February 27, 2019.

²⁶ Celina Ge, "PLA on Call: China's Military Orders Anti-Spy Software for Soldiers' Smartphones," *South China Morning Post*, April 19, 2016.

social media to identify or improve strike targeting for precision weapons (a key way of war for the U.S. military and its allies and partners) highlight the military's recognition of the operational implications of social media's real-time data transmission and content-sharing.²⁷ Similarly, concerns over *catfishing*—use of fake identities designed to lure someone into a mistaken belief they have developed an online relationship (romantic or professional)—reflect a lack of operational security trust within the PLA.²⁸

Vulnerabilities to Social Media–Based Information Operations

Despite the rich environment of hundreds of millions of Chinese social media users and a cornucopia of readily acknowledged Chinese concerns about social media, the reality is that translating this theory into practice against China might be difficult. U.S. operators face several real-world constraints. First, China's online censorship apparatus is certainly the best in the world, meaning that any U.S. narratives that became popular could simply be censored. An alternative solution would be to attempt to evade, degrade, or dismantle the Chinese internet censorship system, but this could be seen as threatening CCP power. Second, the CCP has spent billions of dollars limiting the ability of its citizens to mobilize for mass protests like they did in Tiananmen. However, protests numbering several thousand people do happen occasionally, perhaps even routinely, and sometimes have an impact on local policy.²⁹ Third, the ability to create or amplify messages within China requires a forward presence. Although this might be the simplest problem to solve, China's ostensible real-name registration system for many social media platforms adds a layer of difficulty to such operations.

²⁷ Yuan Ke [袁轲], Zhang Haijuan [张海娟], Liu Zhe [刘哲], 2012.

²⁸ Xia Yuren [夏育仁], 2015.

²⁹ Minnie Chan, "Chinese Protesters Blame Fracking for Earthquakes that Killed Two People in Sichuan," *South China Morning Post*, February 26, 2019a.

Opportunities for Exploitation

A key element shaping the effectiveness of an instance of disinformation is its believability. One way the PLA and the broader Chinese community supporting military operations (political leaders, PLA members' families, private-sector firms on which the PLA relies) might be targeted via disinformation would be to damage morale and distract PLA and PRC leadership with a manufactured crisis—for example, suggesting that a military setback or disaster has occurred. Such an approach could play up news of purported military setbacks or accidents that are actually U.S. disinformation campaigns modeled after actual events from the PLA's own past.

Over the past 70 years, the PLA has twice clashed directly with the United States (once during the Korean War and later during the U.S. war in Vietnam), both times suffering enormous casualties while fighting under technologically adverse conditions (though the PRC's historiography retells both war clashes as victories of standing up to U.S. imperialism). Additionally, China was forced to stand down in the 1954 and 1958 Taiwan Strait crises, and again in 1995–1996 when it sought and failed to coerce Taiwan during that country's first democratic election for the presidency. Chinese forces were also handily defeated by the rear echelon troops of the Socialist Republic of Vietnam when the PRC invaded its southern neighbor in 1979. And China claims that the United States deliberately struck the PRC's embassy in Belgrade during the course of 1999 NATO operations aimed at compelling the Milosevic regime in Serbia to cease its ethnic cleansing campaign in Kosovo (Chinese propaganda claims this action was aimed at humbling China as a rising power.³⁰) These conflicts, setbacks, and humiliations could provide a model for crafting a disinformation campaign aimed at shaping impressions inside China generally and the PLA more specifically so that key actors in the Chinese system become convinced that they are losing and should wind down military operations before a true calamity occurs.

³⁰ For a recent look, see Kevin Ponniah and Lazara Marinkovic, "The Night the US Bombed a Chinese Embassy," BBC, May 7, 2019.

Paired with broader political-military conflicts, U.S. disinformation operations targeting the PLA could also play off past disasters suffered during research and development and/or training and exercises. PLA history also offers several disasters that U.S. disinformation campaigns could use as models, thus increasing campaign realism by appearing similar to past accidents and catastrophes. Some examples of these past military accidents and disasters are deaths related to failures of the PLA's space launch vehicle and ballistic missile programs in Sichuan in 1995 and 1996, the loss of a submarine with all hands on board in 2003, a pair of J-15 carrier jet crashes in 2016, the crash of a J-11B PLAAF fighter in November 2017, separate crashes of a J-15 fighter and a Y-8 modified refueling aircraft in early 2018, and the fatal crash of an unspecified fighter jet in Hainan Island in 2019.³¹

In seeking realism, it is worth bearing in mind that the PLA and the PRC military more broadly rarely provide many initial details when a disaster occurs, and they actively seek to present any outcome—even setbacks—in the best possible light.³² U.S. propaganda might wish to mimic such approaches, proclaiming the heroism of naval crews when they disastrously mishandle their platforms and extolling the bravery of individual pilots whose aircraft malfunction. Chinese audiences have decades of experience reading between the lines on propaganda and might be able to understand that news reporting of a major disaster as a

³¹ Choi Chi-yuk, "Fatal Crash of Chinese J-15 Carrier Jet Puts Question Mark over Troubled Programme," *South China Morning Post*, July 27, 2016; Minnie Chan, "'At Least 12 Crew Members Killed' in Chinese Military Plane Crash," *South China Morning Post*, February 1, 2018a; "Chinese Rocket Tragic Accident" video, YouTube, aired on Discovery Channel, uploaded by ChenchyFlaky September 6, 2006; Ryan Pickrell, "A Chinese Navy Fighter Jet Crashed on a Chinese Island in the South China Sea, Killing Both Pilots," *Business Insider*, March 12, 2019; Sebastien Roblin, "In 2003, a Chinese Submarine Was Lost at Sea. How the Crew Died Is Terrifying," *The National Interest*, March 25, 2018.

³² A classic example of the PLA seeking to deceive even its own commanders about its failings and put a good face on a military setback occurred during the April 2001 crash of a PLA Navy fighter into a U.S. EP-3 maritime patrol craft in international airspace south of Hainan Island. PLA Navy pilot Wang Wei, who died in the incident, was killed when his escape hatch and parachute malfunctioned; he was later proclaimed a "Guardian of Territorial Airspace and Waters." See Minnie Chan, "How a Mid-Air Collision Near Hainan 18 Years Ago Spurred China's Military Modernization," *South China Morning Post*, April 2, 2019b.

heroic victory wherein the motherland's brave sons laid down their lives actually means that a large number of PLA personnel were killed; this could have desired effects on morale and support for any war effort.

China's own broad use of disinformation against its own population—for this is exactly what censorship and propaganda actually amount to: a deliberate distortion of true news and the creation of an artificial narrative intended to replace reality with social (or political) reality—is actually an enormous vulnerability of the Chinese system, particularly the relatively nontransparent PLA and the broader CCP that it serves. As a consequence of the CCP's long history of distorting, covering up, and outright lying to its own people, many Chinese information consumers engage in worst-casing and conspiracy theorizing, and tend to believe that things must be worse—sometimes much worse—than they are reported to be (and sometimes believe them to be worse than they actually are).³³ China has long been considered a “low trust society” and the PRC's own government propaganda and media have carried articles about the problems this can cause for politics and society.³⁴ Such an unfortunate (if largely self-created) situation poses several opportunities for U.S. disinformation campaigns, should the U.S. military determine that it would be beneficial to target the PLA or broader Chinese system with disinformation.

Conclusion

Any determination that the U.S. military, much less USAF, should move to engage in an active disinformation campaign targeting the PLA or broader Chinese society lies beyond the scope of this study. The possible themes we have suggested should be seen as starting points for thinking about such issues rather than firm recommenda-

³³ For one example about panicked buying of salt in response to a DPRK nuclear test, see Laurie Burkitt, “Fearing Radiation, Chinese Rush to Buy . . . Table Salt?” *Wall Street Journal*, May 17, 2011.

³⁴ He Dan, “Trust Among Chinese ‘Drops to Record Low,’” *China Daily*, February 18, 2013; Mark Magnier, “A Crisis of Trust Takes a Toll on Chinese Society,” *Los Angeles Times*, September 24, 2006.

tions about how such operations should be conducted. Experts disagree about whether the advantages or drawbacks of such a campaign are greater. Chinese leaders express substantial anxiety about the possibility of their control over the information channels to the PLA and the Chinese people more broadly, meaning that contesting these could be both escalatory and highly effective. At the same time, China's ability to drown out foreign messaging—and the fact that such a campaign would play into long-standing PRC propaganda themes centered on foreigners attempting to undermine the CCP—could lead to a rally-around-the-flag effect if such disinformation were discovered. It is unclear just how much restraint China exercises in the realm of disinformation or whether U.S. efforts to target China with disinformation would lead to escalation or de-escalation.

As part of deterrence by punishment, some tit-for-tat responses in this domain might be advisable or even necessary, although the merits of an all-out effort to undermine CCP rule via social media disinformation lie beyond the focus of this report and are a matter to be determined by policymakers. The CCP is particularly worried about controlling speakers of Cantonese and residents of Hong Kong, so if China begins targeting Chinese-American service members with disinformation, the U.S. military could consider targeting these populations with anti-CCP messages. If China begins targeting specific U.S. government officials, then the United States could seek to release information about the true wealth of senior Chinese officials. If China spreads disinformation to U.S. allies and partners in an effort to inflame public opinion against U.S. basing and military operations, then the United States could consider releasing data about the actual terms of often-secret Chinese infrastructure investment in those countries.

References

“88% Okinawa Base Burden ‘Too Big,’ Asahi Newspaper Prefectural Survey [沖縄の基地負担「大きすぎ」88% 朝日新聞社県民調査],” *Asahi Shimbun*, February 19, 2019, p. 3.

Ai Jun, “Singapore’s Hypocrisy Exposed by Seized Military Vehicles,” *Global Times*, November 27, 2016.

Allen, David, “Marine Killed by Blast on Okinawa Is ID’d,” *Stars and Stripes*, March 27, 2009.

Allen-Ebraharian, Bethany, “China’s Long Arm Reaches into American Campuses,” *Foreign Policy*, March 7, 2018. As of December 19, 2019: <https://foreignpolicy.com/2018/03/07/chinas-long-arm-reaches-into-american-campuses-chinese-students-scholars-association-university-communist-party/>

Altshuler, Tehilla Shwartz, and Rachel Aridor-Hershkovitz, “Israel’s Proposed ‘Facebook Bill,’” *Lawfare*, August 6, 2018. As of August 7, 2019: <https://www.lawfareblog.com/israels-proposed-facebook-bill>

An Baijie, “Oversight of Military Firms on Rise,” *China Daily*, June 5, 2014. As of December 20, 2019: http://www.chinadaily.com.cn/china/2014-06/05/content_17563486.htm

Aspinwall, Nick, “‘We Are Filipinos, and We Hate China’: China’s Influence in the Philippines, and Backlash Against Tsinoys,” *SupChina*, June 6, 2019.

“Authorities Deny Rumor of Ban on Incense, Ghost Money Burning,” *FocusTaiwan*, July 21, 2017. As of August 7, 2019: <http://focustaiwan.tw/news/aip/201707210016.aspx>

Au-Yong, Rachel, “Facing Up to Fake News: Why We Should Be Worried,” *Straits Times*, December 4, 2016.

Baker, Loren, “Fake Yahoo News Site Reports Chinese Troops Attack Okinawa,” *Search Engine Journal*, October 19, 2005.

Barboza, David, "Billions in Hidden Riches for Family of Chinese Leader," *New York Times*, October 25, 2012. As of August 7, 2019:
<https://www.nytimes.com/2012/10/26/business/global/family-of-wen-jiabao-holds-a-hidden-fortune-in-china.html>

Batongbacal, Jay L., "How to Reinvigorate the US-Philippine Alliance," *The Diplomat*, May 1, 2019.

Beauchamp-Mustafaga, Nathan, "Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations," *China Brief*, Vol. 19, No. 16, September 6, 2019.

Beauchamp-Mustafaga, Nathan, and Michael Chase, *Borrowing a Boat out to Sea: The Chinese Military's Use of Social Media for Influence Operations*, Washington, D.C.: John Hopkins School of Advanced International Studies, 2019.

Beauchamp-Mustafaga, Nathan, Cristina Garafola, Astrid Cevallos, and Arthur Chan, "China Signals Resolve with Bomber Flights over the South China Sea," *War on the Rocks*, August 2, 2016. As of August 7, 2019:
<https://warontherocks.com/2016/08/china-signals-resolve-with-bomber-flights-over-the-south-china-sea>

Beauchamp-Mustafaga, Nathan, Derek Grossman, and Logan Ma, "Chinese Bomber Flights Around Taiwan: For What Purpose?" *War on the Rocks*, September 13, 2017. As of August 7, 2019:
<https://warontherocks.com/2017/09/chinese-bomber-flights-around-taiwan-for-what-purpose/>

"Bella," "The Myth of Multiculturalism in Singapore," *Medium*, June 3, 2017. As of May 14, 2020:
<https://medium.com/@patcheezie/the-myth-of-multiculturalism-in-singapore-d0712706db4>

Bing, Christopher, and Sarah N. Lynch, "U.S. Charges N. Korean Hacker in Sony, WannaCry Cyberattacks," *Reuters*, September 6, 2018.

