STRATEGY FOR EXPLOITING VULNERABILITIES IN CHINESE
INFORMATION CONTROL

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
Information Advantage Scholar

by

KENDALL S. P. GOMBER, MAJOR, U.S. ARMY
M.S., National Intelligence University, Bethesda, MD, 2020
B.S., United States Military Academy, West Point, New York, 2010

Fort Leavenworth, Kansas
2022

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YYYY) 10-06-2022	2. REPORT TYPE Master's Thesis	3. DATES COVERED *(From - To)* AUG 2021 – JUN 2022

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Strategy for Exploiting Vulnerabilities in Chinese Information Control	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)	5d. PROJECT NUMBER
MAJ Kendall S.P. Gomber	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301	8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
While many democracies idealize the free and open flow of information, authoritarian regimes prioritize information as an element to control the population's perception. One method the Communist Party of China (CPC) employs to leverage the influence of the information environment is extensive control in the informational dimension. The CPC ensures that information control is at the forefront of achieving the desired end state during and short of armed conflict. An analysis of the Chinese censorship response in three environments: Tiananmen Square in 1989, Hong Kong Protests in 2019, and Covid -19 in 2020, demonstrates how the Chinese respond when challenged in the informational dimension. Furthermore, understanding how the Chinese Government responds to varying pressure levels in the informational dimension provides insight into how the U.S. Army can exploit Chinese censorship and information control. Finally, three strategies are proposed for the U.S. Army to gain the information advantage when contending with CPC information control.

15. SUBJECT TERMS
Chinese Information Control, Information Advantage, Information Strategy

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. PHONE NUMBER *(include area code)*
(U)	(U)	(U)	(U)	93	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Kendall S.P. Gomber

Thesis Title: Strategy for Exploring Vulnerabilities in Chinese Information Control

Approved by:

_____, Thesis Committee Chair
John H. Modinger, Ph.D.

_____, Member
William M. Raymond, Jr., Ph.D.

_____, Member
LTC Mark B. McCool, M.A.

Accepted this 10th day of June 2022 by:

_____, Assistant Dean of Academics for
Dale F. Spurlin, Ph.D.   Degree Programs and Research

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

STRATEGY FOR EXPLOITING VULNERABILITIES IN CHINESE INFORMATION
CONTROL, by Kendall Gomber, 93 pages.

While many democracies idealize the free and open flow of information, authoritarian
regimes prioritize information as an element to control the population's perception. One
method the Communist Party of China (CPC) employs to leverage the influence of the
information environment is extensive control in the informational dimension. The CPC
ensures that information control is at the forefront of achieving the desired end state
during and short of armed conflict. An analysis of the Chinese censorship response in
three environments: Tiananmen Square in 1989, Hong Kong Protests in 2019, and Covid
-19 in 2020, demonstrates how the Chinese respond when challenged in the informational
dimension. Furthermore, understanding how the Chinese Government responds to
varying pressure levels in the informational dimension provides insight into how the U.S.
Army can exploit Chinese censorship and information control. Finally, three strategies
are proposed for the U.S. Army to gain the information advantage when contending with
CPC information control.

ACKNOWLEDGMENTS

TABLE OF CONTENTS

ACRONYMS

CAC	Cyberspace Administration of China
COVID-19	Coronavirus Disease 2019
CPC	Communist Party of China
FAS	Feasibility, Acceptability, Suitability
FY	Fiscal Year
GEC	Global Engagement Center
MILDEC	Military Deception
NDAA	National Defense Authorization Act
PLA	People's Liberation Army
PRC	People's Republic of China
SSF	Strategic Support Force
TTPs	Tactics, Techniques, and Procedures

TABLES

CHAPTER 1

INTRODUCTION

Background

The rapid and expansive proliferation of information drives a more profound

ability to influence and shape individual and collective perspectives in the current

environment. The Communist Party of China (CPC) strives to fully leverage the power of

the information environment by controlling the informational dimension. Modern CPC

practices of information control are tied to the invention of the world wide web. In 1997,

Wired magazine popularized the term the "Great Firewall of China" to articulate the

CPC's desire to control the spread of information over the world wide web.[1] The publicly

declared purpose of the "Great Firewall of China," officially titled The Golden Shield

Project, is to protect Chinese society from wrong information originating outside the

People's Republic of China (PRC).[2] Despite the early adaptation, the Firewall was not

initially as intrusive as today. However, over the past 25 years, increasing restrictions and

---

[1] Geremie R. Barme and Sang Ye, "The Great Firewall of China," *Wired,* June 1, 1997, https://www.wired.com/1997/06/china-3/.

[2] Sonali Chandel, Zang Jingji, Yu Yunnan, and Sun Jingyao, "The Golden Shield Project of China: A Decade Later—An in-Depth Study of the Great Firewall," *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)* (Guilin, China, 2019): 111, https://www.computer.org/csdl/proceedings-article/cyberc/2019/254200a111/1gjS1msFzmE.

evolutions have enabled the CPC to maintain what experts widely consider the most

extensive and oppressive internet control in the world.[3]

Chinese internet censorship has evolved to match the expansion of technology.

Internet censorship began with the simple blocking of domain names and IP addresses

before advancing to incorporate keyword censorship.[4] The focus then turned to

preventing evasion through the detection of circumvention tools such as virtual private

networks (VPNs).[5] This level of internet censorship results in a society where most young

citizens do not know how the internet looks outside of the firewall restrictions.[6]

Following technical developments, the government transitioned to focus on

developing information control policy. In 2014 the CPC established the Cyberspace

Administration of China (CAC) as the country's internet regulator and information

security element to spearhead modernization and protection efforts. For example, in

2019, the CPC introduced additional rules to minimize dissent toward the Chinese

government online, authorizing the punishment of individuals and platforms for

---

[3] Adrian Shahbaz and Allie Funk, *Freedom on the Net 2021: The Global Drive to Control Big Tech* (Washington, DC: Freedom House, 2021), https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech.

[4] Chandel et al., "The Golden Shield Project of China," 112.

[5] Ibid.

[6] Bang Xiao, "'I Don't Know Facebook or Twitter': China's Great Firewall Generation Z Cut off from the West," *ABC News,* November 9, 2018, https://www.abc.net.au/news/2018-11-10/chinas-great-firewall-generation-who-dont-know-facebook/10479098.

misrepresenting the CPC on the internet.[7] The Chinese government bans most

international social media platforms to enable further information control. However,

Chinese versions replace Western social media platforms with platforms supported by

Chinese companies willing to openly share information with the CPC. For example, the

PRC blocked Twitter in 2009 and instead created Weibo to share ideas limited to 140

characters.[8] Also, the Chinese technology conglomerate Tencent created WeChat as the

Chinese replacement for WhatsApp. However, WeChat shares all stored information with

the Chinese government.[9] WeChat is the most popular messaging app in PRC,

maintaining over one billion monthly active users. According to a 2019 survey, "over

50% of the correspondents said they relied quite heavily on WeChat for information and

communication."[10] A final popular social media site is YY, a Chinese live-streaming

platform with over 300 million registered users enabling connections with a virtual

---

[7] "China Gives Police Powers to Monitor Social Media Friends, Chat Groups," Radio Free Asia News and Information, September 27, 2016, https://search.proquest.com/docview/1823988139?accountid=10504.

[8] BBC, "Social Media And Censorship In China: How Is It Different To The West?" *BBC News*, September 26, 2017, http://www.bbc.co.uk/newsbeat/article/41398423/social-media-and-censorship-in-china-how-is-it-different-to-the-west.

[9] Ibid.

[10] Lotus Ruan, Jeffrey Knockel, and Masashi Crete-Nishihata, *Censored Contagion: How Information on the Coronavirus Is Managed on Chinese Social Media*, Research Report #125 (Toronto, Canada: Citizen Lab, March 3, 2020), 6, https://citizenlab.ca/2020/03/censored-contagion-how-information-on-the-coronavirus-is-managed-on-chinese-social-media/.

community.[11] These social media platforms encompass the robust social media culture where citizens heavily rely on the internet for information.

Internet control is not the limit of CPC censorship. The PRC maintains one of the most restrictive media environments in the world. The PRC's State Administration of Radio, Film, and Television (SARFT) controls all radio, television, satellite, and internet broadcasts within the country.[12] Chinese law prohibits private ownership within the media environment making it fundamentally different than the U.S. media atmosphere.[13] The France-based watchdog group Reporters Without Borders ranked the PRC 177 out of 180 countries in its 2021 worldwide press freedom index, in front of Eritrea, North Korea, and Turkmenistan.[14] The CPC systematically creates barriers for nonstate institutions leading to constraints on the types of information available to the Chinese population.[15]

---

[11] Tomio Geron, "YY.com: China's Unique Real-Time Voice and Video Service with a Virtual Goods Twist," *Forbes*, June 18, 2012, https://www.forbes.com/sites/tomiogeron/2012/06/11/yy-com-chinas-unique-real-time-voice-and-video-service-with-a-virtual-goods-twist/?sh=13ef684a43d1.

[12] "Agencies Responsible For Censorship In China," Congressional-Executive Commission On China, accessed April 19, 2022, https://www.cecc.gov/agencies-responsible-for-censorship-in-china.

[13] Coco Feng, "Beijing Updates Ban On Private News Media, Prohibiting Events," *South China Morning Post*. October 9, 2021, https://www.scmp.com/tech/policy/article/3151778/beijing-reiterates-ban-private-capital-news-media-updating-it-prohibit.

[14] "China," Reporters Without Borders, accessed April 19, 2022, https://rsf.org/en/china.

[15] "Information Control And Self-Censorship In The PRC And The Spread Of SARS," Congressional-Executive Commission On China, accessed April 19, 2022,

The Chinese legal system also encourages individual self-censorship through ill-defined laws and a lack of genuine protection for freedom of expression.[16] For example, Weibo discourse is significantly different from Twitter. People on Weibo tend to post more about their personal lives than discuss politics, likely due to censorship concerns and the internalization of cultural norms.[17] Extensive Chinese censorship and information control results in a fundamentally different understanding of the information environment impacting any U.S. information strategy response.

<div align="center">Problem Statement</div>

While many democracies idealize the free and open flow of information, authoritarian regimes view information as an element to control. The Chinese approach is one such example of information control in authoritarian regimes. Their restrictions within the informational dimension result in information operations being at the forefront of achieving the desired end state both during and short of armed conflict. In 2017, CPC General Secretary Xi Jinping announced a modernization of the People's Liberation Army (PLA) to create a world-class military.[18] The PLA highlights achieving information

---

https://www.cecc.gov/publications/issue-papers/information-control-and-self-censorship-in-the-prc-and-the-spread-of-sars.

[16] Ibid.

[17] BBC, "Social Media And Censorship In China: How Is It Different To The West?"

[18] "Full Text of Xi Jinping's Report at 19th CPC National Congress," Xinhua, November 3, 2017, http://www.xinhuanet.com/english/special/2017-11/03/c_136725942.html.

dominance as a requirement for successful modernization.[19] ATP 7-100.3, *Chinese Tactics*, described stratagems as essential to PLA planners. Rather than describing friendly actions as is common in the U.S. Army, PLA Planners use stratagems to "describe the enemy's mindset, focusing on achieving the desired perceptions by the opponent, and then prescribing ways to exploit this perception."[20] The U.S. Army requires an information strategy that accounts for the Chinese understanding of the informational dimension. New doctrine focuses on understanding Chinese tactics but falls short of providing solutions to counter the unique Chinese approach to information warfare.

<p style="text-align:center;">Purpose of the Study</p>

Understanding how the Chinese Government responds to varying levels of pressure in the informational dimension will provide insights into how the U.S. Army can take advantage of Chinese censorship to gain an information advantage. Lacking examples of the PLA in combat, it is necessary to evaluate the PLA's doctrinal approach to information. PLA doctrine, coupled with examples of the CPC's response to challenges in the information environment, indicates how the Chinese respond when contested in the informational dimension. This study seeks to identify opportunities for

---

[19] Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People's Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), https://www.rand.org/pubs/research_reports/RRA394-1.html.

[20] Headquarters, Department of the Army (HQDA), Army Techniques Publication (ATP) 7-100.3, *Chinese Tactics* (Washington, DC: Army Publishing Directorate, August 9, 2021), 1-13, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN33195-ATP_7-100.3-000-WEB-1.pdf.

U.S. information strategy to exploit vulnerabilities in the informational environment resulting from censorship and information control.

Research Questions

Primary Research Question

How can the U.S. Army exploit vulnerabilities in the Chinese approach to the information environment for an asymmetric advantage?

Secondary Research Questions

1. How does the CPC control information domestically and internationally?

2. How do Chinese information tactics, techniques, and procedures (TTPs) change when challenged?

3. How does the U.S. approach to information operations contrast with the Chinese approach?

Hypothesis

Extensive Chinese censorship and the Chinese way of war's focus on information and deception require a specific information warfare strategy to gain and maintain the information advantage.

Assumptions

This study makes several key assumptions. First, the CPC will continue to control its domestic population's access to information. Second, the PRC will continue modernization efforts synchronized with General Secretary Xi's 2035 plan. Third, the study also assumes that Chinese doctrine is indicative of how the Chinese forces will

respond in contested environments. Finally, the study assumes that past CPC tendencies

indicate future responses when contested in the informational environment.

Definition of Terms

Conflict Continuum: The environment in which the United States "applies the

instruments of national power (diplomatic, informational, military, economic) to achieve

objectives."[21] This definition is consistent with U.S. military joint doctrine.

Informational Dimension: "encompasses where and how information is collected,

processed, stored, disseminated, and protected."[22] This definition is consistent with U.S.

military joint doctrine.

Information Environment: "The aggregate of individuals, organizations, and

systems that collect, process, disseminate, or act on information."[23] This definition is

consistent with U.S. military joint doctrine.

Information Operations: The integrated employment of information-related

capabilities to influence, disrupt, corrupt, or usurp individuals' decision-making.[24] This

definition is similar to but not synonymous with the U.S. Department of Defense's (DoD)

---

[21] Chairman of the Joint Chiefs of Staff (CJCS), Joint Doctrine Note (JDN) 1-19, *Competition Continuum* (Washington, DC: Joint Chiefs of Staff, June 3, 2019), 2, https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf.

[22] Chairman of the Joint Chiefs of Staff (CJCS), Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: Joint Chiefs of Staff, November 27, 2012), I-3, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

[23] Ibid., I-1.

[24] Ibid.

term "information operations." This is a broader definition to encompass the Chinese understanding of information operations which is not limited to an adversary.[25]

Information Superiority: "The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[26] This definition is consistent with U.S. military joint doctrine.

People's Liberation Army (PLA): The PRC's military and organizational structure are comparable to the U.S. DoD. PLA does not refer exclusively to ground forces.[27]

Scope

A holistic strategy to counter the Chinese in the information environment is beyond the scope of this thesis. Instead, it focuses on vulnerabilities that arise from the Chinese approach to information. The evaluation highlights vulnerabilities that arise specifically from censorship and information control. Finally, it includes an analysis of the Chinese censorship response in three environments: Tiananmen Square protests in 1989, Hong Kong protests in 2019, and Coronavirus Disease (COVID-19) global outbreak in 2020, providing insight into how the Chinese respond when challenged in the informational dimension.

