Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

2015-12

Chinese cyber espionage: a complementary method to aid PLA modernization

Ellis, Jamie M.

Monterey, California: Naval Postgraduate School

https://hdl.handle.net/10945/47941

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CHINESE CYBER ESPIONAGE: A COMPLEMENTARY METHOD TO AID PLA MODERNIZATION

by

Jamie M. Ellis

December 2015

Thesis Advisor: Wade L. Huntley
Second Reader: Christopher R. Twomey

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

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 instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the 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 Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2015	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE CHINESE CYBER ESPIONAGE: A COMPLEMENTARY METHOD TO AID PLA MODERNIZATION		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Jamie M. Ellis			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

In 2013, Mandiant published a report linking one People's Liberation Army (PLA) unit to the virtual exploitation of 11 modern U.S. military platforms. In the last two decades, Chinese cyber espionage has cultivated a significant reputation in cyberspace for its high-volume, illicit exploitation of defense technology. At the same time, the PLA has also rapidly modernized its naval, fighter jet, and air defense technologies. This thesis examines trends in Chinese cyber espionage, PLA modernization, and PLA acquisitions methods to determine—from only open-source information—if the categories are related and, if so, the nature of the relationship.

Defense reports suggest there is a strong correlation between China's virtual exfiltration of modern U.S. technology and the PLA's rapid advancement; cyber espionage is the principal driver for PLA modernization. This thesis asks: Does cyber espionage really play a central role in PLA modernization, or does it simply complement alternate procurement methods? This thesis draws from case studies of China's overt acquisitions, indigenous research, and physical espionage operations to demonstrate that the majority of the PLA's modernized military platforms were developed from non-cyber acquisition methods. These studies support this thesis's conclusion that cyber espionage is not the critical component driving forward PLA modernization.

14. SUBJECT TERMS China, Chinese, technology, cyber, espionage, military, modernization, Navy, Air Force, defense, PLA			**15. NUMBER OF PAGES** 161
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

CHINESE CYBER ESPIONAGE: A COMPLEMENTARY METHOD TO AID PLA MODERNIZATION

Jamie M. Ellis
Captain, United States Air Force
B.S., Embry-Riddle Aeronautical University, 2010

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(FAR EAST, SOUTHEAST ASIA, AND THE PACIFIC)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2015**

Approved by: Wade L. Huntley
Thesis Advisor

Christopher R. Twomey
Second Reader

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In 2013, Mandiant published a report linking one People's Liberation Army (PLA) unit to the virtual exploitation of 11 modern U.S. military platforms. In the last two decades, Chinese cyber espionage has cultivated a significant reputation in cyberspace for its high-volume, illicit exploitation of defense technology. At the same time, the PLA has also rapidly modernized its naval, fighter jet, and air defense technologies. This thesis examines trends in Chinese cyber espionage, PLA modernization, and PLA acquisitions methods to determine—from only open-source information—if the categories are related and, if so, the nature of the relationship.

Defense reports suggest there is a strong correlation between China's virtual exfiltration of modern U.S. technology and the PLA's rapid advancement; cyber espionage is the principal driver for PLA modernization. This thesis asks: Does cyber espionage really play a central role in PLA modernization, or does it simply complement alternate procurement methods? This thesis draws from case studies of China's overt acquisitions, indigenous research, and physical espionage operations to demonstrate that the majority of the PLA's modernized military platforms were developed from non-cyber acquisition methods. These studies support this thesis's conclusion that cyber espionage is not the critical component driving forward PLA modernization.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. MAJOR RESEARCH QUESTION AND FINDINGS....1
B. SIGNIFICANCE....5
C. LITERATURE REVIEW....7
D. POTENTIAL EXPLANATIONS AND RESEARCH DESIGN....22
E. THESIS ORGANIZATION....25

II. DEFINING KEY CYBER TERMS....27
A. TRADITIONAL ESPIONAGE VERSUS CYBER ESPIONAGE....27
B. UNDER CYBER WARFARE'S UMBRELLA: COMPARING THE SPECTRUM OF CYBER APPLICATIONS....30
C. CATEGORIZATIONS OF CYBER ACTORS: HACKER GROUPS AND INDIVIDUALS....33
1. Advanced Persistent Threats....33
2. Cyber and Information Warfare Militias....34
3. The Underground Hacking Economy....35
4. Individual Hackers as Hactivists, Patriotic Hackers, White-Hat Hackers, and Cyberterrorists....36
D. INFORMATIONIZATION....38

III. PLA MODERNIZATION MEETS INFORMATIONIZATION....39
A. THE FIRST WAVE: PLA MODERNIZATION FROM 1978–1988....39
B. THE SECOND WAVE: PLA MODERNIZATION FROM 1989–1996....41
C. THE THIRD WAVE: PLA MODERNIZATION FROM 1997–2003....44
1. Defense White Papers as Doctrinal Guidance for PLA Modernization....45
2. International Events Thrusting forward Modernization Efforts....46
3. Adopting a Modern Chinese Cyber Strategy....47
a. The Chinese Academy of Military Sciences' Cyber Experimentation....47
b. Document 27 Emerges as the Blueprint for China's Cyber Strategy....48
4. Physical Modernization Developments....49