Blair, Dennis, and James Kendall, *U.S. Bases in Okinawa: What Must Be Done, and Quickly*, Washington, D.C.: Sasakawa Peace Foundation, 2015.

Blanchard, Ben, "China General Tells Troops Party Trumps State," *Reuters*, April 1, 2009. As of August 7, 2019:
<https://www.reuters.com/article/us-china-military/china-general-tells-troops-party-trumps-state-idUSTRE53029820090401>

———, "China Air Force Goads Taiwan with Hokkien-Language Video," *Reuters*, April 20, 2018. As of August 7, 2019:
<https://www.reuters.com/article/us-china-taiwan-defence/china-air-force-goads-taiwan-with-hokkien-language-video-idUSKBN1HR0G2>

Bo Zhiyue, "Guo Boxiong, Jiang Zemin, and the Corruption of the Chinese Military," *The Diplomat*, July 31, 2015.

- Bogunovic, Goran, "Zalo Is Vietnam's Answer to WhatsApp and It's Growing Big," *Domain.me*, November 7, 2018. As of August 7, 2019:
<https://domain.me/zalo-is-vietnams-answer-to-whatsapp-and-its-growing-big/>
- Bolsover, Gillian, "Computational Propaganda in China: An Alternative Model of a Widespread," *Computational Propaganda Research Project*, April 2017. As of August 7, 2019:
<http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-China.pdf>
- Bradshaw, Samantha, and Philip N. Howard, *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*, Oxford, UK: Computational Propaganda Research Project, December 2017. As of August 7, 2019:
<https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf>
- Brady, Anne-Marie, *Marketing Dictatorship: Propaganda and Thought Work in Contemporary China*, New York: Rowman and Littlefield, 2009.
- , *Magic Weapons: China's Political Influence Activities Under Xi Jinping*, Washington, D.C.: Wilson Center, 2017a.
- , "Plus ça change? Media Control Under Xi Jinping," *Problems of Post-Communism*, Vol. 64, No. 3, 2017b, pp. 128–140.
- , "On the Correct Use of Terms," *China Brief*, Vol. 19, No. 9, May 9, 2019a.
- , "Are We Real Friends? China–Albania Relations in the Xi Era," *Sinopsis*, October 17, 2019b. As of December 18, 2019:
<https://sinopsis.cz/en/are-we-real-friends-albania-china-relations-in-the-xi-era/>
- Branigan, Tania, "China's Hu Jintao Warns Congress Corruption Could Cause Fall of State," *The Guardian*, November 8, 2012.
- Brasor, Philip, "Japan Enters the Post-Truth Age with Distorted MXTV Report on Okinawa Protests," *Japan Times*, February 4, 2017.
- Buckley, Chris, "China Takes Aim at Western Ideas," *New York Times*, August 19, 2013. As of August 7, 2019:
<http://www.nytimes.com/2013/08/20/world/asia/chinas-new-leadership-takes-hard-line-in-secret-memo.html>
- Burkitt, Laurie, "Fearing Radiation, Chinese Rush to Buy . . . Table Salt?" *Wall Street Journal*, May 17, 2011. As of August 7, 2019:
<https://blogs.wsj.com/chinarealtime/2011/03/17/fearing-radiation-chinese-rush-to-buy-table-salt/>
- Burton, Rachael, "Disinformation in Taiwan and Cognitive Warfare," *Global Taiwan Brief*, Vol. 3, No. 22, November 14, 2018. As of August 7, 2019:
<http://globaltaiwan.org/2018/11/vol-3-issue-22/>

Butler, Steven, and Iris Hsu, “Q&A: Taiwan’s Digital Minister on Combating Disinformation Without Censorship,” Committee to Protect Journalists, blog post, May 23, 2019. As of September 17, 2019:
<https://cpj.org/blog/2019/05/qa-taiwans-digital-minister-on-combatting-disinfor.php>

Cai Yintong [蔡印同], “Study Abroad Students: An Important Force for People-to-People External Propaganda [留学生: 民间外宣的重要力量],” *International Communications* [国际传播], March 2009.

———, “Promoting Communication in Life: Talking About How to Use Foreign Students to Communicate Abroad [在生活中促进交流: 谈如何利用外国留学生开展对外传播],” *International Communications* [国际传播], March 2011.

Cannane, Steve, and Echo Hui, “Federal Election 2019: Anti-Labor Scare Campaign Targets Chinese-Australians,” ABC Australia, May 2, 2019. As of June 1, 2020:
<https://www.abc.net.au/news/2019-05-03/federal-election-scare-campaign-targets-chinese-australians/11073514>

Carter, Liz, “Whom Should the Chinese Army Serve—the Party or the State?” *The Atlantic*, October 25, 2012. As of August 7, 2019:
<https://www.theatlantic.com/international/archive/2012/10/whom-should-the-chinese-army-serve-the-party-or-the-state/264104/>

CEIC, “Taiwan Visitor Arrivals,” webpage, undated. As of August 7, 2019:
<https://www.ceicdata.com/en/indicator/taiwan/visitor-arrivals>

Central News Agency, “Sharers of Fake News about Animal Diseases Face Fines in Taiwan,” *Taiwan News*, June 27, 2019. As of August 7, 2019:
<https://www.taiwannews.com.tw/en/news/3733439>

Chan, Minnie, “‘At Least 12 Crew Members Killed’ in Chinese Military Plane Crash,” *South China Morning Post*, February 1, 2018a. As of August 7, 2019:
<https://www.scmp.com/news/china/diplomacy-defence/article/2131643/least-12-crew-members-killed-chinese-military-plane>

———, “The Tiananmen Crackdown Ignited a Decade of Debate on the Chinese Military’s Role, and Where Its Loyalties Should Lie,” *South China Morning Post*, December 7, 2018b. As of August 7, 2019:
<https://www.scmp.com/news/china/military/article/2176754/party-and-gun-where-should-loyalties-chinas-military-lie>

———, “Chinese Protesters Blame Fracking for Earthquakes that Killed Two People in Sichuan,” *South China Morning Post*, February 26, 2019a. As of August 7, 2019:
<https://www.scmp.com/news/china/society/article/2187718/chinese-demonstrators-urge-sichuan-government-and-blame-fracking>

———, “How a Mid-Air Collision Near Hainan 18 Years Ago Spurred China’s Military Modernization,” *South China Morning Post*, April 2, 2019b. As of August 7, 2019:

<https://www.scmp.com/news/china/diplomacy/article/3004383/how-mid-air-collision-near-hainan-18-years-ago-spurred-chinas>

Chang, Gordon, “Now China Wants Okinawa, Site of U.S. Bases in Japan,” *Daily Beast*, June 26, 2017.

Chanlett-Avery, Emma, and Ian Rinehart, *The U.S. Military Presence in Okinawa and the Futenma Base Controversy*, Washington, D.C.: Congressional Research Service, 2016.

Chase, Michael, “Army Day Coverage Stresses PLA’s Contributions and Party Control,” *China Brief*, Vol. 12, No. 16, August 17, 2012.

Chase, Michael S., Jeffrey Engstrom, Tai Ming Cheung, Kristen Gunness, Scott W. Harold, Susan Puska, and Samuel K. Berkowitz, *China’s Incomplete Military Transformation: Assessing the Weaknesses of the Chinese People’s Liberation Army (PLA)*, Santa Monica, Calif.: RAND Corporation, RR-893-USCC, 2015. As of May 19, 2020:

https://www.rand.org/pubs/research_reports/RR893.html

Chen Hanghui [陈航辉], Fang Peng [芳鹏], Yang Lei [杨磊] and Xia Yuren [夏育仁], “Social Media Warfare: A New Dimension to Warfare in the Information Age [社交媒体战: 信息时代战争新维度],” *PLA Daily* [解放军报], September 25, 2015. As of August 14, 2019:

http://www.81.cn/jfjbmap/content/2015-09/25/content_124476.htm

Chen Jie [陈捷], “Create a Shock Team for Military External Propaganda [打造军事外宣队伍的突击队],” *Military Correspondent* [军事记者], June 2015, pp. 53–54. As of August 7, 2019:

http://www.81.cn/big5/jsjz/2015-07/09/content_6579249.htm

Chen, Laurie, “China Troll Army’s Battle Expeditions Leap Great Firewall to Target Hong Kong Anti-Government Protests,” *South China Morning Post*, August 8, 2019. As of August 12, 2019:

<https://www.scmp.com/news/china/society/article/3021798/china-troll-armys-battle-expeditions-leap-great-firewall>

Chen Qingbao [陈庆宝], “Analysis and Countermeasure Research on the US ‘Online Astroturf Army’ [对美国 ‘网络水军’ 的分析及对策研究],” *Military Correspondent* [军事记者], November 2016. As of August 7, 2019:

http://www.81.cn/jsjz/2016-12/01/content_7387432.htm

Chen Wei-han, “MND Plays Down China Aircraft Threat,” *Liberty Times*, December 19, 2016. As of August 7, 2019:

<https://news.ltn.com.tw/news/focus/breakingnews/1921370>

Chen Zhengzhong [陈正中], "Preliminary Thoughts About Strengthening Cyber News Media in Wartime [加强战时网络新闻舆论管控刍议]," *Military Correspondent* [军事记者], July 2014. As of August 7, 2019: http://www.81.cn/jmywyl/2014-08/09/content_6086231.htm

Cheng, Dean, "Chinese Lessons from the Gulf Wars," in Andrew Scobell, David Lai, and Roy Kamphausen, eds., *Chinese Lessons from Other Peoples' Wars*, Carlisle, Pa.: U.S. Army War College Strategic Studies Institute, 2011, pp. 153–200.

Chi Yannian [迟延年], "Cyber Subversion: Security Threats That Must Not Be Taken Lightly [网络颠覆: 不容小觑的安全威胁]," *China Defense News*, August 6, 2009, p. 3.

Chief Information Officer, "Web and Social Media Policies," webpage, undated. As of August 7, 2019: <https://dodcio.defense.gov/DoD-Web-Policy/>

Chin, Josh, "Cyber Sleuths Track Hacker to China's Military," *Wall Street Journal*, September 23, 2015.

China Daily, Facebook account, undated. As of August 7, 2019: <https://www.facebook.com/chinadaily/>

China National Knowledge Infrastructure database, (in Chinese), undated. As of June 10, 2020: <https://new.oversea.cnki.net/index/>

China State Council Information Office, "And Some Photos Brought by PLA Air Force," Twitter post, July 15, 2016. As of June 15, 2019: <https://twitter.com/chinascio/status/753965508274233345>

China Xinhua News, @XHNews, Twitter account, undated. As of August 7, 2019: <https://twitter.com/XHNews>

"China's @PLA Navy Official Account Opens [中国@人民海军 官方微博正式开通]," Sina.com, April 15, 2019. As of July 5, 2019: https://k.sina.com.cn/article_6623517196_18acada0c00100lbak.html

"Chinese Flood Taiwan President-Elect's Facebook, Demanding Return to China," Reuters, January 21, 2016.

"Chinese 'Invasion' Triggers Property Surge in Manila," *Business Mirror*, May 5, 2018.

"Chinese Rocket Tragic Accident" video, YouTube, aired on Discovery Channel, uploaded by ChenchyFlaky, September 6, 2006. As of August 7, 2019: https://www.youtube.com/watch?v=8_EnrVf9u8s

"Chinese Student Charged for Throwing Soybean Pudding at Filipino Officer," BBC, February 14, 2019.

Choi Chi-yuk, "Fatal Crash of Chinese J-15 Carrier Jet Puts Question Mark over Troubled Programme," *South China Morning Post*, July 27, 2016. As of August 7, 2019:

<https://www.scmp.com/news/china/diplomacy-defence/article/1995729/fatal-crash-chinese-j-15-carrier-jet-puts-question-mark>

Chong, Alan, and David Han, "Foreign Policy Lessons from the Terrex Episode," *RSIS Commentary*, No. 22, February 2, 2017.

Chung, Lawrence, "Taiwan's Bid to Tackle 'Fake News' Raises Fears over Freedom of Speech," *South China Morning Post*, October 1, 2018. As of August 7, 2019:

<https://www.scmp.com/news/china/politics/article/2166262/taiwans-bid-tackle-fake-news-raises-fears-over-freedom-speech>

———, "Taiwan 'at the Front Line of Threats' from Beijing, Tsai Ing-wen Tells US Think Tanks," *South China Morning Post*, April 9, 2019a. As of September 17, 2019:

<https://www.scmp.com/news/china/diplomacy/article/3005453/taiwan-frontline-threats-beijing-tsai-ing-wen-tells-us-think>

———, "Taiwan Gets Tough over Fake News Blamed on Beijing 'Disrupting Its Democracy,'" *South China Morning Post*, July 27, 2019b. As of September 17, 2019:

<https://www.scmp.com/news/china/politics/article/3020261/taiwan-gets-tough-over-fake-news-blamed-beijing-disrupting-its>

Chung Li-hua and Jake Chung, "China Using Local 'Agents' to Spread Misinformation Online: Institute," *Taipei Times*, August 4, 2019. As of August 12, 2019:

<http://www.taipeitimes.com/News/front/archives/2019/08/04/2003719873>

Chung Li-hua and William Hetherington, "China Targets Polls with Fake Accounts," *Taipei Times*, November 5, 2018. As of August 7, 2019:

<http://www.taipeitimes.com/News/front/archives/2018/11/05/2003703618>

Cigarral, Ian Nicolas, "More Than 3 Million Chinese Allowed Entry into Philippines Since 2016—Immigration Data," *Philstar*, June 9, 2018.