---

[25] HQDA, ATP 7-100.3, 1-6.

[26] CJCS, JP 3-13, G-3.

[27] HQDA, ATP 7-100.3, 1-3.

The two most significant limitations of this study are time and classification. The Command and General Staff Officers' Course (CGSOC) requires the study to be completed within nine months. A thesis at CGSOC aims to expand the body of knowledge based on publicly available information. Therefore, all research and development are based on publicly available information. The limitation of only using unclassified information is due to both access and usefulness. Through limiting information sources, the study will be more broadly read, considered, and applied.

The environments the study evaluates are a delimitation of the thesis. There are infinite options for evaluating Chinese information control. This thesis is limited to Chinese government responses to Tiananmen Square, pro-democracy protests in Hong Kong, and COVID-19. Tiananmen Square provides a historical case for understanding contemporary information control. Hong Kong demonstrates a limited environment that seeks to counter Chinese censorship influence. Finally, Covid-19 demonstrates the Chinese response when contested on a global scale in the informational dimension. In total, these three cases will provide the basis for identifying opportunities for the United States (U.S.) to gain the information advantage when contesting the PRC in the information environment.

Significance of the Study

The PRC is a near-peer competitor to the United States (U.S.) with significant political and strategic interests that conflict with U.S. national interests. The ultimate goal of the new Chinese grand strategy is to achieve status as a world power. Jinping's modernization strategy upholds information dominance as essential to ensure military

success in any campaign. Therefore, for the U.S. Army to remain competitive with the

PLA, U.S. Army leaders at all levels must fully understand the Chinese mindset

regarding information warfare. Currently, there is a lack of understanding of how to

compete with the Chinese in the informational dimension. This thesis expands where new

doctrine falls short by identifying vulnerabilities in the Chinese approach to information

warfare. Furthermore, it raises awareness about indications and warnings of opportunities

that commanders can identify to counter the Chinese information strategy.

CHAPTER 2

LITERATURE REVIEW

Introduction

This study focuses on understanding multiple sources of information regarding

Chinese information strategy throughout this chapter. This literature review explores the

incongruities between Chinese and U.S. information strategies. The literature used

throughout the research includes official government documents, academic books, peer-

reviewed journals and publications, and reputable websites. This analysis seeks to

address the supporting questions of this thesis, which include:

1. How does the CPC control information domestically and internationally?

2. How do Chinese information tactics, techniques, and procedures (TTPs)

   change when challenged?

3. How does the U.S. approach to information operations contrast with the

   Chinese approach?

As briefly mentioned in chapter one, Chinese information strategy offers a unique

problem for U.S. military strategists. The authoritarian regime's unprecedented ability to

control information significantly impacts the information environment. This chapter

summarizes research regarding information strategy and control to further understand this

unique operating environment. The organization of the material first provides an

overarching view of Chinese censorship, Chinese understanding of deception, the

Chinese focus on information warfare, and concludes by summarizing the current U.S.

strategy for information warfare.

<center>Chinese Censorship</center>

When researching Chinese censorship, most literature can be divided into two areas: the first is censorship methods; in recent years, avenues for censorship are especially focused on information disseminated online, and the second is the "self-censorship" that results from living within the Chinese culture. This section seeks to summarize the findings and importance of these two topics. Chinese publications, global research findings regarding Chinese censorship, U.S. and CPC government documents, nongovernment agency and nonprofit reports, and news reporting inform the topic development.

The CPC incorporates extensive mechanisms within Chinese society for controlling information. One mechanism hereafter referred to as propaganda is the active promotion of Chinese government content. This mechanism is enhanced through censorship, the active suppression of information, and the obstruction of information outlets that counter the government plan.[28] To understand the Chinese perspective on censorship, it is essential to recognize the extensive legacy of Chinese propaganda. The Chinese propaganda system impacts virtually every organization and aspect spreading and communicating information. The Chinese term for "propaganda" is a neutral term meaning "informational messages that publicize and promote a particular political point of view."[29] The Chinese understanding of propaganda's definition opposes the negative

---

[28] Sarah Cook, *Beijing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence since 2017,* Special Report (Washington, DC: Freedom House, January 2020), https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone.

[29] John Dotson, *The Confucian Revival in the Propaganda Narratives of the Chinese Government,* Staff Research Report (Washington, DC: U.S.-China Economic

connotations of disinformation associated with the English definition. An expansive, all-encompassing definition of propaganda is not a new concept in Chinese society.[30]

Propaganda is intertwined with Chinese history, for example, propagating the belief that the emperor existed as a demigod or the "Son of Heaven."[31] This historical integration set the foundation for Chinese society's acceptance of the CPC's extensive use of propaganda.

However, not all scholars unanimously support the idea that there is an uninterrupted history of propaganda within the PRC. Many scholars identify the Republican period following the fall of the Qing dynasty in 1912 as a time when Chinese people maintained and sought independence from the acceptance of political ideology due to weakened government influence.[32] However, even during this period, Chinese journalism did not exist separate from the state, meaning that journalists remained pressured to censor through political affiliations.[33] Additionally, studies on the evolution of Chinese propaganda highlight that although its influence has vacillated throughout

and Security Review Commission, June 20, 2011), 5, https://www.uscc.gov/sites/default/files/Research/Confucian_Revival_Paper.pdf.

[30] David Shambaugh, "China's Propaganda System: Institutions, Processes, and Efficacy," *The China Journal* 57 (January 2007): 28, https://www-jstor-org.lumen.cgsccarl.com/stable/20066240?seq=1.

[31] Michael McCarty, "The Historical Roots of Chinese Communist Propaganda," *The Pulse,* 2005, https://www.baylor.edu/pulse/index.php?id=33634#1d.

[32] Stephen R. Mackinnon, "Toward a History of the Chinese Press in the Republican Period," *Modern China* 23, no. 1 (January 1997): 4, https://www-jstor-org.lumen.cgsccarl.com/stable/189462?seq=1.

[33] Ibid., 5.

Chinese history, it was a central mechanism for establishing the CPC in 1949 and onward.[34] Mao Zedong is widely considered a master propagandist; he relied on a variety of different techniques, including, but not limited to mass mobilization campaigns, creating study groups and ideological monitors throughout society, consistent publication of documents to be memorized and implementing a nationwide system of loudspeakers capable of reaching every citizen.[35]

One way to enhance propaganda is to suppress contrary or unwanted information. In addition to today's Chinese state-run media, the CPC has an established mechanism to censor the information available to the domestic population. The most overt censorship of information is the PRC's treatment of journalists. According to Reporters Without Borders, in addition to the increasingly frequent expulsion of foreign journalists in 2020, the PRC held the record for jailing the most reporters in the world.[36] Experts attribute the Chinese ability to jail reporters to establishing an "extensive and burdensome licensing scheme overall media that bars those without money and political connections from establishing publishing enterprises."[37] Several American newspapers have run articles highlighting the recent undulation of the CPC's allowance of freedom of speech in recent years. The CPC's stance has transitioned between encouraging and openly banning speech. Today, the PRC is withholding the right to freedom of speech to only approved

---

[34] Shambaugh, "China's Propaganda System," 26.

[35] Ibid., 27.

[36] "China," Reporters Without Borders.

[37] "Information Control And Self-Censorship In The PRC And The Spread Of SARS," Congressional-Executive Commission On China.

government officials, known as the "free speech elite."[38] In 2019, *The Guardian* ran an article stating that Chinese journalists will be required to pass a test demonstrating their mastery of Xi Jinping thought. The article quoted journalists who did not demonstrate concern with the test, articulating the need to "correctly lead public opinion."[39] This anecdote demonstrates the Chinese perspective of the fundamental relationship between the government and the media.

Today, in addition to the state-run media that dominates Chinese news, the CPC seeks to use propaganda to influence global perceptions. CPC General Secretary Xi Jinping consistently expanded Chinese foreign power influence. In 2016, Xi said, "Wherever the readers are, wherever the viewers are, that is where propaganda reports must extend their tentacles."[40] International news articles have sought to demonstrate how the PRC's domestic restrictions are taking hold within the international community. One clear example of the PRC's ability to influence Western free speech norms is from September 2021. The United Kingdom warned Bill Browder, an American-born British financier, not to travel to any country with extradition agreements with Hong Kong, including democracies such as South Africa and Portugal.[41] He risked arrest for publicly

---

[38] "Information Control And Self-Censorship In The PRC And The Spread Of SARS," Congressional-Executive Commission On China.

[39] Lily Kuo, "Chinese Journalists to Be Tested on Loyalty to Xi Jinping," *The Guardian*, September 20, 2019, https://www.theguardian.com/world/2019/sep/20/chinese-journalists-to-be-tested-on-loyalty-to-xi-jinping.

[40] Cook, *Beijing's Global Megaphone*.

[41] Suzanne Nossel, "Chinese Censorship Is Going Global," *Foreign Policy*, October 26, 2021, https://foreignpolicy.com/2021/10/26/chinese-censorship-enes-kanter-celtics-browder-is-going-global/.

calling for Britain to push back against human rights abuse in Hong Kong. Another

example of influence occurred in Malaysia regarding the banning of *The Epoch Times*; a

Falun Gong-affiliated newspaper attributed to CPC pressure.[42]

    With obvious examples of the Chinese ability to control the information

environment outside its borders, scholars seek to understand all the methods the PRC is

implementing to gain and maintain its influence. An area of particular focus is the ability

to influence through economic means. For most of the 21st-century, researchers have

remained split on the PRC's ability to influence through economic means. Some scholars

argue that empirical research on the PRC's international influence are inconclusive.[43]

However, some studies (Boston College Professor of political science, Robert Ross's

Balance of Power Politics and the Rise of China: Accommodation and Balancing in East

Asia (2006) and Boston College and Cornell University Professor Jonathan Kirshner's

The Consequences of China's Economic Rise (2008)), support the results of a 2014 study

from Scott L. Kastner, Professor of Government and Politics at the University of

Maryland, who used quantitative research to demonstrate "increased trade dependence on

China is correlated with an increased likelihood of taking an accommodating stance on

---

[42] Wanning Sun, *Media and the Chinese Diaspora: Community, Communications, and Commerce* (New York: Routledge, 2006), xi.

[43] Jonas Gamso, "Is China Exporting Media Censorship? China's Rise, Media Freedoms, and Democracy," *European Journal of International Relations* 27, no. 3 (May 22, 2021): 858, https://journals-sagepub-com.lumen.cgsccarl.com/doi/10.1177/13540661211015722.

the economic issue."[44] Additionally, research from Cornell University Professors of Government Gustavo A. Flores-Macías and Sarah E. Kreps (2013) showed evidence that "trading at higher rates with China leads countries to vote with China on human rights resolutions in the UN General Assembly."[45]

Additionally, in May 2021, Jonas Gamos, a professor at Arizona State University, conducted a study published to evaluate the influence of the PRC's advancing global censorship agenda.[46] Gamos' study evaluated the relationship between trade with the PRC and censorship, hypothesizing that Chinese censorship "norms spread through economic dominance."[47] His results concluded that "exporting to China is accompanied by higher censorship rates in democracies, while censorship rates are stable in authoritarian countries."[48] This report highlights the influence of authoritarian norms on democracies and the expansion of Chinese information control.

In addition to seeking to influence the global information environment, the CPC remains focused on domestic information control regardless of the method of conveyance. The Chinese methods for controlling the internet are as restrictive as those that control the state media. The Great Firewall of China is an internet regulation system

---

[44] Scott L. Kastner, "Buying Influence? Assessing the Political Effects of China's International Trade," *Journal of Conflict Resolution* 60, no. 6 (2016): 980, https://www-jstor-org.lumen.cgsccarl.com/stable/24755936?seq=1. 980.

[45] Gamso, "Is China Exporting Media Censorship?," 861.

[46] Ibid., 858.

[47] Ibid., 860.

[48] Ibid., 687.

that enables the CPC to filter content and block access to websites. To accomplish this level of internet control, the PRC first controls the Internet gateways, where traffic intersects between the PRC and the global internet. Installing firewalls and proxy servers at these gateways enables the government to analyze and manipulate internet traffic.[49] These systems allow the Chinese government to implement technical TTPs to censor the internet. Censorship TTPs include Domain Name Server (DNS) poisoning, blocking access to internet protocol addresses, analyzing and filtering Uniform Resource Locators (URLs), inspecting and filtering packets, resetting connections, and blocking VPNs.[50]

Through the law, the Chinese seek to control the internet via "'internet sovereignty,' a concept that would give countries the right to control their domestic internet space, and 'data sovereignty,' the idea that data is subject to the laws of the country where it was collected."[51] Through the United Nations, the PRC has also proposed an International Code of Conduct on Information Security codifying a country's rights to control the internet.[52] The Chinese intention is not to create a new separate internet but to allow counties to control the existing one, citing a need to protect national

---

[49] Chris Hoffman, "How the 'Great Firewall of China' Works to Censor China's Internet," How-To Geek, last modified September 10, 2017, https://www.howtogeek.com/162092/htg-explains-how-the-great-firewall-of-china-works/.

[50] Ibid.

[51] Dan Blumenthal and Linda Zhang, "China's Censorship, Propaganda & Disinformation," American Enterprise Institute, July 10, 2020, https://www.aei.org/articles/chinas-censorship-propaganda-disinformation/.

[52] Ibid.

sovereignty and public safety. This mentality is shared as countries, including Russia and Iran, have replicated the Chinese model for internet censorship.[53]

Information censorship is an integral part of the government agenda for the CPC. According to Xiao Qiang, a research scientist at the School of Information at the University of California, Berkeley, "China has a politically weaponized system of censorship; it is refined, organized, coordinated, and supported by the state's resources."[54] The prioritization of information control is no longer limited to influencing the domestic population but globally. The current trend for the CPC is a more aggressive approach to influencing foreign media and seeking innovative ways to publish CPC propaganda.[55] Therefore it is more important than ever to identify an effective means for countering CPC information control as it is now extending outside the country's borders.

Chinese society has a history that encourages self-censorship, which is exacerbated with the implementation of the Social Credit System. The Social Credit System consolidates significant data sets for all Chinese citizens. The information is consolidated into a single numerical score. Points are added for good behavior and deducted for bad actions encouraging citizens to act in a manner favorable to the CPC. As

---

[53] James Lewis, *Sovereignty and the Evolution of Internet Ideology* (Washington, DC: Center for Strategic and International Studies, February 4, 2022), https://www.csis.org/analysis/sovereignty-and-evolution-internet-ideology.

[54] Raymond Zhong, Paul Mozur, Jeff Kao, and Aaron Krolik, "No 'Negative' News: How China Censored the Coronavirus," *The New York Times*, December 19, 2020, https://www.nytimes.com/2020/12/19/technology/china-coronavirus-censorship.html.