D. THE FOURTH WAVE: PLA MODERNIZATION FROM 2004–2015 50
1. Public Characterization of Strategic Cyber Modernization 51
2. Physical Modernization Initiatives across the PLA Branches 53
3. Refining China's Modern Cyber Strategy 56
a. Updates to Document 27 56
b. Enhancements to the PLA's Cyber Structure 57
c. Drawing from Western Cyber Strategies to Build China's Cyber Strategy 58
E. SUMMARY 59

IV. COMPUTER NETWORK OPERATIONS WITH "CHINESE CHARACTERISTICS" 61
A. DECONSTRUCTING THE ORGANIZATIONAL FEATURES OF CHINA'S CYBER STRATEGY 62
1. Technical Reconnaissance Bureaus: A Case Study of PLA Unit 78020 67
2. PLA Operational Cyber Departments 68
3. PLA Operational Cyber Bureaus: A Case Study of PLA Unit 61398 71
B. CHINA'S CYBER STRATEGY AS COMPUTER NETWORK OPERATIONS 72
C. SUMMARY 75

V. PLA CYBER AND NON-CYBER ACQUISITION METHODS 77
A. CYBER ESPIONAGE 78
1. A Study of Cyber Espionage Campaigns and Their Targets 79
2. Cyber Intrusions that Likely Assisted PLA Modernization 85
3. Cyber Intrusions that Likely Aided Chinese Domestic Development Objectives 87
a. Five-Year Plans 88
b. Medium- and Long-Term Plans for the Development of Science and Technology 93
c. A Comparison of China's Developmental Goals and Cyber Espionage 94
4. Cyber Intrusions that Likely Aided CCP Foreign Policy Objectives 95
B. ALTERNATE ACQUISITION METHODS 96

1. Foreign Technological Assistance and Trade Agreements 97
2. Traditional Espionage Operations 99
3. Indigenous Research and Development Initiatives 101
a. The IDAR Model 102
b. Research and Development Programs 102
C. A CASE STUDY OF MODERNIZED PLA MILITARY PLATFORMS 104
D. SUMMARY 112

VI. CONCLUSION 113
A. IMPLICATIONS AND RECOMMENDATIONS 113
B. AVENUES FOR FUTURE RESEARCH 119

LIST OF REFERENCES 123

INITIAL DISTRIBUTION LIST 139

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. The Spectrum of Cyber Warfare with Historical Examples Demonstrating the Range and Effectiveness of Cyber Activities.....32

Figure 2. Organization of China's Major Departments and Cyber Missions under the CCP.....64

Figure 3. Organization of PLA Operational Cyber Departments under the CMC.....69

Figure 4. PLA Operational Cyber Bureaus under the Third Department.....70

Figure 5. Timeline of PLA Unit 61398's CNE Incidents from 2006–2013.....77

Figure 6. 12th FYP Strategic Emerging Industries Targeted for Development.....91

Figure 7. Examples of PLA Unit 61398's CNE Targeted Industries by Type and Number of Attacks.....92

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Technical Reconnaissance Bureaus by Region and MUCD 65

Table 2. China's Computer Network Operations (CNO) Strategy Deconstructed 73

Table 3. Chinese Government-sponsored Cyberattacks and their Origins 80

Table 4. Comparison of Previous Five-Year Plans (1996–2015) 89

Table 5. China's 2006–2020 MLP 93

Table 6. A Study of Developmental Timelines and Modernized PLA Platforms 106

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AEW	airborne early warning
AIFV	armored infantry fighting vehicle
AMRAM	air-to-air missile
AMS	Academy of Military Sciences
AMSC	American Superconductor
APT	advanced persistent threat
ASEAN	Association of Southeast Asian Nations
C2	command and control
C4I	command, control, communications, computers, and intelligence
CCP	China's Communist Party
CENTCOM	U.S. Central Command
CIA	Central Intelligence Agency
CILG	Cybersecurity Leading Small Group
CIRA	Center for Intelligence Research and Analysis
CMC	Central Military Commission
CNA	computer network attack
CND	computer network defense
CNE	computer network exploitation
CNO	computer network operations
COMINT	communications intelligence
CPI	critical program information
CSIS	Center for Strategic and International Studies
DDOS	distributed denial of service
DGI	Defense Group Inc.
DOD	Department of Defense
DOJ	Department of Justice
DWP	Defense White Papers

EEA	Economic Espionage Act
EW	electronic warfare
FBI	Federal Bureau of Investigations
FYP	Five-Year Plan
GDP	gross domestic product
GSD	General Staff Department
ICG	International Crisis Group
IDAR	introduce, digest, absorb, and re-innovate
IGCC	Institute on Global Conflict and Cooperation
INEW	Integrated Network Electronic Warfare
IP	Internet Protocol
IR	international relations
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
LSG	Leading Small Group
MLP	Medium and Long-Term Development Plan for Science and Technology
MLPS	multilevel protection scheme
MSS	Ministry of State Security
MUCD	Military Unit Covered Designators
NATO	North Atlantic Treaty Organization
NIPRNET	Non-Secure Internet Protocol Router Network
NSA	National Security Agency
OPM	Office of Personnel Management
OTH	Over-the-Horizon