Cliff, Roger, *China's Military Power: Assessing Current and Future Capabilities*, New York: Cambridge University Press, 2015.

Clover, Charles, "Xi Takes Aim at Military in Anti-Graft Drive," *Financial Times*, February 11, 2018. As of August 7, 2019:

<https://www.ft.com/content/3dba1f32-0c2a-11e8-8eb7-42f857ea9f09>

Cohen, Raphael S., Nathan Beauchamp-Mustafaga, Joe Cheravitch, Alyssa Demus, Scott W. Harold, Jeffrey W. Hornung, Jenny Jun, Michael Schwillie, Elina Treyger, and Nathan Vest, *Combating Foreign Disinformation on Social Media: Study Overview and Conclusions*, Santa Monica, Calif.: RAND Corporation, RR-4373/1-AF, 2021. As of July 2021:

https://www.rand.org/pubs/research_reports/RR4373z1.html

Cohen, Raphael S., Alyssa Demus, Michael Schwille, and Nathan Vest, *U.S. Efforts to Combat Foreign Disinformation on Social Media*, Santa Monica, Calif.: RAND Corporation, 2021, Not available to the general public.

Cole, J. Michael, “Fake News at Work: President Tsai ‘Persecutes Religion in Taiwan,’” *Taiwan Sentinel*, July 20, 2017. As of August 7, 2019: <https://sentinel.tw/fake-news-tsai-persecutes-religion/>

———, “That’s What ‘Fake News’ Looks Like and What It Does to Democracy,” *Taiwan Sentinel*, November 12, 2018. As of August 7, 2019: <https://sentinel.tw/fake-news-kaohsiung-democracy>

Cole, J. Michael, and Shelley Shan, “PRC Steps Up Psychological Warfare Targeted at Taiwan,” *Taipei Times*, August 26, 2011. As of August 7, 2019: <http://www.taipeitimes.com/News/front/archives/2011/08/26/2003511686/1>

Confessore, Nicholas, Gabriel J. X. Dance, Richard Harris, and Mark Hansen, “The Follower Factory,” *New York Times*, January 27, 2018. As of August 7, 2019: <https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html>

Constitution of the Republic of Singapore, Article 152, August 9, 1965.

Cooper, Sam, and Doug Quan, “How a Murky Company with Ties to the People’s Liberation Army Set Up Shop in B.C.,” *Vancouver Sun*, August 26, 2017. As of December 20, 2019: <https://vancouversun.com/news/local-news/how-a-murky-company-with-ties-to-the-peoples-liberation-army-set-up-shop-in-b-c>

Costello, John, and Joe McReynolds, *China’s Strategic Support Force: A Force for a New Era*, Washington, D.C.: National Defense University Press, 2018.

CPEC Official, @CPEC_Official, Twitter account, undated. As of August 7, 2019: https://twitter.com/cpec_official

Crispin, Shawn W., “Rappler-CIA Plot Claim Is Attempt to Cut Funding, Philippine Journalists Say,” Committee to Protect Journalists, May 21, 2019.

Cui Tiankai, @AmbCuiTiankai, Twitter account, undated. As of August 7, 2019: <https://twitter.com/AmbCuiTiankai>

Daiss, Tim, “Anti-U.S. Sentiment in Japan Grows amid Former Marine’s Alleged Murder,” *Forbes*, July 4, 2016.

Dancel, Raul, “Chinese Student in Pudding-Throwing Tantrum ‘Really, Really Sorry’, but Still Faces Deportation from Philippines,” *Straits Times*, February 12, 2019.

DeAeth, Duncan, “Taiwan Military Holds First-Ever Simulated ‘Anti-Fake News’ Exercises,” *Taiwan News*, April 22, 2019. As of August 7, 2019: <https://www.taiwannews.com.tw/en/news/3685796>

Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win*, Washington, D.C., 2019.

Demick, Barbara, “The *Times*, Bloomberg News, and the Richest Man in China,” *New Yorker*, May 5, 2015. As of August 7, 2019:
<https://www.newyorker.com/news/news-desk/how-not-to-get-kicked-out-of-china>

Denyer, Simon, “Taiwan Battles a Brain Drain as China Strives to Woo Talent,” *Washington Post*, April 15, 2018.

Department of Statistics (Singapore,) *Population Trends 2018*, Ministry of Trade and Industry, September 2018. As of June 12, 2019:
<https://www.singstat.gov.sg/-/media/files/publications/population/population2018.pdf>

Diamond, Larry, and Orville Schell, eds., *Chinese Influence and American Interests: Promoting Constructive Vigilance*, Stanford, Calif.: Hoover Institution, 2018.

“Diokno: PH Not in Risk over China Loans, CNN Philippines, November 19, 2018.

“Directives from the Ministry of Truth,” *China Digital Times*, undated. As of August 8, 2019:
<https://chinadigitaltimes.net/china/directives-from-the-ministry-of-truth/>

Do, Anh-Minh, “Zalo: Vietnam’s Flagship Mobile Messaging App Has Arrived,” *TechInAsia*, February 4, 2013. As of August 7, 2019:
<https://www.techinasia.com/zalo-vietnams-flagship-mobile-messaging-app-arrived>

Dobbins, James, Andrew Scobell, Edmund J. Burke, David C. Gompert, Derek Grossman, Eric Heginbotham, and Howard Shatz, *Conflict with China Revisited: Prospects, Consequences, and Strategies for Deterrence*, Santa Monica, Calif.: RAND Corporation, PE-248-A, 2017. As of May 5, 2020:
<https://www.rand.org/pubs/perspectives/PE248.html>

“Document 9: A ChinaFile Translation,” *ChinaFile*, November 8, 2013. As of August 7, 2019:
<http://www.chinafile.com/document-9-chinafile-translation>

DoD—See U.S. Department of Defense.

Doig, Will, “The Belt and Road Initiative Is a Corruption Bonanza,” *Foreign Policy*, January 15, 2019. As of December 20, 2019:
<https://foreignpolicy.com/2019/01/15/the-belt-and-road-initiative-is-a-corruption-bonanza/>

Dong Tao [董涛], “Advancing International Communications for Military News [Toward] Differentiated Audiences [推进军事新闻分众化的国际传播],” *Military Correspondent* [军事记者], September 2018. As of August 7, 2019:
http://www.81.cn/jsjz/2018-09/26/content_9299086.htm

Dotson, John, “Chinese Covert Social Media Propaganda and Disinformation Related to Hong Kong,” webpage, Jamestown Foundation, September 6, 2019. As of September 17, 2019:

<https://jamestown.org/program/chinese-covert-social-media-propaganda-and-disinformation-related-to-hong-kong/>

Drun, Jessica, “Taiwan’s Social Media Landscape: Ripe for Election Interference?” Center for Advanced China Research, blog post, November 13, 2018. As of August 7, 2019:

<https://www.ccpwatch.org/single-post/2018/11/13/Taiwans-Social-Media-Landscape-Ripe-for-Election-Interference>

Economy, Elizabeth C., *The Third Revolution: Xi Jinping and the New Chinese State*, New York: Oxford University Press, 2018.

Elemia, Camille, “‘False, Garbage.’ Maria Ressa, Ellen Tordesillas, PCIJ on Duterte ‘Ouster Plot,’” Rappler, April 22, 2019.

Ellis, Gavin, “China Could Be Using Taiwan as a Testing Ground for Disinformation Campaigns,” *New Zealand Listener*, February 16, 2019. As of September 17, 2019:

<https://www.noted.co.nz/currently/currently-world/china-taiwan-disinformation-testing-ground>

Engstrom, Jeffrey, *System Confrontation and System Destruction Warfare: How the Chinese People’s Liberation Army Seeks to Wage Modern Warfare*, Santa Monica, Calif.: RAND Corporation, RR-1708-OSD, 2018. As of May 5, 2020:

https://www.rand.org/pubs/research_reports/RR1708.html

Erickson, Andrew S., “The China Maritime Militia Bookshelf: Complete with Latest Recommendations & Fact Sheet,” webpage, May 21, 2019. As of December 17, 2019:

<http://www.andrewerickson.com/2019/05/the-china-maritime-militia-bookshelf-complete-with-latest-recommendations-fact-sheet-4/>

Everington, Keoni, “Honduras Denies Rumors of Talks with Beijing on Cutting Ties with Taiwan,” *Taiwan News*, May 28, 2018a. As of August 7, 2019:

<https://www.taiwannews.com.tw/en/news/3441950>

———, “China’s ‘Troll Factory’ Targeting Taiwan with Disinformation Prior to Election,” *Taiwan News*, November 5, 2018b. As of August 7, 2019:

<https://www.taiwannews.com.tw/en/news/3568146>

———, “Chinese Cybergroup Behind Kaohsiung Mayor’s Win Uncovered,” *Taiwan News*, June 27, 2019a. As of August 7, 2019:

<https://www.taiwannews.com.tw/en/news/3733335>

———, “Taiwan’s Foxconn Tycoon Calls Want Want Boss China’s ‘Hatchet Man and Lackey,’” *Taiwan News*, June 27, 2019b.

———, “Slow Yang Charged with Spurring Suicide of Taiwanese Diplomat in Japan with Fake News,” *Taiwan News*, December 2, 2019c. As of June 1, 2020: <https://www.taiwannews.com.tw/en/news/3828724>

Ezaki, Michio, “Kick out US Bases from Okinawa and Jeju, and China Will Build Their Own,” *Japan Forward*, June 13, 2017.

“Faces of Singapore,” VisitSingapore.com, undated. As of May 14, 2020: <https://www.visitsingapore.com/travel-guide-tips/about-singapore/people-of-singapore/>

“Factbox: Duterte Distances Philippines from Ally U.S.,” Reuters, October 21, 2016. As of August 9, 2019: <https://www.reuters.com/article/us-philippines-duterte-usa-factbox/factbox-duterte-distances-philippines-from-ally-u-s-idUSKCN12L1DB>

Felding, Nick, and Ian Cobain, “Revealed: US Spy Operation That Manipulates Social Media,” *The Guardian*, March 17, 2011. As of August 7, 2019: <https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks>

Feng, Emily, “China and the World: How Beijing Spreads the Message,” *Financial Times*, July 12, 2018. As of August 7, 2019: <https://www.ft.com/content/f5d00a86-3296-11e8-b5bf-23cb17fd1498>

Fonbuena, Carmela, “Duterte Gov’t Rejects U.S. Plans to Construct in Palawan Air Base,” Rappler, March 6, 2017.

“Foreign Ministry Spokesperson Geng Shuang’s Regular Press Conference,” Ministry of Foreign Affairs (China), November 28, 2016.

Forsythe, Michael, “Zhou Yongkang, Ex-Security Chief in China, Gets Life Sentence for Graft,” *New York Times*, June 11, 2015. As of August 7, 2019: <https://www.nytimes.com/2015/06/12/world/asia/zhou-yongkang-former-security-chief-in-china-gets-life-sentence-for-corruption.html>

Fravel, M. Taylor, “China’s New Military Strategy: ‘Winning Informationized Local Wars,’” *China Brief*, Vol. 15, No. 13, July 2, 2015.

———, *Active Defense: China’s Military Strategy Since 1949*, Princeton, N.J.: Princeton University Press, 2019.

Funke, Daniel, “These Fact-Checkers Were Attacked Online After Partnering with Facebook,” Poynter, September 10, 2018.

Funke, Daniel, and Daniela Flamini, “A Guide to Anti-Misinformation Actions Around the World,” Poynter, August 2019. As of September 17, 2019: <https://www.poynter.org/ifcn/anti-misinformation-actions/>

Galbraith, Andrew, "Twitter Apologizes for Blocked China Accounts Ahead of Tiananmen Anniversary," Reuters, June 2, 2019. As of August 7, 2019: <https://www.reuters.com/article/us-china-twitter/twitter-apologizes-for-blocked-china-accounts-ahead-of-tiananmen-anniversary-idUSKCN1T30C7>

Gallagher, Mary and Blake Miller, "Can the Chinese Government Really Control the Internet? We Found Cracks in the Great Firewall," *Washington Post*, February 21, 2017. As of August 7, 2019: https://www.washingtonpost.com/news/monkey-cage/wp/2017/02/21/can-the-chinese-government-really-control-the-internet-we-found-cracks-in-the-great-firewall/?noredirect=on&utm_term=.44add65e2ce6

Garnaut, John, "Rotting from Within," *Foreign Policy*, April 16, 2012. As of August 7, 2019: <https://foreignpolicy.com/2012/04/16/rotting-from-within/>

Ge, Celina, "PLA on Call: China's Military Orders Anti-Spy Software for Soldiers' Smartphones," *South China Morning Post*, April 19, 2016. As of December 20, 2019: <https://www.scmp.com/news/china/diplomacy-defence/article/1937085/pla-call-chinas-military-orders-anti-spy-software>

"German Spy Agency Warns of Chinese LinkedIn Espionage," BBC, December 10, 2017. As of August 7, 2019: <https://www.bbc.com/news/world-europe-42304297>

Gibbons-Neff, Thomas, "How a Four-Hour Battle Between Russian Mercenaries and U.S. Commandos Unfolded in Syria," *New York Times*, May 24, 2018.