[55] Sarah Cook, "The Globalization of China's Media Controls: Key Trends from 2018," *The Diplomat*, November 10, 2020, https://thediplomat.com/2018/12/the-globalization-of-chinas-media-controls-key-trends-from-2018/.

stated in government documents, the program's goal is to "allow the trustworthy to roam everywhere under heaven while making it hard for the discredited to take a single step."[56]

The most extensive government-licensed system is Alibaba's Sesame Credit system. Alibaba's system is framed playfully, not unlike an online rating game.[57] Alibaba's system evaluates credit history, fulfillment capacity, personal characteristics, behavior, preferences, and interpersonal relationships. Additionally, saying positive things to others on social media about the Chinese government, for example, nets users additional points. Users can secure both rewards and punishments associated with their scores. They are also placed on black (negative) and red (positive), impacting daily lives. For example, users who end up on the blacklist cannot purchase airline or train tickets, and their children are unable to attend the best schools. On the other hand, the rewards are less impactful - usually low interest on loans and free health checkups.[58]

Once a user links their social credit account to their social media profiles for identity confirmation, the credit company then has permanent and pervasive access to the entirety of the user's digital life. Using Sesame Credit's score-determining algorithm as an example, online input, including the user's interaction with others via social media platforms, is one of three broad categories of input used in calculating a user's social

---

[56] Pete Hunt, "China's Great Social Credit Leap Forward," *The Diplomat*, December 4, 2018, https://thediplomat.com/2018/12/chinas-great-social-credit-leap-forward.

[57] Min Jiang and King-Wa Fu, "Chinese Social Media and Big Data: Big Data, Big Brother, Big Profit?," *Policy & Internet* 10, no. 4 (2018): 381.

[58] Louise Matsakis, "How the West Got China's Social Credit System Wrong," *Wired*, July 29, 2019, https://www.wired.com/story/china-social-credit-score-system/.

credit score. Censors and moderators use social media posts to verify locations, monitor

lifestyles, and ensure the user acts in a manner consistent with the public interest. Posts

viewed as not in keeping with approved state messaging can be placed on a blacklist

while posting positive messages about the government or the economy can raise the

user's social credit score.[59] The purpose of positively reinforcing pro-government social

media posts is twofold. It encourages users to post positive messages to raise their scores,

but it also helps flood social media platforms with pro-government messaging, reducing

dissenting opinions.

Chinese Focus on Deception

It is inadequate to discuss Chinese deception without a thorough discussion of

Sun Tzu's influence over Chinese thought. Sun Tzu thought is central to understanding

the Chinese narrative. For example, his teachings are considered central to the curriculum

taught at the People's Liberation Army National Defense University (PLANDU), the

highest educational institute for the Chinese military.[60] Sun Tzu is credited with writing,

The Art of War, which continues to influence the global understanding of strategy in

war.[61] One of the fundamental principles that drive the Chinese focus on deception is Sun

---

[59] Jiang and Fu, "Chinese Social Media and Big Data?," 383.

[60] Fumio Ota, "Sun Tzu in Contemporary Chinese Strategy," *Joint Force Quarterly* 73 (2nd Quarter 2014): 76-80. https://ndupress.ndu.edu/Media/News/Article/577507/sun-tzu-in-contemporary-chinese-strategy/.

[61] Sunzi and Thomas F. Cleary, *The Art of War* (Boston, MA: Shambhala, 2005); Alessandro Corneli, "Sun Tzu and the Indirect Strategy," *Rivista Di Studi Politici Internazionali* 54, no. 3 (215) (1987): 419, http://www.jstor.org/stable/42738671.

Tzu's principle, "Warfare is the art of deceit."[62] Sun Tzu elaborates that to effectively

accomplish warfare, "Therefore, when able, seem unable; when ready, seem unready; ...

If the enemy seeks some advantage, entice him with it. … Attack where he is not

prepared; go by way of places where it would never occur to him you would go."[63] These

strategies ultimately encourage the Chinese military to integrate misdirection or

deception into planning processes. Sun Tzu contributes that warfare can be fought

indirectly through deception. The PLA focuses on four specific ideologies. First is a

preference for unconventional warfare. Second is the "value of cheating as a traditional

underpinning of deceptive warfare." [64] Third is "the recognition that change keeps

warfare in a constant state of flux." [65] Fourth is "the imperative to focus on benefiting

from and controlling one's superiority in warfare."[66] These concepts are ingrained in the

Chinese Way of War and integrated into military planning.

Many scholars attest that PLA planners' deception operations are not only

accepted and understood but it is expected. In Chinese history, most heroes are defined

---

[62] Sun Tzu, *The Art of Warfare: The First English Translation Incorporating the Recently Discovered Yin-ch'üeh-shan Texts,* trans. Roger Ames (New York: Ballantine Books, 1993), 104.

[63] Ibid.

[64] Mark Metcalf, "Deception Is the Chinese Way of War," *Proceedings* 143, no.2 (February 2017):1368, https://www.usni.org/magazines/proceedings/2017/february/deception-chinese-way-war.

[65] Ibid.

[66] Ibid.

by their cunning and ability to outsmart the enemy, primarily through stratagems.[67] As briefly discussed during chapter one, stratagems are essential to military planning. The Chinese concept of stratagem is not easily translated into English. However, scholars agree that "scheming" and "manipulation" contribute to the basic connotation but highlight that the term cannot be reduced to meaning deception.[68] Timothy Thomas, an analyst at the Foreign Military Studies Office (FMSO), in *Dragon Bytes: Chinese Information-War Theory and Practice from 1995-2003,* defined stratagem as "a maneuver to deceive or outwit an enemy in war. It is a device for obtaining advantage; trick."[69] However, this definition falls short of an accurate Chinese understanding or application of the concept. The etymology actually inspires a more emotional, perceptive, and deeper philosophical meaning for the Chinese use of stratagem. The fundamental nature of stratagems in Chinese society leads to a focus on indirect information strategy.

The Chinese understanding of deception is not limited to its integration and support of military operations. Ren Li, the editor of *Lectures on Sun Tzu's Art of War*, argued that another Sun Tzu principle, "warfare is a way of deception," is also significant because it demonstrates that warfare is inherently asymmetrical and inconsistent.[70] The

---

[67] Eric Anderson and Jeffrey Engstrom, "China's Use of Perception Management and Strategic Deception," Science Applications International Corporation, Reston, VA, November 2009, 18, https://www.uscc.gov/sites/default/files/Research/ ApprovedFINALSAICStrategicDeceptionPaperRevisedDraft06Nov2009.pdf.

[68] Ibid., 8.

[69] Timothy L. Thomas, *Dragon Bytes: Chinese Information-War Theory and Practice from 1995-2003* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 81.

[70] Metcalf, "Deception Is the Chinese Way of War."

Chinese understanding and widespread use and expectation of deception present challenges for the United States. The propensity for the PLA to use deception even at the tactical level and during training enhances the challenges for the U.S. military in identifying intelligence indications and warnings as well as understanding the operational environment.[71] Any deception measures slow decision-making and can delay the response of U.S. military forces and inhibit the ability to gain and maintain the initiative. Therefore, when developing a counterstrategy to Chinese Information control, the principle of deception cannot be ignored.

Deception is not limited to military operations. It is integrated into all aspects of information operations. In fact, deception is the extension of Chinese censorship operations. According to Xiao Qiang, information control is "not just for deleting something. They also have a powerful apparatus to construct a narrative and aim it at any target with huge scale."[72]

<u>Chinese Focus on Information Warfare</u>

The CPC centralizes the coordination of all Chinese information warfare (IW), but a wide range of actors execute it. Research demonstrates that the PRC is "gaining more fundamental influence over key nodes in the flow of information abroad, as Chinese technology firms with close ties to the government build or acquire content-

[71] Aaron Jensen, "Deception Is Key to Chinese Military Strategies," *The Diplomat*, August 8, 2020, https://thediplomat.com/2020/08/deception-is-key-to-chinese-military-strategies/.

[72] Raymond Zhong et al., "No 'Negative' News: How China Censored the Coronavirus."

dissemination platforms used by tens of millions of foreign news consumers."[73] Although discussed in censorship, it is important to understand that this type of influence also demonstrates information warfare for the Chinese.

As a part of modernization efforts in 2016, the PLA established the Strategic Support Force (SSF), a "theater command-level organization to centralize the PLA's strategic space, cyber, electronic, and psychological warfare missions and capabilities."[74] According to the DoD's 2020 Report to Congress, *Military and Security Developments Involving the People's Republic of China*, the SSF is responsible for PLA IW, which includes missions associated with the PLA's concept of "Three Warfares," which are psychological warfare, public opinion warfare, and legal warfare.[75] Finally, the SSF is the only known organization in the PLA to perform psychological warfare operations to "shape international public narratives, weaken the enemy's will, shape diplomatic and political narratives, and advance the PRC's interests through all phases of conflict."[76]

The PLA divides information warfare techniques into two types at the tactical level: information attack and information defense.[77] Information attack is offensive

---

[73] Cook, *Beijing's Global Megaphone*.

[74] Office of the Secretary of Defense (SecDef), *Military and Security Developments Involving the People's Republic of China: Annual Report to Congress* (Washington, DC: Department of Defense, 2020), 61, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.

[75] Ibid., 62.

[76] Ibid., 61.

[77] HQDA, ATP 7-100.3, 5-4.

operations such as attacking adversarial information, command and control, and intelligence systems. Information defense consists of protecting critical friendly resources. Key to Chinese tactics is the integration of these two concepts recognizing that loss of crucial information is unlikely to be overcome through the gain of information attack.[78]

Today, the Chinese are incorporating deception techniques in concert with advancing technology to overcome shortcomings on the battlefield. For Chinese planners, "stratagems are not developed in isolation but by combining human qualitative thinking with computer-assisted quantitative calculations."[79] Integrating technology and stratagems allow Chinese military officials to standardize military response to battlefield actions. Additionally, the Chinese strive to encourage "enemy commanders to develop decisions in the direction set by the Chinese side."[80] Influencing enemy detection systems is one method for influencing adversarial decisions. For example, using technology to promote indicators of fake troop locations or movements ultimately influences the enemy's common operating picture. Inserting simulated data into enemy command systems demonstrates the Chinese desire to integrate deception warfare into virtual battlefields.

In addition to influencing enemy command systems, the Chinese see advancing technology as an opportunity to integrate novel strategies expanding the domains for

---

[78] SecDef, *Military and Security Developments Involving the People's Republic of China*, 5-3.

[79] Thomas, *Dragon Bytes*, 85.

[80] Ibid., 86.

denial and deception operations. The Chinese goal is to incorporate traditional and new strategies to maximize effectiveness as well as expand the options available for military planners. In addition to integrating technology, such as jamming and sabotaging enemy information systems, the Chinese recognize the importance of including civilian information channels. Summarizing the Chinese information warfare strategies, General Dai wrote of the importance of including "electronics as a potential carrier of strategies; the requirement for an active offense in IW; and the need in China for an integrated network-electronic warfare concept."[81] There appears to be a discrepancy in whether the PRC is pursuing information operations as "active offense," "offensive based defense," or "active offensive defense." Still, regardless of the terminology, it is clear that the Chinese are not pursuing a passive information campaign.

Current U.S. Information Strategy

Information is recognized in the United States as an instrument of national power. However, the United States has long struggled with codifying an information strategy. Following the conclusion of World War II, the U.S. Information and Educational Exchange Act of 1948 (Smith-Mundt Bill) established a diplomacy element of the state department, renamed the United States Information Agency (USIA) in 1953.[82] The USIA's mission was "to understand, inform and influence foreign publics to promote the

---

[81] Thomas, *Dragon Bytes*, 93.

[82] William M. Chodkowski, "The United States Information Agency," (Fact Sheet, American Security Project, Washington, DC, November 2012), 4, https://www.scribd.com/document/112346692/Fact-Sheet-The-United-States-Information-Agency.

national interest, and broaden the dialogue between Americans and U.S. institutions, and

their counterparts abroad."[83] The agency was ultimately abolished in 1999 through the

Foreign Affairs Reform and Restructuring Act.[84] However, even during this time with a

formal diplomacy agency, the RAND Corporation published a report titled *Strategic*

Information Warfare: A New Face of War. [85] It argued for the need to develop an

information strategy stating,

> The United States has substantial information-based resources, including complex
> management systems and infrastructures involving the control of electric power,
> money flow, … and other information-dependent items... Conceptually, if and
> when potential adversaries attempt to damage these systems using IW techniques,
> information warfare inevitably takes on a strategic aspect.[86]

This report was published in 1996, and in the subsequent 25 years, the United States has

only increased its reliance on information-dependent systems, significantly enhancing

vulnerabilities in the absence of an effective information strategy.

In 2012, more recently, in August 2020, Representative Michael McCaul (R-TX)

introduced the United States Information Abroad for Strategic Competition Act into the

House of Representatives. The bill's purpose was to "create an information statecraft

---

[83] "Mission Statement," United States Information Agency, accessed January 14, 2022, https://govinfo.library.unt.edu/npr/library/nprrpt/annrpt/vp-rpt96/appendix/usia.html.

[84] Chodkowski, "The United States Information Agency," 4.

[85] Roger C. Molander, Andrew Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, CA: RAND Corporation, January 1, 1996), https://www.rand.org/pubs/monograph_reports/MR661.html.

[86] Ibid., xiii.

strategy for the U.S. government."[87] The expanded purpose of the strategy was "to reduce

the ability of the Communist Party of China (CCP) to influence global discourse, and

such strategy shall include an identification of (1) specific CCP narratives that contribute

to its ability to influence global discourse, (2) counter-narratives that are most effective

and most likely to reduce the ability of the CCP to influence global discourse, and (3)

specific quantitative objectives for advancing such counter-narratives."[88] As of 2021,

there remains no progression on the bill, demonstrating the need for a refocus on a

cohesive U.S. information strategy to counter Chinese influence.

      Many scholars advocate for a whole of government approach to information

strategy while bemoaning the fact that the United States lacks such a strategy. Kevin

Truitte, an international studies analyst, wrote for the Georgetown Security Studies

Review that the purpose of a whole-of-government approach is the security of America's

informational dimension. He advocated for the need to "expand the understanding of

information security while firmly adhering to the freedoms central to American values."[89]

American values are a central concern in the implementation of an information strategy.

---

[87] USIA for Strategic Competition Act., H. Res. 7938, 116th Cong., (August 4, 2020), https://www.congress.gov/bill/116th-congress/house-bill/7938.

[88] Ibid.

[89] Kevin Truitte, "An American National Information Security Strategy," *Georgetown Security Studies Review*, March 11, 2019, https://georgetownsecuritystudiesreview.org/2019/03/11/an-american-national-information-security-strategy/.

Historian Jon Latimer's book, *War in Deception*, articulated the theory that America values integrity and credibility and strives to retain its reputation.[90]

Despite the inconsistent focus on a U.S. information strategy, it is consistent with fundamental American values to pursue a focused U.S. information strategy. One additional resource with the U.S. Department of State is the Global Engagement Center (GEC). The mission of the GEC is "To direct, lead, synchronize, integrate, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States, its allies, and partner nations."[91] With congressional mandates, the GEC competes in the information dimension at scale while also providing and identifying technical solutions to countering disinformation and misinformation. Stringent information controls, such as those seen in the PRC, inhibit citizens' global connection and ability to exchange information freely.