Gita, Ruth Abbey, "Duterte 'Nothing to Do' with Banned Facebook Account," Sunstar, April 1, 2019. As of August 9, 2019: <https://www.sunstar.com.ph/article/1799534>

Gleicher, Nathaniel, "Removing Coordinated Inauthentic Behavior from China," Facebook Newsroom, August 19, 2019. As of September 17, 2019: <https://newsroom.fb.com/news/2019/08/removing-cib-china/>

Gomez, Jim, "Philippines Suspends Abrogation of Defense Pact with US," Associated Press via *Washington Post*, June 2, 2020. As of June 3, 2020: https://www.washingtonpost.com/world/national-security/philippines-suspends-abrogation-of-defense-pact-with-us/2020/06/02/a2dade5c-a533-11ea-898e-b21b9a83f792_story.html

Government of Japan, *National Defense Program Guidelines for FY 2019 and Beyond*, Ministry of Defense (Japan), December 18, 2018. As of August 9, 2019: https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/20181218_e.pdf

Government of Singapore, *Factually*, website, undated. As of July 9, 2019: <https://www.gov.sg/factually>

“Governor Tamaki, ‘An Important Opportunity to Directly Reflect the Prefectural Public’s Will,’ Okinawa Prefecture Announces February 24 for Holding Prefectural Referendum [“沖縄県が県民投票2月24日実施を発表 玉城知事「県民の意思を直接反映させる重要な機会」”], *Ryūkyū Shimpō*, November 27, 2018. As of August 9, 2019:

<https://ryukyushimpo.jp/news/entry-840311.html>

Grossman, Derek, Nathan Beauchamp-Mustafaga, Logan Ma, and Michael Chase, *China’s Long-Range Bomber Flights: Drivers and Implications*, Santa Monica, Calif.: RAND Corporation, RR-2567-AF, November 2018. As of August 7, 2019:

https://www.rand.org/pubs/research_reports/RR2567.html

Grundy, Tom, “Did China’s State-Run News Agency Purchase Twitter Followers?” *Hong Kong Free Press*, April 14, 2015. As of August 7, 2019:

<https://www.hongkongfp.com/2015/04/14/did-chinas-state-run-news-agency-purchase-twitter-followers/>

Han, Jamie, “Communal Riots of 1964,” Singapore Infopedia, undated.

Han, Kirsten, “Why Singapore’s Moves to Curb ‘Fake News’ May Backfire,” *Washington Post*, March 5, 2018. As of July 9, 2019:

https://www.washingtonpost.com/news/global-opinions/wp/2018/03/05/why-singapores-moves-to-curb-fake-news-may-backfire/?utm_term=.bafb92434223

Harold, Scott W., *Defeat, Not Merely Compete: China’s View of Its Military Aerospace Goals and Requirements in Relation to the United States*, Santa Monica, Calif.: RAND Corporation, RR-2588-AF, 2018. As of May 5, 2020:

https://www.rand.org/pubs/research_reports/RR2588.html

He Dan, “Trust among Chinese ‘Drops to Record Low,’” *China Daily*, February 18, 2013. As of August 7, 2019:

http://www.chinadaily.com.cn/china/2013-02/18/content_16230755.htm

Head, Jonathan, “Outlaw or Ignore? How Asia Is Fighting ‘Fake News,’” BBC, April 4, 2018.

Heath, Timothy, “Beijing’s Influence Operations Target Chinese Diaspora,” *War on the Rocks*, March 1, 2018. As of August 7, 2019:

<https://warontherocks.com/2018/03/beijings-influence-operations-target-chinese-diaspora/>

Heginbotham, Eric, Michael Nixon, Forrest E. Morgan, Jacob L. Heim, Jeff Hagen, Sheng Tao Li, Jeffrey Engstrom, Martin C. Libicki, Paul DeLuca, David A. Shlapak, David R. Frelinger, Burgess Laird, Kyle Brady, and Lyle J. Morris, *The U.S.–China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017*, Santa Monica, Calif.: RAND Corporation, RR-392-AF, 2015. As of May 5, 2020:

https://www.rand.org/pubs/research_reports/RR392.html

Heydarian, Richard Javad, "China's Economic Cabbage Strategy," Asia Maritime Transparency Initiative, March 11, 2019.

Hille, Kathrin, "China's 'Sharp Power' Play in Taiwan," *Financial Times*, November 21, 2018. As of August 7, 2019:
<https://www.ft.com/content/5c272b90-ec12-11e8-89c8-d36339d835c0>

———, "Taiwan Primaries Highlight Fears over China's Political Influence," *Financial Times*, July 16, 2019. As of August 7, 2019:
<https://www.ft.com/content/036b609a-a768-11e9-984c-fac8325aaa04>

Hoffman, Samantha, *Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion*, Sydney, Australia: Australian Strategic Policy Institute, 2019. As of December 19, 2019:
<https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion>

Hootsuite, "Digital 2019 United States of America (January 2019)," webpage, January 31, 2019a. As of August 7, 2019:
<https://www.slideshare.net/DataReportal/digital-2019-united-states-of-america-january-2019-v02>

———, "Digital 2019 Japan (January 2019)," webpage, February 3, 2019b. As of August 7, 2019:
<https://www.slideshare.net/DataReportal/digital-2019-south-korea-january-2019-v01>

———, "Digital 2019 Philippines (January 2019)," webpage, February 3, 2019c. As of August 7, 2019:
<https://www.slideshare.net/DataReportal/digital-2019-south-korea-january-2019-v01>

———, "Digital 2019 South Korea (January 2019)," webpage, February 3, 2019d. As of August 7, 2019:
<https://www.slideshare.net/DataReportal/digital-2019-south-korea-january-2019-v01>

———, "Digital 2019 Taiwan (January 2019)," webpage, February 3, 2019e. As of August 7, 2019:
<https://www.slideshare.net/DataReportal/digital-2019-taiwan-january-2019-v01>

———, "Digital 2019 Vietnam (January 2019)," webpage, February 3, 2019f. As of August 7, 2019:
<https://www.slideshare.net/DataReportal/digital-2019-vietnam-january-2019-v01>

Hornung, Jeffrey W., "Japan's 2015 Security Legislation: Changed Rooted Firmly in Continuity," in Mary McCarthy, ed., *Routledge Handbook of Japanese Foreign Policy*, New York: Routledge, 2018, pp. 22–40.

- Horton, Chris, "Specter of Meddling by Beijing Looms over Taiwan's Elections," *New York Times*, November 22, 2018. As of August 7, 2019:
<https://www.nytimes.com/2018/11/22/world/asia/taiwan-elections-meddling.html>
- , "Candidate Seeks Closer China Ties, Shaking Up Taiwan's Presidential Race," *New York Times*, June 6, 2019. As of August 7, 2019:
<https://www.nytimes.com/2019/06/06/world/asia/taiwan-han-president.html>
- Hsiao, Russell, "CCP Propaganda Against Taiwan Enters the Social Age," *China Brief*, Vol. 18, No. 7, April 24, 2018a.
- , "China's Intensifying Pressure Campaign Against Taiwan," *China Brief*, Vol. 18, No. 11, June 19, 2018b.
- , "A Preliminary Survey of CCP Influence Operations in Japan," *China Brief*, Vol. 19, No. 12, June 26, 2019a.
- , "A Preliminary Survey of CCP Influence Operations in Singapore," *China Brief*, Vol. 19, No. 13, July 16, 2019b.
- Hsieh Chun-lin, Lu Yi-hsuan, and Jake Chung, "Control Yuan Members Blast Su Report," *Taipei Times*, May 24, 2019. As of September 17, 2019:
<http://www.taipeitimes.com/News/taiwan/archives/2019/05/24/2003715713/1>
- Hsu, Stacy, "Taiwan Asserts Sovereignty over Diaoyutai," *Taipei Times*, July 19, 2018. As of August 7, 2019:
<http://www.taipeitimes.com/News/taiwan/archives/2018/07/19/2003696948>
- , "Protestors Gather in Taipei, Asking 'Red Media' to Leave Taiwan," *FocusTaiwan*, June 23, 2019. As of August 7, 2019:
<http://focustaiwan.tw/news/acs/201906230011.aspx>
- Hu Xiao [胡晓], "Research on the Influence of Network Propaganda on the Observing Behavior of Young Audiences [网络宣传对青年受众观影行为的影响研究]," *Radio & TV Journal* [视听], July 2016.
- Hu Zhaomin, @SpokespersonHZM, Twitter account, undated. As of June 1, 2020:
<https://twitter.com/SpokespersonHZM>
- Huang Jaw-Nian, "The China Factor in Taiwan's Media," *China Perspectives*, March 2017, pp. 27–36. As of July 29, 2019:
<http://journals.openedition.org/chinaperspectives/7388>
- "Huang Jing, Chinese-American Academic Expelled by Singapore, Is Working in Beijing and Has 'No Hard Feelings,'" *Today*, June 18, 2019.
- Huang Jingjing, "A More Loyal PLA Rebuffs the Heresy of Separating the Party and Military," *Global Times*, June 9, 2017. As of March 9, 2019:
<http://www.globaltimes.cn/content/1052432.shtml>

Huang, Marco, “Chinese Netizens Flood Tsai Ing-Wen’s Facebook Page with Anti-Taiwan Independence Posts,” *Wall Street Journal*, January 21, 2016. As of August 7, 2019:

<https://blogs.wsj.com/chinarealtime/2016/01/21/chinese-netizens-flood-tsai-ing-wens-facebook-page-with-anti-taiwan-independence-posts/>

Huang, Paul, “Chinese Cyber-Operatives Boosted Taiwan’s Insurgent Candidate,” *Foreign Policy*, June 26, 2019. As of August 7, 2019:

<https://foreignpolicy.com/2019/06/26/chinese-cyber-operatives-boosted-taiwans-insurgent-candidate/>

Huntley, Shane, “Maintaining the Integrity of Our Platforms,” Google, August 22, 2019. As of September 17, 2019:

<https://www.blog.google/outreach-initiatives/public-policy/maintaining-integrity-our-platforms/>

“Information of 10,000 U.S. Troops Leaks: Military Network Security Attracts Attention [美国十万军人信息外流 军事网络安全引人关注],” Sohu, July 13, 2006. As of August 7, 2019:

<http://news.sohu.com/20060713/n244239488.shtml>

Insikt Group, *Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion*, Boston, Mass.: Recorded Future, 2019.

Ito, Kazuyuki, “Okinawa Decides to Hold Feb. 24 Referendum on U.S. Base Issue,” *Asahi Shimbun*, November 27, 2018.

“Japan Officially Gave U.S. Consent to Bring in Nuclear Weapons ahead of Okinawa Reversion Accord: Document,” *Japan Times*, August 14, 2017. As of August 7, 2019:

https://www.japantimes.co.jp/news/2017/08/14/national/history/japan-officially-gave-u-s-consent-bring-nukes-ahead-okinawa-reversion-accord-document/#.XScM28RS_IU

“Japanese PM Yukio Hatoyama Resigns amid Okinawa Row,” BBC, June 2, 2010. As of August 9, 2019:

<https://www.bbc.com/news/10211314>

Jennings, Ralph, “In Taiwan, Proposed Sale of Media Group Prompts Concern,” *Los Angeles Times*, November 29, 2012.

———, “Facebook Says It Already Has 97% of Taiwan’s Internet Users, and Now It’s Targeting Businesses,” *Forbes*, October 11, 2018.

———, “In the Name of ‘Fake News,’ Asian Governments Tighten Control on Social Media,” *Los Angeles Times*, February 8, 2019a. As of September 17, 2019: <https://www.latimes.com/world/asia/la-fg-asia-fake-news-20190130-story.html>

———, “Taiwan Seeks to Rein In Freewheeling Media with Tougher Anti-Fake News Laws,” *Voice of America*, April 22, 2019b. As of September 17, 2019: <https://www.voanews.com/east-asia/taiwan-seeks-rein-freewheeling-media-tougher-anti-fake-news-laws>

Jiang Tingting [姜婷婷], “Thoughts on Transmitting International Public Opinion with Regard to Discussions of the South China Sea [关于南海议题国际舆论传播的思考],” *Military Correspondent* [军事记者], December 2017. As of August 7, 2019: http://www.81.cn/jsjz/2017-12/27/content_7886093.htm

Jin Sicong [金思聪], “Characteristics and Public Sentiment Guidance for International Social Media Relating to Chinese Military Agenda Setting: Framework Analysis of Twitter Reporting During the China-U.S. UUV Incident [国际社交媒体涉华军事议题的特点与舆情引导: 中美无人潜航器事件推特报道的框架分析],” *Military Correspondent* [军事记者], August 2018. As of August 7, 2019: http://www.81.cn/jsjz/2018-07/19/content_8093614.htm

Johnston, Eric, “More Than 70% in Okinawa Vote No to Relocation of U.S. Futenma Base to Henoko,” *Japan Times*, February 24, 2019.

Joshi, Ishan, “Fighting Fake News in Asia,” *Asia News Network*, August 28, 2019. As of September 17, 2019: <https://asianews.network/2019/08/28/fighting-fake-news-in-asia/>

Kaiman, Jonathan, “Free Tibet Exposes Fake Twitter Accounts by China Propagandists,” *The Guardian*, July 22, 2014. As of August 7, 2019: <https://www.theguardian.com/world/2014/jul/22/free-tibet-fake-twitter-accounts-china-propagandists>

Kamphausen, Roy, “The General Political Department,” in Kevin Pollpeter and Kenneth W. Allen, eds., *The PLA as Organization v2.0*, Dunn Loring, Va.: Defense Group Inc., 2015.

Kania, Elsa, “The PLA’s Latest Strategic Thinking on the Three Warfares,” *China Brief*, Vol. 16, No. 13, August 22, 2016.

———, “AlphaGo and Beyond: The Chinese Military Looks to Future ‘Intelligentized’ Warfare,” *Lawfare*, June 5, 2017. As of August 7, 2019: <https://www.lawfareblog.com/alpha-go-and-beyond-chinese-military-looks-future-intelligentized-warfare>

Kawashima, Shin, “The Origins of the Senkaku/Diaoyu Islands Issue,” *Asia-Pacific Review*, Vol. 20, No. 2, 2013, pp. 122–145.

Kimura, Maki, “The Anti-US Military Base Struggle in Okinawa, Japan,” *Open Democracy*, February 13, 2016.

King, Gary, Jennifer Pan, and Margaret E. Roberts, “How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument,” *American Political Science Review*, Vol. 111, No. 3, 2017, pp. 484–501.

Kingston, Jeff, “Understanding Anti-Base Sentiment in Okinawa,” *Japan Times*, May 28, 2016.

Kliman, Daniel, Andrea Kendall-Taylor, Kristine Lee, Joshua Fitt and Carisa Nietzsche, *Dangerous Synergies: Countering Chinese and Russian Digital Influence Operations*, Washington, D.C.: Center for a New American Security, May 7, 2020. As of May 27, 2020:
<https://www.cnas.org/publications/reports/dangerous-synergies>

Ko Tin-yau, “How Fake News Led to Suicide of Taiwan Representative in Osaka,” *EJInsight*, September 19, 2018. As of August 7, 2019:
<http://www.ejinsight.com/20180919-how-fake-news-led-to-suicide-of-taiwan-representative-in-osaka/>

Koh Gui Qing and John Shiffman, “Beijing’s Covert Radio Network Airs China-Friendly News Across Washington, and the World,” Reuters, November 2, 2015. As of August 7, 2019:
<https://www.reuters.com/investigates/special-report/china-radio/>

Kōno, Kei, “Okinawa and Nationwide Awareness Regarding U.S. Military Bases in Okinawa: April 2017 ‘Okinawa at 45 Years Since Reversion’ Poll [沖縄米軍基地をめぐる意識 沖縄と全国 ～2017年4月「復帰45年の沖縄」調査～], *NHK*, August 2017.

Koutsoukis, Jason and Cecilia Yap, “China Hasn’t Delivered on Its \$24 Billion Philippines Promise,” Bloomberg, July 25, 2018.

Kurlantzick, Joshua, “How Much Damage Can Duterte Do to the U.S.-Philippine Relationship?” *World Politics Review*, October 7, 2016.

Kyodo, “Japan Plans to Take Steps Against ‘Fake News’ by June,” *Japan Times*, January 14, 2019.

LaFoy, Scott, “I Watch a Lot of CCTV,” Twitter post, November 18, 2018. As of August 7, 2019:
<https://twitter.com/wslafoy/status/931883927882665984>

Lai Dongwei [赖东威], “An Analysis of the Sentence Patterns and the Use of Vocabulary in Taiwanese Social Media [台湾社交媒体中的闽南语句式和词汇使用现象探析],” *Journal of News Research [新闻研究导刊]*, 2017, pp. 268–270.

Lands, David R., “Publicly Available Information: The Secret to Unclassified Data, Part I,” *Over the Horizon*, April 8, 2019. As of August 7, 2019:
<https://othjournal.com/2019/04/08/publicly-available-information-the-secret-to-unclassified-data-part-i/>

Le Yuan [乐媛] and Zhou Xiaoqi [周晓琪], "Social Media Mobilization and Inter-media Agenda-Setting Effects of Social Movement: The Case Study of "Anti-trade Student Movement" in Taiwan [社会运动中的社交媒体动员与媒介议程设置效应:以台湾地区“反服贸学运”为例],” *Chinese Journal of Journalism & Communication* [国际新闻界], June 2019.

Lee, Yimou, "Taiwan President Says Chinese Drills a Threat but Not Intimidated," Reuters, April 15, 2019a.

———, "Taiwan Says China Has Stepped Up Infiltration Efforts," Reuters, May 9, 2019b. As of August 7, 2019:

<https://www.reuters.com/article/us-china-taiwan/taiwan-says-china-has-stepped-up-infiltration-efforts-idUSKCN1SG08F>

Lee, Yimou, and Fabian Hamacher, "Taiwan Passes Law to Combat Chinese Influence on Politics," Reuters, December 31, 2019. As of June 1, 2020:

<https://www.reuters.com/article/us-taiwan-lawmaking/taiwan-passes-law-to-combat-chinese-influence-on-politics-idUSKBN1YZ0F6>

Lee, Yimou, and I-hwa Cheng, "Paid 'News': China Using Taiwan Media to Win Hearts and Minds on Island—Sources," Reuters, August 9, 2019. As of August 12, 2019:

<https://www.reuters.com/article/us-taiwan-china-media-insight/paid-news-china-using-taiwan-media-to-win-hearts-and-minds-on-island-sources-idUSKCN1UZ0I4?il=0>

Lee, Yimou, and James Pomfret, "Taiwan Steps Up Probe into Surveillance by Pro-China Media on Island," *Channel News Asia*, January 18, 2019. As of August 7, 2019:

<https://www.channelnewsasia.com/news/world/taiwan-steps-up-probe-into-surveillance-by-pro-china-media-on-island-11139538>

Lema, Karen, Martin Petty, and Phil Stewart, "Duterte Terminates Philippines Troop Pact, U.S. Calls Move 'Unfortunate,'" Reuters, February 11, 2020. As of June 3, 2020:

<https://www.reuters.com/article/us-philippines-usa-defence/duterte-terminates-philippines-troop-pact-us-calls-move-unfortunate-idUSKBN2050E9>

Leung, Hillary, "Singapore Is the Latest Country to Propose Tough Legislation Against Fake News," *Time*, April 2, 2019. As of July 9, 2019:

<https://time.com/5562501/singapore-fake-news-law-freedom-speech/>

Li Bicheng [李弼程], Hu Huaping [胡华平], and Xiong Ya [熊尧], "Intelligent Agent Model for Online Public Opinion Guidance

[网络舆情引导智能代理模型], *National Defense Science & Technology* [国防科技], No. 3, June 2019, pp. 73–77.

Li Dayong [李大勇], Zhang Shengtao [张圣涛], and Xia Yun [夏云], "Focusing on Improving the Effectiveness of Propaganda for International Military Competition News: Reflection on Army Organized 'International Army Games-2018' Coverage [着力提升国际军事赛事新闻宣传效益: 陆军承办'国际军事比赛-2018'报道回眸]," *Military Correspondent* [军事记者], October 2018. As of August 7, 2019: http://www.81.cn/jsjz/2018-10/25/content_9322221.htm

Li Ruobing [李若冰], "China's Astroturf and Cyber Army Train Mind Superiority with 2020 Elections as Target [中國水軍、網軍九合一練兵「制腦權」, 目標2020大選]," Storm, November 23, 2018. As of August 7, 2019: <https://www.storm.mg/article/643412>

Li Shiyan [李仕燕] and Li Zhicong [李智聰], "An Analysis on Cognitive Differences Between Youth of the Chinese Mainland and Taiwan on Social Media—Take the Cancellation of Hosting Rights of Taichung for East Asian Youth Games As an Example [社交媒体中的两岸青年认知差异评析—以台中市“东亚青运”主办权被取消事件为例]," *Modern Taiwan Studies* [现代台湾研究], February 2019.

Li Yuanyuan [李媛媛], "Fight Against Attacks in the Online Ideology Battle [打好网络意识形态斗争进攻仗]," *Political Workers* [政工导刊], April 2017, pp. 15–16.

Liao Yiwen [廖毅文], "Measures for Guiding Public Opinion on the Internet When Major Surprise Incidents Occur [重大突发事件的互联网舆论引导对策]," *Military Correspondent* [军事记者], June 2011, pp. 20–21.

Lim, Louisa, and Lucy Craft, "Japan's Prime Minister Resigns over U.S. Base," NPR, June 2, 2010. As of August 9, 2019: <https://www.npr.org/templates/story/story.php?storyId=127356895>

Lin, I-fan, "Taiwan's Battle Against Swine Fever Gets Political on PTT," *The News Lens*, January 11, 2019.

Lin Zehong [林则宏], "Wu Pao-chun, Accused of Supporting Taiwan Independence: 'I Am a Chinese Person Who Supports the '1992 Consensus' [遭指台獨 吳寶春: 我是中國人、支持「九二共識」]," *United Daily News* [聯合報], December 10, 2018. As of August 7, 2019: <https://udn.com/news/story/7332/3529153>

Liu Huiyan [刘惠燕], Xiong Wu [熊武], Xu Xianliang [吴显亮], and Mei Shunliang [梅顺量], "Several Thoughts on Promoting the Construction of Cognitive Domain Operations Equipment in the Whole Environment [全媒体环境下推进认知域作战装备发展的几点思考]," *Defense Technology Review* [国防科技], October 2018.

Liu Juntao, "Overseas Chinese and Chinese Soft Power from the Economic Perspective: The Case of Indonesia," *Science-Economy-Society* [科学经济社会], No. 3, December 2012, pp. 35–41.

- Liu Weichao [刘伟超] and Zhou Jun [周军], "New Ideas to Improve Our Army's Network Public Opinion Capability [新理念提升我军网络舆论引导能力]," *New Media* [网络传播], July 2018, pp. 88–90.
- , "The Analysis of Facebook Users' Information Behavior in Taiwan: Through the Two Angles of the User and the Media [台湾地区脸书(Facebook)用户信息行为研究——基于用户和媒介的双重视角]," *Taiwan Studies* [台湾研究], March 2019.
- Liu Xiao [刘肖], "International Communication: Analysis of the Path of Evaluation Indicator Construction and Communication Effectiveness Improvement [国际传播力: 评估指标构建与传播效力提升路径分析]," *Jianghuai Tribune* [江淮论坛], April 2017.
- Liu Xiaodong [刘晓东] and Fan Jingyu [樊净芷], "Be Careful with Posts, Be Wary of Online 'Fishing' [跟帖须谨慎, 警惕网络"钓鱼]," *PLA Daily* [解放军报], November 22, 2015. As of August 7, 2019: http://www.81.cn/jfjbmap/content/2015-11/22/content_129980.htm
- Liu Yi [刘轶], "Do Agenda Setting Well, Seize International Communication Right to Speak [搞好议题设置, 争取国际传播话语权]," *Military Correspondent* [军事记者], September 2018. As of August 7, 2019: http://www.81.cn/jsjz/2018-09/26/content_9299085.htm
- Loo, Bernard F. W., "Making Sense of the Terrex Incident," *Today*, December 6, 2016.
- Lou Sijia [娄思佳], "On Military Broadcasting to Taiwan: Strategies for Leveraging Non-Native Social Media [论对台军事广播: 借力非本土社交媒体的策略]," *China Broadcasts* [中国广播], August 2017, pp. 29–32.
- Luo Ji [罗辑], "Using Instant Messaging Tools to Build a Full Media Editing Platform [运用即时通信工具构建全媒体编务平台初探]," *Military Correspondent* [军事记者], October 2014, pp. 17–18.
- Ma Chao [马超] and Sun Hao [孙皓], "The Characteristics of Russian Public Opinion Propagation: Taking 'Russia Today' TV Station as an Example [俄罗斯对外舆论传播的特点: 以'今日俄罗斯'电视台为例]," *Military Correspondent* [军事记者], June 2018. As of August 7, 2019: http://www.81.cn/jsjz/2018-06/14/content_8061994.htm
- Magnier, Mark, "A Crisis of Trust Takes a Toll on Chinese Society," *Los Angeles Times*, September 24, 2006.
- "Mainland Restrictions to Be Lifted on Line and KakaoTalk, South Korean Diplomat Says," *South China Morning Post*, June 13, 2019. As of August 7, 2019: <https://www.scmp.com/article/1566125/mainland-restrictions-be-lifted-line-and-kakaotalk-south-korean-diplomat-says>
- Manantan, Mark, "Commentary: What the Huawei Espionage Controversy Means to the Philippines," *Philstar*, March 25, 2019.