Scholars advocate for specific U.S. policy regarding other authoritarian regimes, such as North Korea. Nat Kretchun, the deputy director at the Open Technology Fund, a U.S. government-funded organization supporting internet freedom technologies, wrote that to implement an effective strategy against North Korea, the United States must coordinate "leveraging cutting-edge and legacy technologies, enlisting the diplomatic

---

[90] John Latimer, *Deception in War* (Woodstock: The Overlook Press, 2001).

[91] "Global Engagement Center: Core Mission & Vision," U.S. Department of State, January 20, 2022, https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/.

support and understanding of international partners, and finding ways to foster the

technical skills among North Koreans themselves that will enable them to circumvent the

digital restrictions placed on them."[92] These recommendations are necessary for any U.S.

information strategy today.

[92] Nat Kretchun, *The Need for a New US Information Strategy for North Korea*, Special Report No. 451 (Washington, DC: United States Institute of Peace, June 2019), 14, https://www.usip.org/sites/default/files/2019-07/sr_451-the_need_for_a_new_u.s._information_strategy_for_north_korea.pdf.

CHAPTER 3

RESEARCH METHODOLOGY

Introduction

There is extensive discussion across the Department of Defense (DoD) regarding the importance of the informational dimension, but there is a need to develop specific strategies to counter adversaries' unique information approaches. The purpose of this chapter is to describe the methodology used to determine a DoD information strategy to effectively exploit vulnerabilities within Chinese information control processes.

Through an evaluation of the data within three events where the CPC seeks to control information, there is an opportunity to create a precise information strategy to counter Chinese information control effects. The recommended strategy is developed using the insights gained from the case analysis and assessed using Dr. Harry Yarger's assessment criteria, a professor at the U.S. Army War College. Dr. Yarger developed three screening criteria to test military strategy validity: feasibility, acceptability, and suitability (FAS).[93]

Method

Using a qualitative research approach, this study identifies vulnerabilities in Chinese information control. The qualitative research method is the best approach to

---

[93] Harry Yarger, *Strategic Theory for the 21st Century: The Little Book on Big Strategy* (Carlisle, PA: U.S. Army War College, Strategic Studies Institute, February 2006), 70, https://apps.dtic.mil/dtic/tr/fulltext/u2/a444141.pdf.

study this topic, given the complex and descriptive nature of the problem.[94] The Chinese

reaction to challenges in the informational dimension can only be evaluated in its real-life

context. Therefore, the research evaluates three past environments when events

challenged Chinese information control mechanisms and procedures. This study

evaluated three cases: the Tiananmen Square protests, the Hong Kong democracy

protests, and the response to COVID-19.

The reason to analyze these three specific events is that they demonstrate Chinese

information control in unique information environments. The Tiananmen Square protests

can be evaluated historically to understand the longstanding effects of information

control, as well as the information being relatively uncontested. The Hong Kong

democracy protests were able to be responded to deliberately as the situation was known,

developed slowly, and moderately contested information environment. Finally, COVID-

19 was an unexpected event in a severely contested information environment that the

Chinese government had to respond to.

<center>Data Collection and Analysis</center>

The primary data collection will be document analysis. The purpose is to fully

understand the Chinese response to challenges in the informational dimension to enable

an adequate response. Through the thorough analysis of the data collected, the researcher

will identify vulnerabilities to exploit in information strategy. Sufficient data was also

---

[94] R. K. Yin, *Case Study Research: Design and Methods,* 5th ed. (Thousand Oaks, CA: Sage, 2014), quoted in Aikaterni Argyrou, "Making the Case for Case Studies in Empirical Legal Research," *Utrecht Law Review* 13, no. 3 (December 2017): 100.

collected to enable the researcher to deduce whether the Chinese information control

efforts in each case were considered a success or failure.

The author examined each case through a series of filters, followed by an

evaluation of the impact of the Chinese response:

1. CPC identifies an event warranting a coordinated response;

2. It then determines both international and domestic responses;

3. Is this a deliberate or unexpected event?

4. What type of information is being controlled?

5. What is the effect of the information control?

The first step when examining the events is to conduct an overview of each event case.

During this segment, the goal is to extract the distinct vulnerabilities that can be applied

to develop a military strategy. The second step involves an analysis of similarities and

differences in the information control response. This comparison enables the analysis of

the vulnerabilities of the information strategy. The third step is the development of U.S.

courses of action to counter the vulnerabilities. Finally, this strategy is evaluated for its

validity.

Evaluation Criteria

Validity has three screening criteria. First, feasibility evaluates the strategy's

ability to "be executed with the resources available."[95] Another way to understand the

concept of feasibility is to ask the questions, "Can the action be accomplished by the

---

[95] Yin, *Case Study Research,* 100.

means available?" or "Can I squeeze this fruit with my hand?"[96] The following questions assess the strategy's feasibility:

1. Are there financial means to accomplish this strategy?

2. Does the technology exist to accomplish this strategy?

3. Are there personnel qualified to accomplish this strategy?

Second, acceptability scrutinizes if the "effects sought justify the objectives pursued."[97] Acceptability can be more clearly understood through the following types of questions. "Are the effects as well as the methods and resources used to achieve those efforts justified and acceptable to the body politic?" or "Is the juice worth the squeeze?"[98] The following questions evaluate the strategy's acceptability:

1. Is the strategy acceptable to the people of the United States?

2. Is the strategy acceptable to U.S. allies?

Finally, suitability examines the strategy's ability to "accomplish the strategic effects desired."[99] The suitability of the strategy answers questions like "Will the strategy's attainment accomplish the effect desired" or "will the squeeze produce the juice I want?"[100] The following questions evaluate the strategy's suitability:

---

[96] U.S. Army Command and General Staff College (CGSC), "C203: Power and Strategy Slides," (PowerPoint presentation, C203: Power and Strategy Briefing, Fort Leavenworth, KS, 13 September 2021), slide 33.

[97] Yarger, *Strategic Theory for the 21st Century*, 70.

[98] CGSC, "C203: Power and Strategy Slides," slide 33.

[99] Yarger, *Strategic Theory for the 21st Century*, 70.

[100] CGSC, "C203: Power and Strategy Slides," slide 33.

1. Will the strategy target vulnerabilities in the PRC's information strategy?

2. Will the strategy advance U.S. national interests?

3. Will the strategy provide an advantage for the U.S. Military?

4. Is the strategy compatible with international norms?

Summary

The methodology for this thesis evaluated three contested information environments through a specific lens. These evaluations identify vulnerabilities that the United States can exploit with a targeted information strategy. The strategy is developed using the data collected to create a strategy to counter CPC's information control effectively. The strategy is then evaluated using FAS assessment and screening criteria.

CHAPTER 4

ANALYSIS

This chapter analyzes how the CPC has used information control to respond

during three unique contested information environments. The analysis enables an

understanding of CPC response to various information pressures. Events are evaluated

first by explaining the event, followed by the Chinese identification of the need for

information control. Next, the narrative explains the ability for deliberation before the

event, the international and domestic response, and the controlled information types.

Finally, the chapter concludes with an evaluation of the effects of the information control.

This evaluation identifies the opportunities and vulnerabilities that emerge from the

analysis to enable the creation of targeted U.S. Army information strategies.

Tiananmen Square 1989

From April 15 to June 4, 1989, Chinese students led democracy protests

countering the CPC in Tiananmen Square, Beijing. The protests ended when the CPC

sent PLA troops to remove students forcibly.[101] The protests rose to international renown

due to the release of chilling pictures of the event. Especially striking a photo displaying

a single unarmed man carrying two shopping bags standing in front of and temporarily

stopping a column of tanks on June 5, 1989.

Before the "Tank Man," an estimated one million people joined protests in

Beijing to protest various issues, primarily the CPC and corruption, free speech, and lack

---

[101] *The Tank Man,* produced by Antony Thomas (*PBS*, April 11, 2006),
http://www.pbs.org/wgbh/frontline/film/tankman/.

of reforms. The protests culminated in a hunger strike on May 13th, leading CPC leaders to visit protesters on May 19th and declare martial law on May 20th.[102] However, in the following weeks, protesters returned to Tiananmen Square. On the evening of June 3rd, the PLA forcibly removed thousands of demonstrators from Tiananmen Square. The next day the bloodshed continued when people tried to return to the square to identify what had happened. Soldiers were tasked with defending the square and indiscriminately shot people trying to enter the area.[103] On the morning of June 5th, the military was undoubtedly in charge of the square, with unknown numbers of Chinese citizens killed and wounded.[104] Images of the Tiananmen Square Massacre spread worldwide, shocking politicians and private citizens alike.

Coordinated Information Response

The CPC recognized the need to immediately control information coming out of Tiananmen Square. State Department cables reported on June 2nd, "The Beijing city government yesterday expanded press restrictions, prohibiting coverage of student

---

[102] "1989 Tiananmen Square Protests," Amnesty International UK, January 5, 2022, https://www.amnesty.org.uk/china-1989-tiananmen-square-protests-demonstration-massacre.

[103] *The Tank Man,* produced by Antony Thomas.

[104] U.S. Embassy Beijing, Secretary of State's Morning Summary for June 2, 1989, China: Stalemate Continues, June 2, 1989, in National Security Archive Electronic Briefing Book No. 16, *Tiananmen Square, 1989: The Declassified History,* ed. Jeffrey Richelson and Michael Evans, document 8. National Security Archive, June 1, 1999, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB16/index.html.

demonstrators and requiring that all other reporting receive prior approval."[105] However, preemptive attempts to censor were insufficient. Following the crackdown, the Chinese censorship focused on concealing an accurate number of people killed and injured in the event. The Chinese Red Cross initially announced 2,600 people were killed but later retracted that figure to the government-supported number 241.[106] Initial reports from official sources stated that only 300 people were killed in the conflict.

<div align="center">International and Domestic Response</div>

The initial local domestic response centered on the establishment of regaining public order. Beijing's loudspeakers announced martial law and instructed citizens to remain indoors.[107] However, these efforts were only minimally effective as citizens sought to find children, friends, and family in the aftermath of the military action in Tiananmen Square. It was ultimately additional military power, not information, that brought control to the streets of Beijing.[108]

In a cable on July 11, 1989, the recently appointed U.S. Ambassador to the PRC, James Lilley, identified nine Chinese government responses following the international reaction to the Tiananmen Square incident:

---

[105] U.S. Embassy Beijing, Secretary of State's Morning Summary for June 2, 1989.

[106] *The Tank Man,* produced by Antony Thomas.

[107] Ibid.

[108] Ibid.

1. Established an extensive anti-U.S. propaganda campaign utilizing themes from the Cultural Revolution and 1970s.

2. Suddenly restricted arms sales and cut off military and high-level contacts.

3. The Chinese media used to reiterate and flame the tension to encourage conflict.

4. Increased shows of military capability around foreign areas to encourage foreigners to reduce profile.

5. Encouraged a narrative of the U.S. as a corrupting force and prevented international visitors from accepting invitations.

6. Postponed peace corps program.

7. Media intimidation, especially of Voice of America.

8. Attempted to establish the U.S. as the "single bogeyman."[109]

9. Remained cordial if not welcoming to American business opportunities and people.[110]

Lilley also stated that the PRC's most valuable lesson learned in the immediate aftermath of Tiananmen was to restrict foreign observation prior to taking contentious action. He stated that the CPC learned the best process moving forward was to "Close the

---

[109] The CPC likely selected the United States as the primary target for Chinese blame because at the time the United States was in fact the primary foreign influence throughout the PRC. A secondary benefit was that Chinese accusations might drive a wedge between the United States. and its allies, especially in South and Central America where they were sensitive to criticisms of the United States as an imperialistic nation.

[110] U.S. Embassy Beijing, Cable to Secretary of State, PLA Ready to Strike, May 21, 1989, in National Security Archive Electronic Briefing Book No. 47, *The U.S. "Tiananmen Papers,"* ed. Michael L. Evans, document 8, National Security Archive, June 4, 2001, 3-4, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB47/.

door to beat the dog."[111] This statement was made to demonstrate the Chinese leadership

regretted not restricting foreign access because any additional violence against its own

population would risk a reduction in international support. The CPC demonstrated that

maintaining international support was secondary to staying in power.

Deliberate or Unexpected Event

This response was deliberate as they responded to a situation that had been

developing for months. It was clear that once the CPC enacted marshal law, there would

be a need for information operations to control the story.

Methods and Types of Information Controlled

Controlling the narrative was essential for both sides of the incident. Protesters

sought to tell their story and create moments such as giving water to Soldiers.[112] The CPC

took a stringent approach to information despite Deng Xiaoping's age; he was the

decision authority for all information regarding Tiananmen. In addition to manipulating

and controlling information detaining people is another method the CPC employed to

reduce dissent within the domestic population.[113]

The 1989 events at Tiananmen Square remain highly censored on the Chinese

internet and across Chinese social media platforms. In 2019, the University of Toronto

---

[111] U.S. Embassy Beijing, Cable to Secretary of State, PLA Ready to Strike, May 21, 1989, 4.

[112] *The Tank Man,* produced by Antony Thomas.

[113] "Human Rights Activism in Post-Tiananmen China," Human Rights Watch, November 5, 2021, https://www.hrw.org/news/2019/05/30/human-rights-activism-post-tiananmen-china#.

and the University of Hong Kong released a study citing 3,237 censored words related to June 4, 1989.[114] Each year in preparation for the anniversary of June 4th, Chinese authorities increase their security posture. These actions include forcing known activists to leave their hometowns for guarded "vacations," restricting activists' movement and communication, tracking, and detainment.[115]

<center>Effect of Information Control</center>

The initial information control focused on maintaining order and preventing demonstrations' resurgence throughout the PRC. The follow-up focused on identifying ways to minimize damage to the Chinese international reputation. Deng Xiaoping focused on identifying a way forward, which was instituting economic reforms while restricting any political reform.[116] The overarching strategy was to ensure the Chinese people recognized that maintaining civil order, preventing chaos, and achieving economic success are predicated on not challenging the government. This idea led to a fundamental feeling that self-regulation is central to Chinese prosperity.

---

[114] Citizen Lab and Weiboscope HKU, "China's Censored Histories: Commemorating the 30th Anniversary of the Tiananmen Square Massacre," *Global Voices*, April 17, 2019, https://globalvoices.org/2019/04/17/chinas-censored-histories-commemorating-the-30th-anniversary-of-the-tiananmen-square-massacre/.

[115] "China: Tiananmen Injustice Fuels Repression 30 Years On," Human Rights Watch, October 28, 2020, https://www.hrw.org/news/2019/05/30/china-tiananmen-injustice-fuels-repression-30-years.

[116] M. E. Sarotte, "China's Fear of Contagion: Tiananmen Square and the Power of the European Example," *International Security* 37, no. 2 (2012): 159, https://www-jstor-org.lumen.cgsccarl.com/stable/23280417?seq=1.