Mandhana, Niharika, "In Global Tech Battle, a Balky U.S. Ally Chooses China," *Wall Street Journal*, July 15, 2019. As of August 7, 2019:

<https://www.wsj.com/articles/in-global-tech-battle-the-philippines-has-chosen-sides-not-the-u-s-11563205891>

Marchadesch, Barbara, "Duterte Blasts Carpio over South China Sea Stance," MSN, November 28, 2018.

Marquez, Consuelo, "DICT Signs MOU with Russian Firm to Boost Cybersecurity," *Inquirer.Net*, September 25, 2018.

Martinson, Ryan D., "The Courage to Fight and Win: The PLA Cultivates Xuexing for the Wars of the Future," *China Brief*, Vol. 16, No. 9, June 1, 2016.

Mattis, Peter, "China's 'Three Warfares' in Perspective," *War on the Rocks*, January 30, 2018. As of August 7, 2019:

<https://warontherocks.com/2018/01/chinas-three-warfares-perspective/>

Mazarr, Michael J., Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends*, Santa Monica, Calif.: RAND Corporation, RR-2713-OSD, 2019. As of May 5, 2020:

https://www.rand.org/pubs/research_reports/RR2713.html

McCombs, Maxwell E., and Donald L. Shaw, "The Agenda-Setting Function of Mass Media," *Public Opinion Quarterly*, Vol. 36, No. 2, Summer 1972, pp. 176–187.

McLaughlin, Timothy, "A U.S. Ally Is Turning to China to 'Build, Build, Build,'" *The Atlantic*, May 8, 2019.

McReynolds, Joe, ed., *China's Military Strategy*, Washington, D.C.: Brookings Institution Press, 2016.

Mendoza, Ronald U., and Miann S. Banaag, "Is the Philippines' Pro-China Policy Working?" *The Diplomat*, November 14, 2018.

Miao Jian [苗健], "With the Help of Overseas Open Internet Information Platform: Seeking Equal Right to Speak [借助海外开放式互联网信息平台: 谋求对等话语权]," *Southeastern Communication* [东南传播], August 2014, pp. 7–9.

Ministry of National Defense of the People's Republic of China, "China Air Force Weibo, WeChat Public Account Open

[中国空军官方微博、微信公众号开通运行]," November 10, 2015. As of August 7, 2019:

https://www.mod.gov.cn/edu/2015-11/10/content_4628124.htm

Mo Li [莫莉], "Democratic Deliberations Are Still Noisy Self-Talk: The Content of the DPP Candidate Facebook in the 2016 Taiwan Election and the Participation of Netizens [民主的商议还是喧嚣的自语:2016年台湾地区选举中民进党候选人脸谱网内容及网民参与研究]," *Journalism and Mass Communication Monthly* [新闻界], August 2017.

Mogato, Manuel, "Duterte Says He Wants U.S. Special Forces out of Southern Philippines," Reuters, September 12, 2016.

Monaco, Nicholas J., "Computational Propaganda in Taiwan: Where Digital Democracy Meets Automated Autocracy," Computational Propaganda Research Project, working paper, June 2017. As of August 7, 2019:
<http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Taiwan-2.pdf>

———, "Beijing's Computational Propaganda Goes Global: The Significance of China's Debut as a Disinformation Actor," Digital Intelligence Lab via Medium, September 12, 2019a. As of December 20, 2019:
<https://medium.com/digintel/beijings-computational-propaganda-goes-global-the-significance-of-china-s-debut-as-a-e220145dc90a>

———, "Welcome to the Party: A Data Analysis of Chinese Information Operations," Digital Intelligence Lab via Medium, September 18, 2019b. As of December 20, 2019:
<https://medium.com/digintel/welcome-to-the-party-a-data-analysis-of-chinese-information-operations-6d48ee186939>

Morales, Neil Jerome, "Philippine Regulator Revokes News Site's License over Ownership Rules, Media Outraged," Reuters, January 15, 2018.

Morales, Neil Jerome, and Karen Lema, "China Telecom, Local Tycoon Team up to Win Philippine Telco License," Reuters, November 6, 2018.

Mourdoukoutas, Panos, "Filipinos Are Beginning to See the Ugly Side of Chinese Investments," *Forbes*, March 21, 2019.

Mozur, Paul, "Live from America's Capital, a TV Station Run by China's Communist Party," *New York Times*, February 28, 2019a. As of August 7, 2019:
<https://www.nytimes.com/2019/02/28/business/cctv-china-usa-propaganda.html>

———, "Facing Legal Scrutiny, China's State TV Recalls Its U.S. Head," *New York Times*, March 8, 2019b. As of August 7, 2019:
<https://www.nytimes.com/2019/03/08/business/china-state-tv-us.html>

Musico, Jelly, "Lorenzana Orders Review of 67-Year-Old US-PH Military Pact," Philippine News Agency, December 28, 2018.

Nakashima, Ellen, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, February 27, 2019.

National Library Board (Singapore), “Fact-Checking Using Multiple Sources,” webpage, undated. As of July 9, 2019:
<https://sure.nlb.gov.sg/blog/seniors/sn0004>

“News That US Could Rent Itu Aba Is ‘Fake,’ Institute Says,” *Taipei Times*, July 1, 2018. As of August 7, 2019:
<http://www.taipeitimes.com/News/taiwan/archives/2018/07/01/2003695894>

Ng, Alfred, “US Officials in Contact with TikTok over Political Disinformation,” CNET.com, March 3, 2020. As of May 28, 2020:
<https://www.cnet.com/news/us-officials-in-contact-with-tiktok-over-political-disinformation/>

Ng, Kelly, “The Big Read: In an Era of Fake News, the Truth May Not Always Be out There,” *Today*, June 2, 2017.

Nip, Joyce Y.M., and Chao Sun, “China’s News Media Tweeting, Competing with US Sources,” *Westminster Papers in Communication and Culture*, Vol. 13, No. 1, 2018, pp. 98–122. As of August 7, 2019:
<http://doi.org/10.16997/wpcc.292>

“Okinawa Dailies Fact-Check, Debunk Rumors Spread During Gubernatorial Race,” *Mainichi*, October 1, 2018.

“Okinawa Gov.’s ‘China Connection’ Nothing but ‘Fake News,’ but Spreads via Internet,” *Mainichi*, June 18, 2017.

Okinawa Prefectural Government, *What Okinawa Wants You to Understand About the U.S. Military Bases*, Naha, Japan, March 2018.

Olesen, Alexa, “Where Did Chinese State Media Get All Those Facebook Followers?” *Foreign Policy*, July 7, 2015. As of August 7, 2019:
<http://foreignpolicy.com/2015/07/07/china-facebook-peoples-daily-media-soft-power/>

“Originator of Fake News: I Can’t Stand It That the Public Will Can Bend by Biased News
 [フェイクニュースの発信者「偏った情報で民意が歪められるの耐えられない」],” *Okinawa Times*, February 2, 2019.

Pan, Jason, “China Subverting Elections: Premier,” *Taipei Times*, November 2, 2018. As of August 7, 2019:
<http://www.taipeitimes.com/News/front/archives/2018/11/02/2003703459>

Parker, Emily, “Can WeChat Thrive in the United States?” *MIT Technology Review*, August 11, 2017. As of August 7, 2019:
<https://www.technologyreview.com/s/608578/can-wechat-thrive-in-the-united-states/>

Parliament (Singapore), Protection from Online Falsehoods and Manipulation, Bill Number 10/2019, April 1, 2019. As of July 9, 2019:
<https://www.parliament.gov.sg/docs/default-source/default-document-library/protection-from-online-falsehoods-and-manipulation-bill10-2019.pdf>

Peng Xingdou, “A Look at WeChat Management Through ‘the Boyfriend Who Shelled Chestnuts,’” *Huoqianbing Bao*, March 3, 2017, p. 3.

“*People’s Daily* Comments on Emperor’s Expedition on FB: Post-90s [Generation], We Believe in You! [人民日报评帝吧出征FB: 90后, 相信你们!],” Sina.com, January 22, 2016. As of August 7, 2019:
<http://tech.sina.com.cn/i/2016-01-22/doc-ifyxnuvxe8360645.shtml>

People’s Daily, “Video Reveals DF-41,” Twitter post, November 17, 2018. As of August 7, 2019:
<https://twitter.com/PDChina/status/931765898087604224>

People’s Liberation Army Academy of Military Science Military Strategy Department, *Science of Military Strategy* [战略学], 3rd ed., Beijing, China: Academy of Military Science Press, 2013.

People’s Liberation Army Air Force, “Air Force Release [空军发布],” Weibo post, undated. As of August 7, 2019:
<https://m.weibo.cn/p/1005055707057078>

Petty, Martin, “As Philippines’ Duterte Visits Vietnam, U.S. Jibes Hang over New Partnership,” Reuters, September 29, 2016.

“PH, Russia Communication Offices to Partner in Info Dissemination,” Interaksyon, May 30, 2017.

“Philippines’ Duterte Tells Obama to ‘Go to Hell,’” BBC, October 4, 2016. As of August 9, 2019:
<https://www.bbc.com/news/world-asia-37548695>

Pickrell, Ryan, “A Chinese Navy Fighter Jet Crashed on a Chinese Island in the South China Sea, Killing Both Pilots,” *Business Insider*, March 12, 2019. As of August 7, 2019:
<https://www.businessinsider.com/chinese-navy-fighter-jet-crash-hainan-2019-3>

Pitlo III, Lucio Blanco, “Ambiguity and Changing Times Compel Review of the Philippine-U.S. Mutual Defense Treaty,” Asia Maritime Transparency Initiative, February 8, 2019.

“PLA Air Force Releases Apparent H-6K Photographed with Taiwan’s Jade Mountain [解放军空军发布疑似轰-6K与台湾玉山合影],” *Observer* [观察者], December 17, 2016. As of August 10, 2019:
http://www.guancha.cn/military-affairs/2016_12_17_384771.shtml

PLAAF—See People’s Liberation Army Air Force.

“Polls Show Taiwanese Public Indifferent to Tsai: Poll Expert Michael You,” *Taiwan News*, May 25, 2019. As of August 7, 2019: <https://www.taiwannews.com.tw/en/news/3710534>

Ponniah, Kevin, and Lazara Marinkovic, “The Night the US Bombed a Chinese Embassy,” *BBC*, May 7, 2019. As of August 8, 2019: <https://www.bbc.com/news/world-europe-48134881>

Poushter, Jacob, and Caldwell Bishop, “People in the Philippines Still Favor U.S. over China, but Gap Is Narrowing,” Pew Research Center, September 21, 2017. As of August 7, 2019:

<https://www.pewresearch.org/global/2017/09/21/people-in-the-philippines-still-favor-u-s-over-china-but-gap-is-narrowing/>

Pu Duanhua [濮端华], “An Analysis of China’s Public Opinion Strategy in the Diaoyu Islands Dispute [钓鱼岛争端中的我舆论斗争策略探析],” *Military Correspondent* [军事记者], October 2012.

Public Security Intelligence Agency (Japan), *Annual Report 2016: Review and Prospects of Internal and External Situations*, Tokyo, Japan, January 2017.

Public Service Division (Singapore), “Cultivating a Harmonious Society, Becoming One People,” Prime Minister’s Office, undated. As of August 10, 2019: <https://www.psd.gov.sg/heartofpublicservice/our-institutions/cultivating-a-harmonious-society-becoming-one-people/>

Qian Yibin [钱一彬] and Zhou Xiaoyuan [周小苑], “Cut Off the Network Fraud Black Industry Chain [斩断网络诈骗黑色产业链钱],” *People’s Daily*, July 5, 2018. As of August 7, 2019: http://www.xinhuanet.com/fortune/2018-07/05/c_1123080409.htm

Ranada, Pia, “Duterte to Russia: I’m About to ‘Cross Rubicon’ with US,” *Rappler*, September 28, 2016.

———, “PH, Russia Sign Defense Agreement, 9 Other Deals,” *Rappler*, May 25, 2017a.

———, “PH, Russia Sign 8 Agreements, Including Extradition Treaty,” *Rappler*, November 14, 2017b.

———, “LIST: Deals Signed During Xi Jinping’s Trip to Philippines,” *Rappler*, November 20, 2018.

Ravelo, Jenny Lei, “Japan, China Battle for ODA Influence in the Philippines,” *Devex*, November 20, 2018.

“(Recruiting at LINE@) Information and Opinions on Fake News in the Okinawa Public Referendum [【LINE@で募集中】沖縄県民投票のフェイクニュース情報 意見],” *Okinawa Times*, January 7, 2019.