The effects of the extensive censorship of Tiananmen Square continue to be seen today. Most assessments of the incident are bottom-up explanations of what happened from people on the ground rather than a top-down explanation of why decisions were made.[117] As time has passed, there are increasing regulations and restrictions regarding commemorating the event. As the population that remembers the events begins to die, the PRC might effectively erase Tiananmen Square from its history. For example, Beijing college students in 2006 were unable to identify the event when confronted with famous pictures of the incident.[118]

In 2021, workers removed a monument at a Hong Kong university that commemorated the Tiananmen Square incident, the last statue publicly commemorating the event within the PRC.[119] Since 2020, the government was also able to utilize COVID-19 as justification to ban commemorative vigils in Hong Kong.[120] However, the desire to control the information does lead to vulnerabilities. In attempts to ensure the effective censorship of all information related to June 4th, the CPC at times censored posting with words including "today (今天)," "yesterday (昨天)," and "tomorrow (明天)."[121] This kind of censorship adds attention to the event rather than reducing the interest.

---

[117] Sarotte, "China's Fear of Contagion," 159.

[118] *The Tank Man,* produced by Antony Thomas.

[119] The Associated Press, "Hong Kong University Removes Tiananmen Massacre Statue," *NPR,* December 23, 2021, https://www.npr.org/2021/12/23/1067163101/hong-kong-university-removes-tiananmen-massacre-statue.

[120] Ibid.

[121] Citizen Lab and Weiboscope HKU, "China's Censored Histories."

<u>Hong Kong Democracy Protests 2019</u>

In 2019, proposed amendments to Hong Kong's extradition law, specifically to allow extradition to mainland China, catalyzed months of continuous, extensive, and sometimes violent protests and demonstrations throughout Hong Kong. Due to Hong Kong's history as a British colony and classification as a special administrative region, Hong Kong maintains a unique relationship with the PRC as a part of the "one country, two systems" arrangement. This arrangement enabled Hong Kong to maintain some degree of autonomy, maintaining its judiciary and a separate legal system, including rights of freedom of assembly and freedom of speech.[122]

Coordinated Information Response

The CPC's initial response to the protests was publicly ignoring their existence. This approach could be categorized as the wait-it-out approach. The CPC used this approach, recognizing that the protesters had life commitments and time constraints. In contrast, the government has an indefinite amount of time to respond and influence perceptions.[123] A clear example of active CPC censorship was that instead of covering protesters storming the Legislative Council in July 2019, the PRC's state-controlled

[122] *The Constitution of the People's Republic of China: The Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China*, The Government of the Hong Kong Special Administrative Region of the People's Republic of China, May 2021, 67, https://www.basiclaw.gov.hk/filemanager/content/en/files/basiclawtext/basiclaw_full_text.pdf.

[123] J. J. Rose, "How China Is Winning the Hong Kong Propaganda War," *The Interpreter,* November 19, 2019, https://www.lowyinstitute.org/the-interpreter/how-china-winning-hong-kong-propaganda-war.

media showed propaganda celebrating the 1997 handover.[124] However, as the protests protracted, complete blackout in the information dimension was unsustainable. As protests continued and news of the campaign spread, the CPC's rhetoric transitioned, and the disinformation campaign intensified.

International and Domestic Response

Internationally, the CPC was unable to suppress information regarding the protests. Instead, their information strategy focused on disinformation. In August 2019, Facebook, Twitter, and Google all announced the identification of accounts originating in the PRC, spreading false news or attempting to manipulate information about the Hong Kong protests.[125] Once the domestic population was aware of the protests in Hong Kong, the CPC shifted efforts from suppression of information to actively promoting the story and depicting the protesters as rioters actively misrepresenting footage to denigrate the protesters on Chinese state-run media.[126]

Chinese media also sought the blame for protests on foreign interference, namely the U.S. one popular theory posited the Central Intelligence Agency incited and funded

---

[124] Nicole Einbinder, "China's State-Controlled Media Has Completely Ignored Coverage of Hong Kong Protests," *Business Insider,* July 2, 2019, https://www.businessinsider.com/chinas-state-controlled-media-ignored-coverage-hong-kong-protests-2019-7.

[125] Emily Stewart, "How China Used Facebook, Twitter, and YouTube to Spread Disinformation about the Hong Kong Protests," *Vox,* August 20, 2019, https://www.vox.com/recode/2019/8/20/20813660/china-facebook-twitter-hong-kong-protests-social-media.

[126] Steven Lee Myers and Paul Mozur, "China Is Waging a Disinformation War against Hong Kong Protesters," *The New York Times*, August 13, 2019, https://www.nytimes.com/2019/08/13/world/asia/hong-kong-protests-china.html.

the Hong Kong protesters.[127] After a protester was shot in the eye with a police beanbag round in August, the PRC highlighted a video of the protester accepting cash, trying to make the point that the entire incident was fake—when in fact, it was the video that was fake.[128] Authorities worked to keep the narrative patriotic and straightforward within the Chinese firewall. When some Hong Kong protesters, distraught by the violence, created digital apologies and even condolences on mainstream Chinese social media sites, the posts were almost immediately censored.[129]

Deliberate or Unexpected Event

The CPC was able to plan its campaign slowly, as the protests within Hong Kong not only had precedent but were the response to years of gradual erosion of Hong Kong's autonomy.[130] The calculated approach allowed for the preferred strategy of complete censorship to mainland China to be implemented until no longer feasible. Once the information was reaching the population despite information control, the CPC switched to a deliberate disinformation campaign. The information control then transitioned from

---

[127] Emily Feng and Amy Cheng, "China State Media Present Their Own Version of Hong Kong Protests," *NPR*, August 14, 2019, https://www.npr.org/2019/08/14/751039100/china-state-media-present-distorted-version-of-hong-kong-protests.

[128] Ibid.

[129] Ibid.

[130] Alvin Y.H. Cheung, "Can We Finally Admit That 'One Country, Two Systems' Is Dead in Hong Kong?" Just Security, April 30, 2020, https://www.justsecurity.org/69936/can-we-finally-admit-that-one-country-two-systems-is-dead-in-hong-kong/.

full censorship to publicizing and withholding information that supported the official CPC narrative regarding the protesters.

Type of Information Controlled

The CPC primarily focused on controlling information across mainland the PRC through the Chinese Firewall. Censors erased the content of the Hong Kong rallies, including the public apology of Hong Kong Chief Executive Carrie Lam regarding her handling of the extradition law. The Chinese Firewall also banned less obvious content. For example, QQ, one of the PRC's most popular music streaming sites, removed the song "Can You Hear the People Sing" from the musical *Les Misérables* likely because it invoked the protesters' spirit.[131]

Effect of Information Control

The information gap between the publicized information and reality sometimes generates confusion on Chinese social media. For example, users were puzzled about why Hong Kong's stock market suddenly rose following the news about the extradition bill's withdrawal which was suppressed on the mainland. Users wondered why the government would cave to a radical fringe after observing weeks of coverage of violent protests.[132] The CPC disinformation campaign, as well as pushing the movement into

[131] Robyn Dixon, "The 'Great Firewall': China Censors Videos, Social Media Posts of Hong Kong Protests," *Los Angeles Times*, June 18, 2019, https://www.latimes.com/world/la-fg-china-hong-kong-censorship-20190618-story.html.

[132] Shibani Mahtani, Gerry Shih, and Tiffany Liang, "With Threats and Propaganda, China Tries to Silence Support for Hong Kong Protests," *The Washington Post*, September 6, 2019, https://www.washingtonpost.com/world/asia_pacific/with-

violence, effectively marginalized the movement. It narrowed the target and emphasized the hardcore protesters, who can be portrayed as radicals, thus tarring the whole movement.[133] Finally, this characterization justified police violence in ending the protests.

Coronavirus Disease (COVID-19) 2020

In December 2019, officials in Wuhan, China, confirmed the infection of dozens of people with a pneumonia-like illness. The disease was identified as a new type of coronavirus called novel coronavirus, later renamed COVID-19. While international reporting indicated that officials in Wuhan delayed initial reports of the virus, much credit is given to whistleblowers within Wuhan to inform the world of the severity. Li Wenliang, an ophthalmologist, took to social media to warn about Wuhan's strange new viral outbreak.[134] His actions resulted in information about the virus spreading much faster than official channels. The initial government response was to admonish him for spreading lies and threatening public order. However, as the virus spread, he was recognized as a hero. He ultimately died of COVID-19 on February 7, 2020, sparking further interest and recognition for what was happening within Wuhan despite the censorship of official information.[135]

---

threats-and-propaganda-china-tries-to-silence-support-for-hong-kong-protests/2019/09/06/72ab704c-cfb0-11e9-a620-0a91656d7db6_story.html.

[133] Rose, "How China Is Winning the Hong Kong Propaganda War."

[134] Zhong et al., "No 'Negative' News."

[135] Ibid.

Coordinated Information Response

The CPC immediately began censorship of COVID-19 related information. On December 31, 2019, when the Wuhan Municipal Health Commission issued its first public notice on the disease, research out of the University of Toronto identified keywords like "武汉不明肺炎" (Unknown Wuhan Pneumonia) and "武汉海鲜市场" (Wuhan Seafood Market) were already being censored.[136] However, the information response soon turned to chaos, mostly following Li Wenliang's death due to his notoriety across mainland China. Recently exposed confidential directives immediately following his death demonstrated the concern and desperation for the CPC to control information. One directive sent to local propaganda workers and news outlets stated, "do not use push notifications, do not post commentary, do not stir up speculation. Safely control the fervor in online discussions, do not create hashtags, gradually remove from trending topics, strictly control harmful information."[137]

International and Domestic Response

Throughout 2020, *The New York Times* and ProPublica, a nonprofit investigative newsroom, reportedly reviewed thousands of documents concluding that Chinese officials controlled information to prevent panic and correct falsehood. They also sought to make the virus look less severe and highlight the authorities' proficiency to maintain

---

[136] Ruan, Knockel, and Crete-Nishihata, *Censored Contagion*.

[137] Zhong et al., "No 'Negative' News."

its international image.[138] The Chinese COVID -19 information response also included an extensive international campaign to spread disinformation globally, mainly focused on the virus's origins. This strategy included the extensive use of western social media platforms to ensure they were reaching a global audience.[139] While the PRC did aim to divert blame for the virus, its principle aim with information control was to protect its international reputation.

Deliberate or Unexpected Event

Despite being the epicenter of COVID-19, the PRC was well-placed to combat the disease. It has a centralized epidemic response system, and most Chinese adults remember the 2003 outbreak of Severe Acute Respiratory Syndrome (SARS) and the impact on society.[140] However, there was unexpected international pressure that resulted from the aggressive spread of COVID-19. This caused confusion for the CPC within the information environment. Since the CPC was never able to effectively control the narrative or spread of information it led the CPC to publicize conspiratorial narratives to diminish criticism of its initial failure to contain COVID-19.

---

[138] Zhong et al., "No 'Negative' News."

[139] Jessica Brandt and Bret Schafer, "Five Things to Know about Beijing's Disinformation Approach," Alliance For Securing Democracy, June 24, 2020, https://securingdemocracy.gmfus.org/five-things-to-know-about-beijings-disinformation-approach/.

[140] Talha Burki, "China's Successful Control of Covid-19," *The Lancet. Infectious Diseases* 20, no.11 (November 2020): 1240-1241, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7544475/.

Type of Information Controlled

Chinese censors considered controlling COVID-19 information an "unprecedented challenge."[141] The CAC controlled the information strategy beginning with ordering the publication of only government published material. As the virus spread, the directives transitioned to controlling the narrative focusing on promoting heroic efforts and instructing "that "negative" news about the virus was not promoted."[142] CAC officers also focused on removing content regardless of the medium that indicated any unrest or chaos.

When Li Wenliang's death hit a nerve with the population, CAC recognized that it would be counterproductive to continue extreme censorship with the population and instead permitted postings focused on grief and concern. Still, even these were limited, ultimately deeming a video of grief from Li Wenliang's mother as "taking advantage of this incident to stir up public opinion."[143] Finally, the local CAC offices began keeping scorecards, evaluating different platforms and media sources on how well they aligned their content with the CPC agenda.[144] This formal structure directly encouraged alignment with pro-government messaging in the same way linking social credit scores with social media influences personal discord.

---

[141] Zhong et al., "No 'Negative' News."

[142] Ibid.

[143] Ibid.

[144] Ibid.

Effect of Information Control

Research indicates that the domestic population began questioning Wuhan's

official story (particularly after the lockdown on January 23, 2020). One result of the

confusion was an increase in circumventing information control. Examples of tools used

to circumvent the firewall included the increased VPN downloads, account creation on

western social media platforms (most blocked since 2009), and Chinese language

Wikipedia (blocked since 2015) access.[145] For example, immediately following the

Wuhan lockdown, Twitter experienced a 10 percent increase in accounts active from

within the PRC as well as Chinese language accounts geo-locating to the PRC increased

1.4-fold.[146] In addition to the increase in accounts which can also be attributed to the

increasing spread of government officials on western social media, there was a

disproportionate increase in followers from mainland China of blocked Chinese language

news organizations and exiled dissidents.[147]

Comparative Analysis

The analysis of Tiananmen Square in 1989, Hong Kong Protests in 2019, and

COVID-19 Response in 2020 demonstrates that the CPC's ultimate motivation for

manipulating information is to enforce and embolden strong CPC support and encourage

---

[145] Keng-Chi Chang, William R. Hobbs, Margaret E. Roberts, and Zachary C. Steinert-Threlkeld, "Covid-19 Increased Censorship Circumvention and Access to Sensitive Topics in China," *Proceedings of the National Academy of Sciences* 119, no. 4 (2022).

[146] Ibid.

[147] Ibid.

consensus within the domestic population. Table 1 summarizes the findings of the

analysis.

Table 1.   Summary of Event Analysis

Event	Coordinated Information Response	International Narrative	Domestic Narratives	Deliberate/ Unexpected	Types of Control	Effect
Tiananmen Square Incident of 1989	Yes	Open Economy	Importance of maintaining public order	Deliberate	Media, Foreign Journalists, Detainment, Keywords	Erasing the event from history
Hong Kong Protests of 2019	Yes	Disinformation	Complete suppression transitioned to messaging disinformation	Deliberate	Media, Internet, Keywords, Music	Confusion as to the truth
Covid-19 Response of 2020	Yes	Disinformation	Importance of maintaining public order and Chinese competency	Unexpected	Media, Internet, Keywords	Attempts to circumvent information control

Source: Created by author.

The censorship response to crises does create opportunities that the U.S. military

can exploit. The first vulnerability results from the censorship of terms to restrict

conversation. These restrictions lead to over-censorship (for example, censoring the word

"tomorrow" on social media leading up to the anniversary of the Tiananmen Square

incident). The censoring of common words calls attention to the concern leading citizens

to question the reason. Ultimately, this action could increase interest and awareness of the

event. Second, since the Chinese population is very aware of the government's

censorship and information control, especially online, people create alternative language

or nicknames to discuss controversial events and people. The ability to effectively

penetrate the Chinese information dimension relies on an accurate understanding of

alternative terms. Third, there is an opportunity to exploit the information gap and confusion that results from the suppression of information. This gap emerges when the CPC fails to make a holistic narrative to explain events; for example, there is confusion when the story does not align with reality, such as Hong Kong's stock prices.

Finally, as observed in the immediate aftermath of COVID-19, there is a significant increase in media and news consumption during crisis situations.[148] The increased awareness of the Chinese domestic population results in the need and desire to circumvent CPC information control mechanisms. Therefore, a response strategy must include opportunities to circumvent information controls and drive those seeking information to reputable information.

Since crisis motivates people to track news closely, and in the PRC, this increased engagement outside sources, what might start as seeking one type of information could expose additional censored information not necessarily directly related to the crisis.[149] Contrary to CPC's goals, Chinese citizens' actions following a crisis reveal that what effectively works for information control during normal times is a vulnerability during a crisis. The analysis supports that CPC does censorship provides vulnerabilities to influence that population in times of crisis. Consequently, the U.S. military needs to identify strategies to penetrate the extensive Chinese information control effectively.

---

[148] Chang et al., "Covid-19 Increased Censorship Circumvention and Access to Sensitive Topics in China."

[149] Ibid.

FAS Analysis

The military and U.S. Army need to exploit the vulnerabilities that arise from censorship in the information dimension to prepare for conflict or opportunity. The military strategies must support the overarching political and economic strategies to counter CPC censorship, such as strategies supporting internet freedom worldwide, restricting extradition treaties to the PRC, and economic restrictions to ensure a synchronized whole of government approach. The insights gained from event evaluation contributed to the development of three strategies with different levels of escalation for the U.S. Army to target CPC information control. The purpose of the strategies is to promote knowledge and potentially resistance within the domestic Chinese population against objectives counter to the United States' objectives and simultaneously increase the legitimacy and familiarity with U.S. narratives.

It was important to identify strategies capable of meeting FAS criteria during strategy development. The goal was the creation of strategies nested with the current Indo-Pacific Strategy and supportive of the U.S. Army's mission. The Indo-Pacific Strategy highlights five objectives: "advance a free and open Indo-Pacific, build connections within and beyond the region, drive regional prosperity, bolster Indo-Pacific security, and build regional resilience to transnational threats."[150] These objectives set the foundation for strategy development coupled with DoD's capabilities and the U.S. Army's mission.

---

[150] U.S. President, *Indo Pacific Strategy of the United States* (Washington, DC: The White House, February 2022, 7, https://www.whitehouse.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf.

"Elements of Information Attack" in Edward Waltz's *Information Warfare Principles and Operations* inspired the descriptions of the information strategies. He describes direct attacks as ones that "specifically engage the target's internal information seeking to manipulate, control, and event destroy the information or the infrastructure of the target."[151] As opposed to indirect attacks which "focus on influencing perception by providing information to the target without engaging the information infrastructure of the target."[152] Whether the strategy is active or passive is dependent on the strategy's invasiveness. The active strategy invades the CPC information the while passive is noninvasive and relies on the flow of information.[153]

The first strategy is a passive indirect strategy which is a focus on information creation and transparency. The systematic creation of information will support the proliferation of U.S. Army narratives. An increase in the amount of Chinese language information available that supports the U.S. Army narrative will enable stronger influence. Although this information might not immediately penetrate Chinese borders, it will influence the Chinese diaspora population and be available should the Chinese population circumvent information controls. A focus on information transparency also encourages the open and free society consistent with the values of the United States. The second strategy is an active indirect strategy focusing on information exposure and initiating turbulence and distraction within their system. Finally, the third strategy is an

---

[151] Edward Waltz, *Information Warfare Principles and Operations* (Boston, MA: Artech House, 1998), 168.

[152] Ibid., 165.

[153] Ibid., 252.

57

active direct strategy seeking to penetrate and disrupt the effectiveness of CPC information control. For example, this strategy would include making VPNs available within application stores, reducing the number of censored websites, and pushing specific trending topics.

Strategy One: Creation and Transparency (Passive/Indirect)

Feasibility

1. Are there financial means to accomplish this strategy?

Yes. The U.S. Army has the financial resources necessary to complete this strategy. The highest cost is ensuring effective language translation. In fact, the Fiscal Year (FY) 2022 National Defense Authorization Act (NDAA) authorizes funds to support "A plan for more effectively fulfilling the intelligence and information requirements of the combatant commands."[154] This strategy is an element of enabling combatant commands to compete in the information dimension.

2. Does the technology exist to accomplish this strategy?

Yes. Strategy one does not require any special or unique technology.

3. Are there personnel qualified to accomplish this strategy?

---

[154] National Defense Authorization Act for Fiscal Year 2022, S. Res. 2792, 117th Cong., (September 21, 2021), Report (to Accompany S. 2792) on to Authorize Appropriations for Fiscal Year 2022 for Military Activities of the Department of Defense, for Military Construction, and for Defense Activities of the Department of Energy, to Prescribe Military Personnel Strengths for Such Fiscal Year, and for Other Purposes. 2021, 546, https://www.congress.gov/bill/117th-congress/senate-bill/2792.

Yes. This strategy will require data analysts, linguists, and public affairs. All of these specialties already exist within the U.S. Army. The requirement would be either additional or realignment of resources.

Acceptability

1. Is the strategy acceptable to the people of the United States?

Yes. This strategy aligns with the national values and would be acceptable to the American people. In the 2021 *Interim National Security Strategic Guidance*, President Joseph Biden articulated a vision with the intent to "prevail in strategic competition with China or any other nation."[155] A part of this vision included "standing up for our values abroad."[156] This strategy is consistent with this agenda.

2. Is the strategy acceptable to U.S. allies?

Yes. This strategy aligns consistently with international norms through the concerted effort of sharing information. The 2021 *Interim National Security Strategic Guidance* highlighted the importance of collaborating with democracies and allies around the globe, especially in contrast to the threat of authoritarian states.[157]

Suitability

1. Will the strategy target vulnerabilities in CPC's information control strategy?

---

[155] U.S. President, *Interim National Security Strategy Guidance of the United States of America* (Washington, DC: The White House, March 2021), https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

[156] Ibid.

[157] Ibid.

Yes. This strategy exploits the vulnerabilities identified in the CPC information control strategy. Chinese citizens have exposure to more comprehensive information through a concerted effort to circumvent information control or social interactions. The circumvention is critical because while the Chinese population might be limited to specific social media platforms, their family members who live outside of the PRC are also on those social media platforms and more globally recognized platforms with additional information.

2. Will the strategy advance U.S. national interests?

Yes. The strategy will advance U.S. national interests through exposure to information. When Chinese citizens successfully circumvent information controls, there needs to be information available to support the decision and opinion making. Information sharing is consistently cited in strategic guidance in order to advance national interests.[158]

3. Will the strategy provide an advantage for the U.S. military?

Yes. This strategy provides an advantage for the U.S. military because if there is a transition to conflict, information consistent with U.S. military strategy is already staged within the information environment. This strategy is consistent with inoculation theory which contends the best way to establish a resistance to persuasive influence is through

---

[158] U.S. President, *Interim National Security Strategy Guidance of the United States of America.*

the preemptive exposure to ideas.[159] When the Chinese information strategy transitions to

disinformation, citizens will already be exposed to other ideas.

4. Is the strategy compatible with international norms?

Yes. There will be no concern from the international community regarding

increasing transparency and information. Freedom of expression is cited as a fundamental

human right in Article 19 of the Universal Declaration of Human Rights.[160]

<div align="center">

Strategy Two: Exposure and Initiating Turbulence and
Distraction within their System (Active/Indirect)

</div>

<u>Feasibility</u>

1. Are there financial means to accomplish this strategy?

Yes. If appropriately prioritized, this strategy can be financed through the FY2022

NDAA. The cost is minimal, requiring only specific intelligence requirements and

information sharing.

2. Does the technology exist to accomplish this strategy?

Yes. There is no unique technology required to accomplish this strategy. In fact,

in response to the 2022 Russian invasion of Ukraine, there have been information

exposures similar to those recommended in this strategy.[161] The United States

---

[159] Josh Compton, Ben Jackson, and James A. Dimmock, "Persuading Others to Avoid Persuasion: Inoculation Theory and Resistant Health Attitudes," *Frontiers in Psychology* 7 (2016): 122, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4746429/.

[160] "Universal Declaration of Human Rights," United Nations, 2017, https://www.un.org/en/about-us/universal-declaration-of-human-rights.

[161] Greg Myre, "As Russia Threatens Ukraine, the U.S. 'Pre-Bunks' Russian Propaganda," *NPR*, February 8, 2022, https://www.npr.org/2022/02/08/1079213726/as-russia-threatens-ukraine-the-u-s-pre-bunks-russian-propaganda.

preemptively publicized the Russian information strategy. Nina Jankowicz, author of

How To Lose the Information War: Russia, Fake News, and the Future of Conflict,

described the government strategy as *prebunking*, "Rather than debunking, the (U.S. and

British) governments are getting ahead of a potential Russian narrative and attempting to

pre-bunk it with this intelligence that they've been declassifying."[162] If the United States

were to obfuscate how this information was collected, it could further exacerbate concern

within the target country about how the information is being collected.

    3.   Are there personnel qualified to accomplish this strategy?

    Yes. The most complicated aspect of this strategy is aligning the narrative

holistically and understanding the second and third-order effects of releasing information.

Acceptability

    1.   Is the strategy acceptable to the people of the United States?

    Yes. There has been a positive response to the exposure of information regarding

the information strategy for the Russian invasion of Ukraine. Additional transparency of

information is consistent with overarching American values. Additionally, deception is an

accepted element of warfare. The DoD defined deception as: "Military deception

(MILDEC) is actions executed to deliberately mislead adversary military, paramilitary, or

violent extremist organization decision-makers, thereby causing the adversary to take

specific actions (or inactions) that will contribute to the accomplishment of the friendly

---

[162] Myre, "As Russia Threatens Ukraine, the U.S. 'Pre-Bunks' Russian Propaganda."

mission."[163] The inclusion of the concept in doctrine demonstrates the acceptability of the practice.

2. Is the strategy acceptable to U.S. allies?

Yes. In 2021, United States Agency for International Development (USAID) published a report titled *How Information Disorder Affirms Authoritarianism and Destabilizes Democracy*. This report concluded that the PRC is the key actor manipulating information across Asia and the Pacific region.[164] Any effort to increase transparency and information flow is likely to be supported.

Suitability

1. Will the strategy target vulnerabilities in The PRC's information strategy?

Yes. A critical vulnerability in Chinese information control is the societal understanding that suppression of information is key to the government's success. As Chinese citizens identify and then share counter-narratives, there will be an effort to seek out additional information.

2. Will the strategy advance U.S. national interests?

---

[163] Chairman of the Joint Chiefs of Staff (CJCS), Joint Publication (JP) 3-13.4, *Military Deception* (Washington, DC: Joint Chiefs of Staff, January 26, 2012), vii, https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf.

[164] "How Information Disorder Affirms Authoritarianism and Destabilizes Democracy," United States Agency for International Development, December 2021, https://pdf.usaid.gov/pdf_docs/PA00Z3JC.pdf.

Yes. President Biden identified Chinese increasing assertiveness as a threat to U.S. national interests. The CPC's ability to control information is counter to the foundation of democratic values of the American way of life.

3. Will the strategy provide an advantage for the U.S. military?

Yes. The deception campaign will support military strategy by influencing the enemy's decision cycle. Ultimately, the success or failure of forces on the battlefield comes down to these individual decisions that are highly reliant on command decisions. Therefore, understanding the influence of individual cognitive processes is essential to successfully gaining an advantage with the information available. Deception operations target inherent cognitive processes as well as exploit cognitive biases. The United States can successfully disrupt the Chinese decision cycle by exposing information and implying an internal threat.

4. Is the strategy compatible with international norms?

No. Although it is acceptable to incorporate deception into military actions, U.S. Army deception operations expect that they take place in the environment of armed conflict. Therefore, the deception strategy is not acceptable until military activities progress within the range of armed conflict. Additionally, there are other proponents of the U.S. Government that are more equipped to effectively complete this strategy that the U.S. Army.

Strategy Three: Penetration and Disruption (Active/Direct)

Feasibility

1. Are there financial means to accomplish this strategy?

Yes. There is funding included in the FY2022 funding to support the research and development of technological advancements.

2. Does the technology exist to accomplish this strategy?

Yes. There are opportunities to circumvent information controls observed during the COVID-19 response.

3. Are there personnel qualified to accomplish this strategy?

Yes. The DoD has prioritized troop modernization, including special technical skills.

Acceptability

1. Is the strategy acceptable to the people of the United States?

No. In the current environment, violation of another country's sovereignty is not acceptable. However, this strategy's acceptability is limited to conflict. Offensive cyber operations could likely escalate, and the CPC would see any infiltration as a threat to its internet sovereignty.

2. Is the strategy acceptable to U.S. allies?

No. The strategy is likely to be seen as a violation of sovereignty. However, there is a changing perception of offensive cyber operations, especially during conflict. In June 2021, NATO created a new Comprehensive Cyber Defence Policy including a more prominent role of offensive cyber operations agreeing to "employ the full range of

capabilities to deter actively, defend against, and counter the full spectrum of cyber threats."[165]

Suitability

 1. Will the strategy target vulnerabilities in the PRC's information strategy?

 Yes. The infiltration would enable Chinese citizens to circumvent information controls and introduce narratives supporting friendly forces. During the Russian invasion of Ukraine the changes in Russian civilian internet usage demonstrated the effectiveness of this strategy for example, one company reported a 3500% increase in Russians getting VPNs coinciding with when the Russian government began censoring media and social media platforms.[166]

 2. Will the strategy advance U.S. national interests?

 Yes. This strategy would advance U.S. national interests in competition through the exposure of information. It would also force the Chinese government to focus on internal narratives to its population rather than projecting power.

 3. Will the strategy provide an advantage for the U.S. military?

 Yes. The strategy's increased information flow benefits the U.S. military as the PLA would be required to focus on internal control over power projection.

---

 [165] Erica D. Lonergan and Mark Montgomery, "Pressing Questions: Offensive Cyber Operations and NATO Strategy," Modern War Institute, January 25, 2022, https://mwi.usma.edu/pressing-questions-offensive-cyber-operations-and-nato-strategy/.

 [166] John Koetsier, "Russia Forcing Google to Delist VPN Websites, but 400,000+ Russians Are Downloading VPNs Daily," *Forbes*, March 23, 2022, https://www.forbes.com/sites/johnkoetsier/2022/03/21/russia-forcing-google-to-delist-vpn-websites-but-400000-russians-are-downloading-vpns-daily/?sh=b5d5393448ae.

4. Is the strategy compatible with international norms?

No. The strategy is incompatible with the acceptable international norms below armed conflict. According to *The Tallinn Manual*, a tool for policy and legal experts on how international law applies to cyber operations, "Any interference by a State with cyber infrastructure aboard a platform, wherever located, that enjoys sovereign immunity constitutes a violation of sovereignty."[167] However, if the United States established that the offensive cyber operations are in response to a breach of international law, the breach is attributable to the PRC. Establishing an attributable crime would support the escalation to make this strategy valid.

Comparative Analysis

As summarized in Table 2 below, only one proposed strategy is feasible within the FAS framework in today's operating environment with the PRC. The invalidity arises from two strategies not being suitable or acceptable across all aspects of the competition continuum. In 2019, Joint Doctrine Note 1-19, *Competition Continuum,* introduced the idea of competition continuum, stating, "Rather than a world either at peace or at war, the competition continuum describes a world of enduring competition conducted through a mixture of cooperation, competition below armed conflict, and armed conflict."[168]

---

[167] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Operations* (Cambridge, UK: Cambridge University Press, 2013), 23.