- Reeves, Jeffrey, Jeffrey W. Hornung, and Kerry Lynn Nankivell, *Vying for Influence: How Competition Between China and Japan Is Shaping the Asia-Pacific's Regional Security*, New York: Routledge, 2017.
- Rekhi, Shefali, "ST to Share Insights from Fight Against Fake News," *Straits Times*, October 26, 2017. As of July 9, 2019: <https://www.straitstimes.com/singapore/st-to-share-insights-from-fight-against-fake-news>
- "Resolution Calls for Hsieh Briefing on Diplomat's Death," *Taipei Times*, December 25, 2018. As of September 17, 2019: <http://www.taipeitimes.com/News/front/archives/2018/12/25/2003706746>
- Rickards, Jane, "The Battle Against Disinformation," *Taiwan Business Topics*, American Chamber of Commerce in Taipei, August 21, 2019. As of September 17, 2019: <https://topics.amcham.com.tw/2019/08/battle-against-disinformation/>
- Roblin, Sebastien, "In 2003, a Chinese Submarine Was Lost at Sea. How the Crew Died Is Terrifying," *The National Interest*, March 25, 2018. As of August 7, 2019: <https://nationalinterest.org/blog/the-buzz/2003-chinese-submarine-was-lost-sea-how-the-crew-died-25072>
- Rui Han [芮晗], "An Analysis of Our Countermeasures Against the US Authorities' Indictment of Chinese Military Officers [美起诉我军官 '网络窃密' 的舆情应对策略探析]," *Military Correspondent* [军事记者], August 2014.
- The SACO Final Report on Futenma Air Station (an Integral Part of the SACO Final Report)*, Ministry of Foreign Affairs (Japan), December 2, 1996. As of August 9, 2019: <https://www.mofa.go.jp/region/n-america/us/security/96saco2.html>
- Saunders, Phillip C., Arthur S. Ding, Andrew Scobell, Andrew N. D. Yang, and Joel Wuthnow, eds., *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*, Washington, D.C.: National Defense University Press, 2019.
- Saunders, Phillip C., and Joel Wuthnow, "China's Goldwater-Nichols? Assessing PLA Organizational Reforms," *INSS Strategic Forum*, April 2016. As of August 7, 2019: <https://apps.dtic.mil/dtic/tr/fulltext/u2/1006824.pdf>
- Schmidt, Michael S., and David E. Sanger, "5 in China Army Face U.S. Charges of Cyberattacks," *New York Times*, May 19, 2014. As of August 7, 2019: <https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html>
- Scobell, Andrew, David Lai, and Roy Kamphausen, eds., *Chinese Lessons from Other Peoples' Wars*, Carlisle, Pa.: Strategic Studies Institute, 2011.

Searight, Amy E., “Chinese Influence Activities with U.S. Allies and Partners in Southeast Asia,” testimony before the U.S.-China Economic and Security Review Commission, April 5, 2018. As of June 10, 2019:

https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180406_Hearing_Amy%20Searight_Written_Statement_April%205%202018.pdf?u6.PMk9Xjxi7ojAhLXImnv_OciYnjHE3y

Sebenius, Alyza, “Facebook, Twitter Can’t Find China Election Meddling Trump Claims,” *Bloomberg*, October 24, 2018.

Shambaugh, David, “China’s Soft-Power Push,” *Foreign Affairs*, July 2015. As of August 7, 2019:

<https://www.foreignaffairs.com/articles/china/2015-06-16/china-s-soft-power-push>

Shan, Shelley, “CtiTV Penalized Another NT\$1M for Pomelo Story,” *Taipei Times*, April 11, 2019.

Shen Jinke [申进科], “Optimize Information Provision to Lead Online Public Opinion [优化信息供给引领网络舆论],” *Xinhua*, December 8, 2017. As of August 7, 2019:

www.xinhuanet.com/mrdx/2017-12/08/c_136809637.htm

Sheng Peilin [盛沛林] and Li Xue [李雪], “On ‘Public Opinion Decapitation’ [论 ‘舆论斩首],” *Journal of the PLA Nanjing Institute of Politics*, May 2006, pp. 114–117.

Shih, Gary, “Chinese Censors Go Old School to Clamp Down on Twitter: A Knock on the Door,” *Washington Post*, January 4, 2019. As of August 7, 2019:

https://www.washingtonpost.com/world/asia_pacific/chinese-censors-go-old-school-to-clamp-down-on-twitter-a-knock-on-the-door/2019/01/04/1bd462e4-f331-11e8-9240-e8028a62c722_story.html

Shin Sugok, “The Recent Merging of Anti-Okinawa and Anti-Korean Hate in the Japanese Mass Media,” *Asia-Pacific Journal: Japan Focus*, Vol. 17, No. 1, January 15, 2019.

Sim, Royston, “Hong Kong to Return 9 SAF Terrex Vehicles to Singapore: Ministry of Foreign Affairs,” *Straits Times*, January 24, 2017.

———, “Select Committee Releases 22 Proposals to Combat Fake News,” *Straits Times*, September 21, 2018. As of July 9, 2019:

<https://www.straitstimes.com/singapore/select-committee-releases-22-proposals-to-combat-fake-news>

Sim, Walter, “The Race Issue: How Far Has Singapore Come?” *Straits Times*, November 8, 2015.

“Singapore Bans Chinese-American Scholar as Foreign Agent,” AP News, August 4, 2017.

- “Singapore Fake News Law a ‘Disaster’ for Freedom of Speech, Says Rights Group,” *The Guardian*, May 9, 2019. As of July 9, 2019: <https://www.theguardian.com/world/2019/may/09/singapore-fake-news-law-a-disaster-for-freedom-of-speech-says-rights-group>
- Sinopec, @SinopecNews, Twitter account, undated. As of August 7, 2019: <https://twitter.com/sinopecnews>
- State Council Information Office of the People’s Republic of China, China’s Military Strategy, May 27, 2015. As of August 7, 2019: http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm
- Statista, “Frequency of WeChat Use in the United States as of January 2018,” webpage, March 21, 2019. As of August 7, 2019: <https://www.statista.com/statistics/815194/wechat-usage-frequency-usa/>
- Stevenson, Alexandra, “Soldiers in Facebook’s War on Fake News Are Feeling Overrun,” *New York Times*, October 9, 2018.
- Stokes, Mark, and Russell Hsiao, “The People’s Liberation Army General Political Department: Political Warfare with Chinese Characteristics,” Project 2049 Institute, October 14, 2013. As of August 7, 2019: <https://project2049.net/2013/10/14/the-peoples-liberation-army-general-political-department-political-warfare-with-chinese-characteristics/>
- Strong, Matthew, “Military Denies Yushan in China Bomber Picture: Peak Likely to be Mount Beidawu in Southern Taiwan: Experts,” *Taiwan News*, December 17, 2016. As of August 7, 2019: <https://www.taiwannews.com.tw/en/news/3053731>
- , “Taiwan Police Detain Man for Spreading Fake News about President,” *Taiwan News*, October 6, 2018. As of August 7, 2019: <https://www.taiwannews.com.tw/en/news/3546358>
- , “Taiwan Police Find Author of Fake Video About Premier Su Tseng-chang,” *Taiwan News*, July 10, 2019. As of August 7, 2019: <https://www.taiwannews.com.tw/en/news/3742144>
- Su Juan [苏娟], “Analysis on the Characteristics of the Spread of Military-Related Public Opinion on the Internet [网络涉军舆情传播特点探析],” *Military Correspondent* [军事记者], March 2017. As of August 7, 2019: http://www.81.cn/jsjz/2017-03/17/content_7529652.htm
- Sun Guangyong [孙广勇], “New Media: The Double Edged Sword in a Changing Southeast Asian Society [新媒体: 东南亚社会转型的双刃剑],” *Military Correspondent* [军事记者], February 2015. As of August 7, 2019: http://www.81.cn/jsjz/2015-02/15/content_6357230.htm

Sun Wenjing [孙文静] and Wang Lin [王林], "The Scarborough Shoal Incident in the Eyes of Foreign Media and Revelations for Our Propaganda Abroad [外媒眼中的黄岩岛事件及对我外宣之启示]," *Military Correspondent* [军事记者], October 2012.

S.U.R.E. Campaign, "About Us," National Library Board, undated. As of July 9, 2019:

<https://sure.nlb.gov.sg/about-us/sure-campaign/>

"Taiwan Opposition Leader Tsai Ing-wen's Facebook Page Flooded with Posts from the Mainland," Reuters, November 12, 2015.

"Taiwan's Taoists Protest Against Curbs on Incense and Firecrackers," BBC News, July 23, 2017.

Tan Yingshuai [谭英帅], "The Practice and Thinking of News Propaganda for the Army Hosting the 'International Military Competition-2017'

[陆军承办"国际军事比赛—2017"新闻宣传的实践与思考]," *Military*

Correspondent [军事记者], January 2018. As of August 7, 2019:

http://www.81.cn/jsjz/2018-01/26/content_7922585.htm

Tang, Dashan, "Tibet Should Build a Major External Propaganda Structure," *Tibet Daily*, September 14, 2013, p. 3.

Tanner, Murray Scot, *Chinese Economic Coercion Against Taiwan: A Tricky Weapon to Use*, Santa Monica, Calif.: RAND Corporation, MG-507-OSD, 2007. As of May 12, 2020:

<https://www.rand.org/pubs/monographs/MG507.html>

Taylor, Guy, "Philippine Defense Official Review of 1951 Mutual Defense Treaty," *Washington Times*, March 5, 2019.

Teng, Kuan Yung, "10 'Fake News' Hoaxes That Went Viral in Singapore," *Must Share News*, April 19, 2017.

Teng Pei-ju, "Authorities to Monitor Chinese Influence on Taiwanese Media:

Tsai," *Taiwan News*, May 12, 2019. As of August 7, 2019:

<https://www.taiwannews.com.tw/en/news/3699992>

"Terrex: Hong Kong to Return Singapore Army Vehicles," BBC, January 25, 2017.

Tian Hong [田弘], Lin Gang [林冈], and Fan Zhiqiang [凡志强], "A Study of the Interaction in Facebook Between Public and Mayors of Kaohsiung, Taipei,

and New Taipei [台湾地方政府领导人使用社交媒体互动研究——以高雄、台

北、新北三市市长Facebook为例]," *Journal of Shanghai*

[上海交通大学学报(哲学社会科学版)], February 2018.

To, James Jiann Hua, *Hand to Hand, Heart to Heart: Qiaowu and the Overseas Chinese*, University of Canterbury, New Zealand, thesis, 2009. As of December 19, 2019:

<https://ir.canterbury.ac.nz/handle/10092/4288>

- Toh, Michelle, "Google Says Singapore Risks Hurting Innovation with Fake News Law," CNN, May 9, 2019. As of July 9, 2019:
<https://www.cnn.com/2019/05/09/tech/singapore-fake-news-law-tech/index.html>
- Treyger, Elina, Joe Cheravitch, and Raphael S. Cohen, *Russian Disinformation Efforts on Social Media*, Santa Monica, Calif: RAND Corporation, RR-4373/2-AF, forthcoming.
- Tritten, Travis, and Chiyomi Sumida, "Protests on Okinawa Aren't Always What They Appear to Be," *Stars and Stripes*, May 23, 2013.
- Tsek.ph, homepage, undated. As of August 7, 2019:
<https://tsek.ph/>
- Tseng Wei-chen, "Lawmaker Seeks Detention for Spreading Fake News," *Taipei Times*, June 10, 2018. As of September 17, 2019:
<http://www.taipeitimes.com/News/front/archives/2018/06/10/2003694626>
- Tu, Aaron, and Jonathan Chin, "Beijing Using Emergent Media to Attract Youth," *Taipei Times*, July 22, 2019. As of August 7, 2019:
<http://www.taipeitimes.com/News/front/archives/2019/07/22/2003719085>
- Tu, Aaron, and William Hetherington, "Defense Bureau to Tackle Propaganda from China," *Taipei Times*, March 4, 2019. As of August 7, 2019:
<http://www.taipeitimes.com/News/taiwan/archives/2019/03/04/2003710821>
- Twitter Safety, "Information Operations Directed at Hong Kong," Twitter Blog, August 19, 2019. As of September 17, 2019:
https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html
- Uren, Tom, Elise Thomas, and Jacob Wallis, "Tweeting Through the Great Firewall," Australian Strategic Policy Institute, September 3, 2019. As of September 17, 2019:
<https://www.aspi.org.au/report/tweeting-through-great-firewall>
- USAF—*See* U.S. Air Force.
- U.S. Air Force, *Air Force Social Media Guide*, 4th ed., 2013.
- , Policy Directive 35-1, March 8, 2018. As of August 7, 2019:
<https://fas.org/irp/doddir/usaf/afpd35-1.pdf>
- U.S. Attorney's Office Southern District of New York, U.S. Department of Justice, "Patrick Ho, Former Head of Organization Backed by Chinese Energy Conglomerate, Sentenced to 3 Years in Prison for International Bribery and Money Laundering Offenses," March 25, 2019. As of December 20, 2019:
<https://www.justice.gov/usao-sdny/pr/patrick-ho-former-head-organization-backed-chinese-energy-conglomerate-sentenced-3>

U.S. Department of Defense, *Annual Report to Congress on Military and Security Developments Involving the People's Republic of China*, Washington, D.C., 2001–2009.