[168] CJCS, JDN 1-19, 2.

Table 2.   FAS Analysis

Strategic Information Approach	Validity		
	Feasibility	Acceptability	Suitability
Creation and Transparency (Passive/ Indirect)	Valid	Valid	Valid
Exposure and Initiating turbulence and distraction within their system (Active/ Indirect)	Valid	Valid (Competition Below Threshold of Armed Conflict)	Invalid (Armed Conflict)
Penetration and Disruption (Active/ Direct)	Valid	Invalid (Armed Conflict)	Invalid (Armed Conflict)

Source: Created by author.

When evaluating the strategies' validity, it was clear that the distinction between interactions with the PRC must be included in the conclusion. Although the doctrine is clear that military forces are never solely in a specific phase of the continuum but instead campaigns through a mixture of cooperation, competition below armed conflict, and armed conflict to achieve the desired strategic objectives.[169] The strategies' suitability depends on the level of the campaign because of the consequences of escalation. Only on strategy is valid because the current state between the United States and the CPC remains below the threshold of armed conflict.

---

[169] CJCS, JDN 1-19, 5.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

This study served to identify ways for the U.S. Army to penetrate denied areas in a CPC controlled information environment. The CPC takes full advantage of today's technology and innovation to implement its vision for information control. This employment ranges from media control to industry censorship and ultimately individual self-regulation. One of the most influential end states of technological information control is the links between digital life and everyday activity through a social credit account. The linkage of a social credit account and a social media profile results in the credit company and government's permanent and pervasive access to the user's entire digital life enabling its influence and ultimately changes in personal activities. The understanding that a user's associations can influence their social credit score leads to self-regulation and network regulation. Individuals are inclined to disassociate from controversial people regardless of their relationship and demonstrate government loyalty. As the people in a user's network increase their vocal support of the government, others are likely to follow, creating a holistically more harmonious society.

The focus of the Chinese on information control means that when competing in the information dimension, the U.S. military must understand and consider the Chinese population's perspective for interacting and understanding information and its influence over personal action. The 2022 U.S. *Indo-Pacific Strategy* stated the first objective is to "advance a free and open Indo-Pacific."[170] Encompassed in this objective is that the

---

[170] U.S. President, *Indo Pacific Strategy of the United States,* 7.

United States will "bolster freedom of information and expression and combat foreign interference by supporting investigative journalism, promoting media literacy and pluralistic and independent media, and increasing collaboration to address threats from information manipulation."[171] The ability to penetrate CPC information control is consistent and supportive of this objective of the Indo-Pacific Strategy.

The primary research question driving the study was how can the U.S. Army exploit vulnerabilities in the Chinese approach to the information environment for an asymmetric advantage? The answer is through a targeted information strategy that exploits the gaps created through information control. The vulnerabilities this study identified are over censorship, the pursuit of clarifying information, and desynchronized narratives. Therefore, the strategy cannot be limited to one course of action and must account for the contested information environment. Although any narrative development is specific to event considerations, the U.S. Army can prepare to implement escalation strategies to ensure the exploitation of these vulnerabilities during an event. This chapter further discusses these strategies later.

A secondary research question was how does the CPC control information domestically and internationally? Domestically, the CPC focuses most efforts on controlling the digital information dimension. The CPC accomplishes must of its information control with restrictions implemented through The Golden Shield Project. However, censorship is not limited to government control; society also encourages self-censorship, as demonstrated in self-regulation, and can manifest with companies

---

[171] U.S. President, *Indo Pacific Strategy of the United States,* 8.

imposing information control to receive favorable government action. This study reveals the primary reason for CPC information control is for preservation and to ensure the CPC's influence and social stability. The secondary reason is the desire to extend influence outside the PRC's borders. There is potential for increased Chinese influence in other countries through an increase in their economic power and influence. The influence is consistent with the stated goal to achieve "the great rejuvenation of the Chinese nation" by 2049.[172]

Another secondary research question asked in this study was how do Chinese information TTPs change when challenged? Changing TTPs were evaluated through the event selection; each event represented a different level of contention in the information environment. The amount of pressure and penetration in the information dimensions changed drastically in the three events. The result is that the preferred course of action for the CPC is the complete removal of any unfavorable information. When that tactic becomes unsustainable, either through time or publicity, there is a shift to a disinformation campaign. However, focused censorship does not lessen due to the new disinformation campaign. The purpose of that campaign is to explain discrepancies or to protect the CPC's reputation.

The third and final secondary research question was how does the United States' approach to information operations contrast with the Chinese approach? The primary differentiation between the U.S. and Chinese perspectives is how the U.S. interprets censorship, which is usually in a very critical manner, as Americans tend to view

---

[172] SecDef, *Military and Security Developments Involving the People's Republic of China*.

information control as antithetical to national values of democracy and freedom. Another

significant influence is how censorship impacts Chinese activism. As was seen prior to

the Tiananmen Square incident, there was a history of large scale in person activism.

Today, this activism in the PRC has moved online and in a more passive manner to

operate within the restricted CPC guidelines.

<div align="center">Strategy to Exploit Chinese Information Control</div>

The recommended strategy for countering Chinese information control is a range

of responses to enable escalation and de-escalation consistent with the intensity of the

conflict or competition. Strategy one, information creation and transparency, is the least

intrusive and recommended outside of armed conflict. Strategy one is an increased

production and publication of information consistent with the U.S. military's narrative

with the PRC. This strategy requires interagency support, ensuring a consistent narrative

across the U.S. Government, particularly synchronized with the Global Engagement

Center within the U.S. Department of State. This strategy is contingent on Chinese

language production and identifying amplifying mediums to push information. The result

of strategy one is transparency and informing the Chinese diaspora for the intended

purpose of organic information sharing between people. This information flow should

reduce the support for CPC's narratives and enable acceptance for external narratives.

Strategy two, exposure and initiating turbulence and distraction within their

system, is a slight escalation that should be utilized regarding a specific incident or event;

however, the U.S. Army is not the appropriate organization to carry out this strategy. The

strategy intends to expose information to publicize the CPC information strategy. This

information might include intelligence demonstrating how information is being withheld

from the Chinese people and pre-bunking any misinformation and disinformation campaigns. Preemptive information dissemination will inoculate the public against information forthcoming from the CPC. A secondary purpose would be to release the information in a manner that implies it results from an espionage agent within the CPC. Any chaos will force the CPC to focus efforts on internal control rather than external influence. This strategy should be integrated into a whole of government approach, and not simply a U.S. Army responsibility.

Strategy three, penetration and disruption of The Golden Shield Project, is a significant escalation and only acceptable in times of war. The intent behind any intrusion would be to reduce the effectiveness of the Chinese Firewall. One possible avenue of infiltration is increasing VPN availability. Circumvention capability allows access to censored content and enables opportunities and exposure to additional information for the domestic Chinese population. Another method would be to change search restrictions allowing access and searches for typically censored information. Circumvention techniques would be particularly effective when censorship increases interest in an event, as observed during the COVID-19 response.

All three strategies exploit the phenomenon that people want access to information and desire to know the truth. The pursuit of information is particularly true of a society that understands its information is being controlled and censored. CPC's censorship creates vulnerabilities through over censorship and spotlighting events. However, the opportunities that arise from the vulnerabilities are time sensitive, resulting in the high importance of having prepared methods of response in preparation for an

opportunity to compete in the information dimension. Enabling the United States to remain proactive rather than reactive.

To implement a strategy that successfully counters CPC's information control, the U.S. Army needs to ensure that information operations are fully integrated into the campaign and operational plans. As the ideas of information advantage proliferate, U.S. Army commanders need to recognize the intricacies accompanying any decision. When competing with the PRC to gain the information advantage, U.S. Army forces must operate within the established Chinese information environment. Without understanding, CPC's information control operations will not be effective in the Chinese information environment.

Areas for Future Study

To create a complete and detailed strategy to counter CPC's information control in the information dimension, there is a need for additional research. Areas of future study would include a technical evaluation of the tools the CPC's uses to conduct its censorship analysis and information control. Also, to fully understand the influence of any information strategy targeting the Chinese population, it is necessary to study further the cultural changes and effects of information control has had on Chinese society over the last 30 years. Finally, strategy implementation would benefit from an assessment of escalatory thresholds, especially within the information dimension, which would enable more effective and creative implementation of this strategy. The United States needs to understand the thresholds for escalation from a Chinese perspective for realistic employment.

Although it is impossible to explore every aspect of CPC's censorship, this thesis presented a few vulnerabilities the U.S. Army can exploit when competing in the information dimension. During the 2022 invasion of Ukraine, the effectiveness of Ukraine and the United States' ability to counter Russia in the information dimension highlighted the value that stems from competing in this space. A government's total information control does not prevent opportunities for penetration and can instead be exploited to expand the influence of the U.S. Army. This thesis sets conditions for further research to improve the U.S. Army's interpretations and influence on the Chinese domestic population.

BIBLIOGRAPHY

Amnesty International UK. "1989 Tiananmen Square Protests." January 5, 2022. https://www.amnesty.org.uk/china-1989-tiananmen-square-protests-demonstration-massacre.

Anderson, Eric, and Jeffrey Engstrom. "China's Use of Perception Management and Strategic Deception." Science Applications International Corporation, Reston, VA, November 2009. https://www.uscc.gov/sites/default/files/Research/ApprovedFINALSAICStrategicDeceptionPaperRevisedDraft06Nov2009.pdf.

The Associated Press. "Hong Kong University Removes Tiananmen Massacre Statue." *NPR*. December 23, 2021. https://www.npr.org/2021/12/23/1067163101/hong-kong-university-removes-tiananmen-massacre-statue.

Barme, Geremie R., and Sang Ye. "The Great Firewall of China." *Wired*. June 1, 1997. https://www.wired.com/1997/06/china-3/.

BBC. "Social Media And Censorship In China: How Is It Different To The West?" *BBC News*. September 26, 2017. http://www.bbc.co.uk/newsbeat/article/41398423/social-media-and-censorship-in-china-how-is-it-different-to-the-west.

Blumenthal, Dan, and Linda Zhang. "China's Censorship, Propaganda & Disinformation." American Enterprise Institute. July 10, 2020. https://www.aei.org/articles/chinas-censorship-propaganda-disinformation/.

Brandt, Jessica, and Bret Schafer. "Five Things to Know about Beijing's Disinformation Approach." Alliance for Securing Democracy. June 24, 2020. https://securingdemocracy.gmfus.org/five-things-to-know-about-beijings-disinformation-approach/.

Burke, Edmund J., Kristen Gunness, Cortez A. Cooper III, and Mark Cozad. *People's Liberation Army Operational Concepts*. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RRA394-1.html.

Burki, Talha. "China's Successful Control of Covid-19." *The Lancet Infectious Diseases* 20, no. 11 (November 2020):1240-1241. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7544475/.

Chairman of the Joint Chiefs of Staff. Joint Doctrine Note 1-19*, Competition Continuum.* Washington, DC: Joint Chiefs of Staff, June 3, 2019. https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf.

———. Joint Publication 3-13*, Information Operations.* Washington, DC: Joint Chiefs of Staff, November 27, 2012. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

———. Joint Publication 3-13.4, *Military Deception.* Joint Washington, DC: Chiefs of Staff, January 26, 2012. https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/ Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf.

Chandel, Sonali, Zang Jingji, Yu Yunnan, and Sun Jingyao. "The Golden Shield Project of China: A Decade Later—An In-Depth Study of the Great Firewall." *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC).* Guilin, China, 2019, 111-119. https://www.computer.org/csdl/proceedings-article/cyberc/2019/254200a111/ 1gjS1msFzmE.

Chang, Keng-Chi, William R. Hobbs, Margaret E. Roberts, and Zachary C. Steinert-Threlkeld. "Covid-19 Increased Censorship Circumvention and Access to Sensitive Topics in China." *Proceedings of the National Academy of Sciences* 119, no. 4 (2022).

Cheung, Alvin Y.H. "Can We Finally Admit That 'One Country, Two Systems' Is Dead in Hong Kong?" Just Security. April 30, 2020. https://www.justsecurity.org/ 69936/can-we-finally-admit-that-one-country-two-systems-is-dead-in-hong-kong/.

Chodkowski, William M. "The United States Information Agency." Fact Sheet, American Security Project, Washington, DC, November 2012. https://www.scribd.com/document/112346692/Fact-Sheet-The-United-States-Information-Agency.

Citizen Lab and Weiboscope HKU. "China's Censored Histories: Commemorating the 30th Anniversary of the Tiananmen Square Massacre." *Global Voices.* April 17, 2019. https://globalvoices.org/2019/04/17/chinas-censored-histories-commemorating-the-30th-anniversary-of-the-tiananmen-square-massacre/.

Compton, Josh, Ben Jackson, and James A. Dimmock. "Persuading Others to Avoid Persuasion: Inoculation Theory and Resistant Health Attitudes." *Frontiers in Psychology* 7 (2016): 122. https://www.ncbi.nlm.nih.gov/pmc/articles/ PMC4746429/.

Congressional-Executive Commission On China. "Agencies Responsible For Censorship In China." Accessed April 19, 2022. https://www.cecc.gov/agencies-responsible-for-censorship-in-china.

———. "Information Control And Self-Censorship In China And The Spread Of SARS." Accessed April 19, 2022. https://www.cecc.gov/publications/issue-papers/ information-control-and-self-censorship-in-the-prc-and-the-spread-of-sars.

The Constitution of the People's Republic of China: The Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China. The Government of the Hong Kong Special Administrative Region of the People's Republic of China. May 2021. https://www.basiclaw.gov.hk/filemanager/content/en/files/basiclawtext/basiclaw_full_text.pdf.

Cook, Sarah. *Beijing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence since 2017.* Special Report. Washington, DC: Freedom House, January 2020. https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone.

———. "The Globalization of China's Media Controls: Key Trends from 2018." *The Diplomat.* November 10, 2020. https://thediplomat.com/2018/12/the-globalization-of-chinas-media-controls-key-trends-from-2018/.

Corneli, Alessandro. "Sun Tzu and the Indirect Strategy." *Rivista Di Studi Politici Internazionali* 54, no. 3 (215) (1987): 419-445. http://www.jstor.org/stable/42738671.

Dixon, Robyn. "The 'Great Firewall': China Censors Videos, Social Media Posts of Hong Kong Protests." *Los Angeles Times.* June 18, 2019. https://www.latimes.com/world/la-fg-china-hong-kong-censorship-20190618-story.html.

Dotson, John. *The Confucian Revival in the Propaganda Narratives of the Chinese Government.* Staff Research Report. Washington, DC: U.S.-China Economic and Security Review Commission, June 20, 2011. https://www.uscc.gov/sites/default/files/Research/Confucian_Revival_Paper.pdf.

Einbinder, Nicole. "China's State-Controlled Media Has Completely Ignored Coverage of Hong Kong Protests." *Business Insider.* July 2, 2019. https://www.businessinsider.com/chinas-state-controlled-media-ignored-coverage-hong-kong-protests-2019-7.

Feng, Coco. "Beijing Updates Ban On Private News Media, Prohibiting Events." *South China Morning Post.* October 9, 2021. https://www.scmp.com/tech/policy/article/3151778/beijing-reiterates-ban-private-capital-news-media-updating-it-prohibit.

Feng, Emily, and Amy Cheng. "China State Media Present Their Own Version of Hong Kong Protests." *NPR.* August 14, 2019. https://www.npr.org/2019/08/14/751039100/china-state-media-present-distorted-version-of-hong-kong-protests.

Gamso, Jonas. "Is China Exporting Media Censorship? China's Rise, Media Freedoms, and Democracy," *European Journal of International Relations* 27, no. 3 (May 22, 2021): 858–883. https://journals-sagepub-com.lumen.cgsccarl.com/doi/10.1177/13540661211015722.

Geron, Tomio. "YY.com: China's Unique Real-Time Voice and Video Service with a Virtual Goods Twist." *Forbes*. June 18, 2012. https://www.forbes.com/sites/tomiogeron/2012/06/11/yy-com-chinas-unique-real-time-voice-and-video-service-with-a-virtual-goods-twist/?sh=13ef684a43d1.

Headquarters, Department of the Army. Army Techniques Publication 7-100.3, *Chinese Tactics*. Washington, DC: Army Publishing Directorate, August 9, 2021. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN33195-ATP_7-100.3-000-WEB-1.pdf.

Hoffman, Chris. "How the 'Great Firewall of China' Works to Censor China's Internet." How-To Geek. Last updated September 10, 2017. https://www.howtogeek.com/162092/htg-explains-how-the-great-firewall-of-china-works/.

Hsu, Jeremy. "The Strava Heat Map Shows Even Militaries Can't Keep Secrets from Social Data." *Wired*. January 29, 2018. https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.

Human Rights Watch. "Human Rights Activism in Post-Tiananmen China." Last modified November 5, 2021. https://www.hrw.org/news/2019/05/30/human-rights-activism-post-tiananmen-china#.

———. "China: Tiananmen Injustice Fuels Repression 30 Years On." October 28, 2020. https://www.hrw.org/news/2019/05/30/china-tiananmen-injustice-fuels-repression-30-years.

———. "Human Rights Activism in Post-Tiananmen China." November 5, 2021. https://www.hrw.org/news/2019/05/30/human-rights-activism-post-tiananmen-china#.

Hunt, Pete. "China's Great Social Credit Leap Forward." *The Diplomat*. December 4, 2018. https://thediplomat.com/2018/12/chinas-great-social-credit-leap-forward.

Jensen, Aaron. "Deception Is Key to Chinese Military Strategies." *The Diplomat*. August 8, 2020. https://thediplomat.com/2020/08/deception-is-key-to-chinese-military-strategies/.

Jiang, Min, and King-Wa Fu. "Chinese Social Media and Big Data: Big Data, Big Brother, Big Profit?" *Policy & Internet* 10, no. 4 (2018): 372–392.

Kastner, Scott L. "Buying Influence? Assessing the Political Effects of China's International Trade." *Journal of Conflict Resolution* 60, no. 6 (2016): 980-1007. https://www-jstor-org.lumen.cgsccarl.com/stable/24755936?seq=1.

Koetsier, John. "Russia Forcing Google to Delist VPN Websites, but 400,000+ Russians Are Downloading VPNs Daily." *Forbes*. March 21, 2022. https://www.forbes.com/sites/johnkoetsier/2022/03/21/russia-forcing-google-to-delist-vpn-websites-but-400000-russians-are-downloading-vpns-daily/?sh=b5d5393448ae.

Kretchun, Nat. *The Need for a New US Information Strategy for North Korea*. Special Report No. 451. Washington, DC: United States Institute of Peace, June 2019. https://www.usip.org/sites/default/files/2019-07/sr_451-the_need_for_a_new_u.s._information_strategy_for_north_korea.pdf.

Kuo, Lily. "Chinese Journalists to Be Tested on Loyalty to Xi Jinping." *The Guardian*., September 20, 2019. https://www.theguardian.com/world/2019/sep/20/chinese-journalists-to-be-tested-on-loyalty-to-xi-jinping.

Latimer, John. *Deception in War*. Woodstock: The Overlook Press, 2001.

Lewis, James. *Sovereignty and the Evolution of Internet Ideology*. Washington, DC: Center for Strategic and International Studies, February 4, 2022. https://www.csis.org/analysis/sovereignty-and-evolution-internet-ideology.

Lonergan, Erica D., and Mark Montgomery. "Pressing Questions: Offensive Cyber Operations and NATO Strategy." Modern War Institute. January 25, 2022. https://mwi.usma.edu/pressing-questions-offensive-cyber-operations-and-nato-strategy/.

Mackinnon, Stephen R. "Toward a History of the Chinese Press in the Republican Period." *Modern China* 23, no. 1 (January 1997): 3–32. https://www-jstor-org.lumen.cgsccarl.com/stable/189462?seq=1.

Mahtani, Shibani, Gerry Shih, and Tiffany Liang. "With Threats and Propaganda, China Tries to Silence Support for Hong Kong Protests." *The Washington Post*. September 6, 2019. https://www.washingtonpost.com/world/asia_pacific/with-threats-and-propaganda-china-tries-to-silence-support-for-hong-kong-protests/2019/09/06/72ab704c-cfb0-11e9-a620-0a91656d7db6_story.html.

Matsakis, Louise. "How the West Got China's Social Credit System Wrong." *Wired*. July 29, 2019. https://www.wired.com/story/china-social-credit-score-system/.

Matthews, Miriam, Katya Migacheva, and Ryan Andrew Brown. *Russia and China: Superspreaders of Malign and Subversive Information on Covid-19*. Santa Monica, CA: RAND Corporation. April 29, 2021. https://www.rand.org/pubs/research_reports/RRA112-11.html.

McCarty, Michael. "The Historical Roots of Chinese Communist Propaganda." *The Pulse*. 2005. https://www.baylor.edu/pulse/index.php?id=33634#1d.

Metcalf, Mark. "Deception Is the Chinese Way of War." *Proceedings* 143, no. 2 (February 2017): 1368. https://www.usni.org/magazines/proceedings/2017/february/deception-chinese-way-war.

Molander, Roger C., Andrew Riddile, and Peter A. Wilson. *Strategic Information Warfare: A New Face of War*. Santa Monica, CA: RAND Corporation. January 1, 1996. https://www.rand.org/pubs/monograph_reports/MR661.html.

Myers, Steven Lee, and Paul Mozur. "China Is Waging a Disinformation War against Hong Kong Protesters." *The New York Times*. August 13, 2019. https://www.nytimes.com/2019/08/13/world/asia/hong-kong-protests-china.html.

Myre, Greg. "As Russia Threatens Ukraine, the U.S. 'Pre-Bunks' Russian Propaganda." *NPR*. February 8, 2022. https://www.npr.org/2022/02/08/1079213726/as-russia-threatens-ukraine-the-u-s-pre-bunks-russian-propaganda.

Nossel, Suzanne. "Chinese Censorship Is Going Global." *Foreign Policy.* October 26, 2021. https://foreignpolicy.com/2021/10/26/chinese-censorship-enes-kanter-celtics-browder-is-going-global/.

Office of the Secretary of Defense. *Military and Security Developments Involving the People's Republic of China: Annual Report to Congress.* Washington, DC: Department of Defense, 2020. https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.

Ota, Fumio. "Sun Tzu in Contemporary Chinese Strategy." *Joint Force Quarterly* 73 (2nd Quarter 2014): 76-80. https://ndupress.ndu.edu/Media/News/Article/577507/sun-tzu-in-contemporary-chinese-strategy/.

Pomerleau, Mark. "US Army Emphasizes 'Information Advantage.'" C4ISRNet. May 25, 2021. https://www.c4isrnet.com/information-warfare/2021/05/25/us-army-emphasizes-information-advantage/.

Purbrick, Martin. "A Report of the 2019 Hong Kong Protests." *Asian Affairs* 50, no. 4 (2019): 465–487. https://www-tandfonline-com.lumen.cgsccarl.com/doi/full/10.1080/03068374.2019.1672397.

Radio Free Asia News and Information. "China Gives Police Powers to Monitor Social Media Friends, Chat Groups." September 27, 2016. https://search.proquest.com/docview/1823988139?accountid=10504.

Reporters Without Borders. "China." Accessed April 19, 2022. https://rsf.org/en/china.

Rose, J. J. "How China Is Winning the Hong Kong Propaganda War." *The Interpreter*. November 19, 2019. https://www.lowyinstitute.org/the-interpreter/how-china-winning-hong-kong-propaganda-war.

Ruan, Lotus, Jeffrey Knockel, and Masashi Crete-Nishihata. *Censored Contagion: How Information on the Coronavirus Is Managed on Chinese Social Media*. Research Report #125. Toronto, Canada: Citizen Lab, The University of Toronto, March 3, 2020. https://citizenlab.ca/2020/03/censored-contagion-how-information-on-the-coronavirus-is-managed-on-chinese-social-media/.

Sarotte, M..E. "China's Fear of Contagion: Tiananmen Square and the Power of the European Example." *International Security* 37, no. 2 (2012): 156–182. https://www-jstor-org.lumen.cgsccarl.com/stable/23280417?seq=1.

Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Operations*. Cambridge, UK: Cambridge University Press, 2013.

Shahbaz, Adrian and Allie Funk. *Freedom on the Net 2021: The Global Drive to Control Big Tech.* Washington, DC: Freedom House, 2021. https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech.

Shambaugh, David. "China's Propaganda System: Institutions, Processes, and Efficacy." *The China Journal* 57 (January 2007): 25–58. https://www-jstor-org.lumen.cgsccarl.com/stable/20066240?seq=1.

Stewart, Emily. "How China Used Facebook, Twitter, and YouTube to Spread Disinformation about the Hong Kong Protests." *Vox*. August 20, 2019. https://www.vox.com/recode/2019/8/20/20813660/china-facebook-twitter-hong-kong-protests-social-media.

Sun Tzu. *The Art of Warfare: The First English Translation Incorporating the Recently Discovered Yin-ch'üeh-shan Texts.* Translated by Roger Ames. New York: Ballantine Books, 1993.

Sun, Wanning. *Media and the Chinese Diaspora: Community, Communications, and Commerce*. New York: Routledge, 2006.

Sun, Wu. *The Art of War: Sun Zi's Military Methods*. New York: Columbia University Press, 2007.

Sunzi, and Thomas F. Cleary. *The Art of War*. Boston, MA: Shambhala, 2005.

The Tank Man. Produced by Antony Thomas. Frontline, Season 2006, Episode 10. *PBS*, April 11, 2006. 1 hr., 24 min. http://www.pbs.org/wgbh/frontline/film/tankman/.

Thomas, Timothy L. *Dragon Bytes: Chinese Information-War Theory and Practice from 1995-2003*. Fort Leavenworth, KS: Foreign Military Studies Office, 2004.

Truitte, Kevin. "An American National Information Security Strategy." *Georgetown Security Studies Review*. March 11, 2019. https://georgetownsecuritystudiesreview.org/2019/03/11/an-american-national-information-security-strategy/.

U.S. Army Command and General Staff College. "C203: Power and Strategy Slides." PowerPoint Presentation, C203: Power and Strategy Briefing, Fort Leavenworth, KS, September 13, 2021.

U.S. Congress. U.S. Information and Educational Exchange Act of 1948. Public Law 402, 80th Cong., 2nd sess. (January 27, 1948). https://www.usagm.gov/who-we-are/oversight/legislation/smith-mundt/.

U.S. Congress. House. USIA for Strategic Competition Act. H. Res. 7938, 116th Cong., (August 4, 2020). https://www.congress.gov/bill/116th-congress/house-bill/7938.

U.S. Congress. Senate. National Defense Authorization Act for Fiscal Year 2022. S. Res. 2792, 117th Cong., (September 21, 2021). Report (to Accompany S. 2792) on to Authorize Appropriations for Fiscal Year 2022 for Military Activities of the Department of Defense, for Military Construction, and for Defense Activities of the Department of Energy, to Prescribe Military Personnel Strengths for Such Fiscal Year, and for Other Purposes. https://www.congress.gov/bill/117th-congress/senate-bill/2792.

U.S. Department of State. "Global Engagement Center: Core Mission & Vision." Accessed January 20, 2022. https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/.

U.S. Embassy Beijing. Cable to Secretary of State, PLA Ready to Strike, May 21, 1989. In National Security Archive Electronic Briefing Book No. 47, *The U.S. "Tiananmen Papers,"* edited by Michael L. Evans, document 8. National Security Archive, June 4, 2001. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB47/.

———. Secretary of State's Morning Summary for June 2, 1989, China: Stalemate Continues, June 2, 1989. In National Security Archive Electronic Briefing Book No. 16, *Tiananmen Square, 1989: The Declassified History,* edited by Jeffrey Richelson and Michael Evans, document 8. National Security Archive, June 1, 1999. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB16/index.html.

United Nations. "Universal Declaration of Human Rights." 2017. https://www.un.org/en/about-us/universal-declaration-of-human-rights.

United States Agency for International Development (USAID). *How Information Disorder Affirms Authoritarianism and Destabilizes Democracy*. Washington, DC: USAID, December 2021. https://pdf.usaid.gov/pdf_docs/PA00Z3JC.pdf.

United States Information Agency. "Mission Statement" Assessed April 19, 2022. https://govinfo.library.unt.edu/npr/library/nprrpt/annrpt/vp-rpt96/appendix/usia.html.

U.S. President. *Interim National Security Strategy Guidance of the United States of America*. Washington, DC: The White House, March 2021. https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

———. *Indo Pacific Strategy of the United States*. Washington, DC: The White House, February 2022. https://www.whitehouse.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf.

Waltz, Edward. *Information Warfare Principles and Operations*. Boston, MA: Artech House, 1998.

Xiao, Bang. "'I Don't Know Facebook or Twitter': China's Great Firewall Generation Z Cut off from the West." *ABC News*. November 9, 2018. https://www.abc.net.au/news/2018-11-10/chinas-great-firewall-generation-who-dont-know-facebook/10479098.

Xinhua. "Full Text of Xi Jinping's Report at 19th CPC National Congress." November 3, 2017. http://www.xinhuanet.com/english/special/2017-11/03/c_136725942.html.

Yarger, Harry. *Strategic Theory for the 21st Century: The Little Book on Big Strategy*. Carlisle, PA: U.S. Army War College, Strategic Studies Institute. February 2006. https://apps.dtic.mil/dtic/tr/fulltext/u2/a444141.pdf.

Yin, R. K. *Case Study Research: Design and Methods, 5th ed*. Thousand Oaks, CA: Sage, 2014. Quoted in Aikaterni Argyrou, "Making the Case for Case Studies in Empirical Legal Research." *Utrecht Law Review* 13, no. 3 (December 2017).

Zhong, Raymond, Paul Mozur, Jeff Kao, and Aaron Krolik. "No 'Negative' News: How China Censored the Coronavirus." *The New York Times*. December 19, 2020. https://www.nytimes.com/2020/12/19/technology/china-coronavirus-censorship.html.