U.S. Department of State, “Global Social Media Presence,” webpage, undated. As of August 7, 2019:

<https://www.state.gov/global-social-media-presence/>

Valencia, Mark, “Whither the US-Philippines Alliance? Analysis,” *Eurasia Review*, March 12, 2019.

Venzon, Cliff, “Duterte Soft Pedals on ‘Sensitive’ China Issues,” *Nikkei Asian Review*, December 20, 2016. As of August 9, 2019:

<https://asia.nikkei.com/Spotlight/Duterte-s-Philippines/>

Duterte-soft-pedals-on-sensitive-China-issues

———, “Philippines’ Wireless Leader Pushes on with Huawei 5G Launch,” *Nikkei Asian Review*, February 12, 2019.

“VERA Files Joins Facebook’s Third-Party Fact-Checking Program in PH,” VERA Files, April 13, 2018.

“Verifying Disinformation in the Okinawa Gubernatorial Election: Fake ‘Even When Communist Party Candidate Onaga Visited America, He Couldn’t Meet Any U.S. Government Official’

[沖縄県知事選で偽情報検証: フェイク「共産党出馬の翁長知事が訪米しても政府関係者の誰にも会えなかった」],” *Okinawa Times*, September 27, 2018.

Viray, Patricia Lourdes, “Senate Minority Wants Probe into Chinese Planes in Davao, Chinese Shows on PTV,” Philstar, July 9, 2018.

Wan, Cara, “No Need to Be Overly Worried About Fake News Laws, Says Ong Ye Kung,” *Straits Times*, April 29, 2019. As of July 9, 2019:

<https://www.straitstimes.com/singapore/>

no-need-to-be-overly-worried-about-fake-news-laws-says-ong

Wang Dapeng [王大鹏], Yue Chunying [岳春颖], and Yan Jie [严洁],

“Research on the Use of Social Media in Election Propaganda in Taiwan: An Analysis Based on In-Depth Interview

[台湾地区选举宣传中社交媒体的使用研究: 一种基于深度访谈的分析],” *Modern Communication*, [现代传播(中国传媒大学学报)], May 2016.

Wang Juntao and Anne-Marie Brady, “Sword and Pen: The Propaganda System of the People’s Liberation Army,” in Anne-Marie Brady, ed., *China’s Thought Management*, London: Routledge, 2011, pp. 124–145.

Wang Kai [王凯], Yu Wei [余伟], Yang Sha [杨莎], Wu Min [吴敏], Hu Yahui [胡亚慧], and Li Shijun [李石君], “Location Inference Method in Online Social Media with Big Data [种大数据环境下的在线社交媒体位置推断方法],” *Journal of Software* [软件学报], Vol. 26, No. 11, 2015, pp. 2951–2963.

- Wang Linyao [王锦尧] and Li Jiaxin [李嘉鑫], “Cultivation of New Media Audience in Military Culture Communication [军事文化传播中新媒体受众的培养],” *Military Correspondent* [军事记者], February 2016. As of August 7, 2019:
http://www.81.cn/jsjz/2016-02/19/content_6919237.htm
- Weisgerber, Marcus, “U.S. Military Should Add Deception to Its Playbook, Pacific Air Forces General Says,” *Defense One*, December 18, 2019. As of December 20, 2019:
<https://www.defenseone.com/threats/2019/12/us-military-should-add-deception-its-playbook-pacific-air-forces-general-says/161982/>
- White, Edward, “Taiwan Warns of ‘Rampant’ Fake News amid China Interference Fears,” *Financial Times*, April 2, 2019. As of September 17, 2019:
<https://www.ft.com/content/0edbf61e-01a6-11e9-99df-6183d3002ee1>
- “Why Is Hate Speech and Fake News Against Okinawa Spreading? Is There Hope for the Internet Era? ‘Fact Check’ Discussion (2)”
 [“なぜ沖縄に対するフェイク情報、ヘイト言説が流れるのか? ネットの時代に希望はあるのか? 「ファクトチェック」座談会【2】”], *Ryūkyū Shimpō*, May 24, 2019.
- Wong, Cassandra, “Singapore Cannot Count on Social Media Platforms to Protect It from Fake News: Edwin Tong,” Yahoo News, November 20, 2018.
- Wong, Edward, Matthew Rosenberg, and Julian E. Barnes, “Chinese Agents Helped Spread Messages That Sowed Virus Panic in U.S., Officials Say,” *New York Times*, April 22, 2020. As of May 28, 2020:
<https://www.nytimes.com/2020/04/22/us/politics/coronavirus-china-disinformation.html>
- Wong, Tessa, “Singapore Fake News Law Polices Chats and Online Platforms,” BBC, May 9, 2019. As of July 9, 2019:
<https://www.bbc.com/news/world-asia-48196985>
- Wu, Rong-I, Russell Hsiao, J. Michael Cole, William Stanton, Mark Stokes, and Stephen M. Young, *The Global Taiwan Brief*, Vol. 3, No. 24, December 12, 2018. As of August 7, 2019:
<http://globaltaiwan.org/2018/12/vol-3-issue-24/>
- Wu Rui [吴瑞], “Be on Guard Against Other Kinds of Soft Warfare [警惕另类软战争],” *Military Correspondent* [军事记者], November 2013, pp. 53–54.
- Wu Xiujuan [吴秀娟], Wu Wei [吴瑛], Zhan Yating [詹雅婷], and Xu Bowen [徐博文], “Communication and Awareness of the Concept of Community for Common Destiny in the Post-Soviet Space [人类命运共同体理念在后苏联空间的传播与认同],” *International Communications* [国际传播], March 2018.

Wu Yanlin [吴艳林], “Process and Characteristics of the Development of Israel’s Online Public Opinion Offense and Defense [以色列网络舆论攻防的发展历程及特点],” *Military Correspondent* [军事记者], October 2018. As of August 7, 2019: http://www.81.cn/jsjz/2018-10/25/content_9322228.htm

Wu Yinsheng [吴银胜] and Mei Jianbing [梅建兵], “Some Inspirations Drawn from the Application of the Booming Social Media in the Psychological Warfare [社交媒体的迅猛发展及心理战运用的几点启示],” *Defense Science and Technology* [国防科技], May 2011, pp. 77–80.

Wuthnow, Joel, and Phillip C. Saunders, *Chinese Military Reforms in the Age of Xi Jinping: Drivers, Challenges, and Implications*, Washington, D.C.: National Defense University Press, 2017. As of August 7, 2019: <https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/ChinaPerspectives-10.pdf>

“Xi Jinping Millionaire Relations Reveal Fortunes of Elite,” Bloomberg, June 29, 2012. As of August 7, 2019: <https://www.bloomberg.com/news/articles/2012-06-29/xi-jinping-millionaire-relations-reveal-fortunes-of-elite>

Xia Yuren [夏育仁], “Beware of the ‘Fisher’ in the ‘Friend Circle’ [警惕‘朋友圈’中的‘钓鱼人’],” *PLA Daily* [解放军报], September 25, 2015. As of August 7, 2019: http://www.81.cn/jfjbmap/content/2015-09/25/content_124477.htm

Xiao Fei [肖飞], “An Initial Exploration on Strategies for Guiding Public Opinion About New High-Tech Weapons and Equipment: Taking Reports About J-15 Shipborne Aircraft as an Example [高新技术武器装备的舆论引导对策初探：以歼-15舰载机报道为例],” *Military Correspondent* [军事记者], May 2013.

———, “Analysis on the Countermeasures to Strengthen the Construction of Our Military’s New Media Power [加强我军新媒体力量建设的对策探析],” *Military Correspondent* [军事记者], January 2017. As of August 7, 2019: http://www.81.cn/jsjz/2017-01/06/content_7440635.htm

Xiao Tianliang [肖天亮], ed., *Science of Military Strategy* [战略学], Beijing, China: National Defense University Publishing House [北京国防大学出版社], 2015.

Xu Mei, “The Driving Force and Restraining Factors of Southeast Asian Chinese in the Promotion of Chinese Soft Power,” *Southeast Asian Studies* [东南亚研究], Vol. 6, 2010, pp. 58–65.

Yang, Sophia, “Kaohsiung Tank Accident Adds One Dead to Four,” *Taiwan News*, August 19, 2016. As of August 7, 2019: <https://www.taiwannews.com.tw/en/news/2968252>

———, “China’s Pro-Unification 31 Measures for Taiwan Have Failed: Academia Sinica Scholar,” *Taiwan News*, January 26, 2019a.

———, “Taiwan’s Want Want Received NT\$2.8 Billion State Grant from China in 2017,” *Taiwan News*, April 23, 2019b.

Ye Zheng [叶征], *Lectures on the Science of Information Operations* [信息作战学教程], Beijing, China: Academy of Military Science Press [军事科学出版社], 2013.

Yeh, Joseph, “Foreign Ministry Denies Reported Plan to Punish Late Diplomat,” *Focus Taiwan*, December 21, 2018. As of September 17, 2019: <http://focustaiwan.tw/news/AIPL/201812210019.aspx>

Yu Chunguang [于春光], “Enhance Public Opinion Guidance Capability for International Hotspot Events [提升国际热点事件舆论引导能力],” *Military Correspondent* [军事记者], July 2012. As of August 7, 2019: http://www.cssn.cn/dubao/201907/t20190719_4936312.shtml

Yuan Ke [袁轲], Zhang Haijuan [张海娟], and Liu Zhe [刘哲], “Research on the New Trend of Information and Network Warfare [信息网络战新趋势研究],” *Digital Technology & Application* [数字技术与应用], December 2012.

Zeng Huafeng [曾华峰] and Shi Haiming [石海明], *Mind Control: The Rules of War and National Security Strategy in the Era of Global Media* [制脑权: 全球媒体时代的战争法则与国家安全战略], Beijing, China: People’s Liberation Army Publishing House [解放军出版社], 2014.

Zhang Gugu [张汨汨], “Actively Use Overseas Social Media to Participate in Military External Propaganda [积极利用海外社交媒体参与军事外宣],” *Military Correspondent* [军事记者], August 2016, pp. 59–60. As of August 7, 2019: http://www.81.cn/jsjz/2016-09/09/content_7250007.htm

Zhang, Lim Min, “Fighting Fake News Here with Legislation,” *Straits Times*, May 13, 2019. As of July 9, 2019: <https://www.straitstimes.com/opinion/fighting-fake-news-here-with-legislation>

Zhang Yu, “Taiwan Actress’ Welcoming Comments on *Liaoning* Put Her Under Scrutiny,” *Global Times*, January 19, 2017. As of August 7, 2019: <http://www.globaltimes.cn/content/1029767.shtml>

Zhang Yuliang [张玉良], ed., *The Science of Campaigns* [战役学], Beijing, China: National Defense University Press [国防大学出版社], 2006.

Zheng, William, “How Official Chinese Propaganda Is Adapting to the Social Media Age as Disaffection Spreads Among Millennials,” *South China Morning Post*, February 10, 2019. As of August 7, 2019: <https://www.scmp.com/news/china/politics/article/2185300/how-official-chinese-propaganda-adapting-social-media-age>

Zhong, Raymond, Steven Lee Myers, and Jin Wu, “How China Unleashed Twitter Trolls to Discredit Hong Kong’s Protesters,” *New York Times*, September 18, 2019. As of September 17, 2019: <https://www.nytimes.com/interactive/2019/09/18/world/asia/hk-twitter.html>

Zhou Yang [周洋], "Analysis of ISIS' Social Media Organization Structure and Public Opinion Strategy [ISIS 社交媒体组织架构与舆论策略解析]," *Military Correspondent* [军事记者], May 2016, pp. 56–58.

Zhu Ningning [朱宁宁], "An Analysis of Russia's Unfolding of Media Warfare Tactics amid the Turbulent Political Situation in Ukraine [乌克兰政局动荡中俄对乌舆论战谋略运用探析]," *Military Correspondent* [军事记者], May 2014.

The Chinese military's focus on information warfare is expanding to include information operations on social media. Given the possibility of U.S.-China conflict over Taiwan or another regional contingency, understanding how the People's Liberation Army (PLA) thinks about the use of disinformation campaigns on social media has emerged as an important question for U.S. national security policymakers and defense planners. This report describes how the PLA might direct social media disinformation campaigns against the United States and its armed forces, especially the U.S. Air Force. The authors conducted interviews with regional experts during three trips to Asia and reviewed Chinese-language writings and analyses of publicly attributed, or at least reasonably suspected, examples of Chinese disinformation and other malign social media activity on both Chinese and foreign platforms. The authors identify key Chinese practices and the supporting infrastructure and conditions needed to engage in successful social media disinformation campaigns and conclude that China is using Taiwan as a test bed for developing attack vectors. The authors recommend being competitive in shaping and countering messages on social media, working to engage and protect Chinese-American service members (China's most likely targets), and incorporating adversary social media disinformation into future wargames.

\$32.00

ISBN-10 1-9774-0719-6
ISBN-13 978-1-9774-0719-1www.rand.org