PLA	People’s Liberation Army
PLAAF	PLA Air Force
PLAN	PLA Navy
PMS	Preparation for Military Struggle
PRC	People’s Republic of China
R&D	research and development
RDA	research, development, and acquisitions
RMA	Revolution in Military Affairs
RMB	renminbi
SAM	surface-to-air missile
SEI	strategic emerging industries
SIGINT	signals intelligence
SILG	State Informationization Leading Group
SIPRNET	Secret Internet Protocol Router Network
SME	subject matter expert
S&T	science and technology
TRANSCOM	U.S. Transportation Command
TRB	Technical Reconnaissance Bureau
TTP	tactics, techniques, and procedures
UAV	unmanned aerial vehicle
UNK	unknown

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Looking back from where I started, the limited knowledge and understanding I had on my thesis topic evolved to an extraordinary degree. This was primarily because of my primary advisor, Dr. Wade Huntley, to whom I owe a great deal of gratitude. Dr. Huntley shattered all my preconceived notions, challenged me to think outside the box, and continually forced me to raise conceptual questions I would not have originally asked. His enthusiasm for cyber applications, East Asia regional topics, and teaching in general not only greatly expanded my knowledge, but also got me interested in my thesis topic areas of Chinese cyber espionage and PLA modernization. I would also like to thank my second reader, Christopher Twomey, for his willingness to challenge my foundational knowledge on China and for his help throughout this thesis process. Finally, I would like to thank my family for their love, motivational words, and support through this process. Adam, you were my rock during this process. My family kept me focused on the ultimate goal of producing a well-rounded, professional thesis product. I am extremely grateful to you all.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MAJOR RESEARCH QUESTION AND FINDINGS

In 2007, the U.S. Air Force reported that Chinese cyber espionage operations exploited terabytes of confidential U.S. government and military data.[1] In 2013, Mandiant, published a report linking one People's Liberation Army (PLA) cyber unit to the virtual exploitation of 11 modern U.S. military platforms. In June 2015, the United States accused China of sponsoring a cyberattack against the Office of Personnel Management (OPM) that breached over four million U.S. government workers' security clearance information.[2] Just one month prior, the U.S. Department of Justice (DOJ) indicted three Tianjin University professors and three other People's Republic of China (PRC) nationals for economic cyber espionage.[3] Over the last two decades, China has cultivated a significant reputation in the virtual realm for its illicit acquisition of foreign technology and trade secrets through cyber espionage.[4] China is not the only nation to engage in cyber activities targeting other states: Russia, the United States, Japan, Israel, Iran, and North and South Korea also have significant virtual presences.[5] China's

[1] Desmond Ball, "China's Cyber Warfare Capabilities," *Security Challenges* 7, no. 2 (Winter 2011): 88, http://www.securitychallenges.org.au/ArticlePDFs/vol7no2Ball.pdf; Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation for the U.S.-China Economic and Security Review Commission* (McLean, VA: Northrup Grumman, 2009), 51, http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf.

[2] Ellen Nakashima, "Chinese Hackers Breach Federal Government Personnel Office," *Washington Post*, June 4, 2015, http://www.msn.com/en-us/news/us/chinese-hackers-breach-federalgovernment%e2%80%99s-personnel-office/ar-BBkHFqx.

[3] "U.S. Indicts 6 Chinese Citizens with Economic Espionage," *PressTV*, May 19, 2015, http://www.presstv.ir/Detail/2015/05/19/411879/US-Justice-Department-China-economic-espionage; Gina Chon, "U.S. Accuses Chinese Professors of Spying," *Financial Times*, May 19, 2015, http://www.ft.com/intl/cms/s/0/5268d752-fe3b-11e4-be9f-00144feabdc0.html#axzz3azag9iPl; Greg Austin, "What the U.S. Gets Wrong About Chinese Cyberespionage," *Diplomat*, May 26, 2015, China-U.S. Focus, http://www.chinausfocus.com/peace-security/what-the-us-gets-wrong-about-chinesecyberespionage/.

[4] *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2015* (Washington, DC: Office of the Secretary of Defense, April 7, 2015), 54–55, http://www.defense.gov/pubs/2015_China_Military_Power_Report.pdf; Austin, "What U.S. Gets Wrong."

[5] Martin C. Libicki, Lillian Ablon, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hacker's Bazaar* (Santa Monica, CA: RAND, 2014), 6, http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

authoritarian government structure, however, makes its cyber profile unique in that the deeper motivations for China's targeted cyber campaigns are unclear and ambiguous.[6]

China's 2015 Defense White Papers assert that cybersecurity development and preparation for winning "informationized wars" are the PRC's and PLA's top priorities, but China's method of accomplishing these objectives is enigmatic.[7] The increased frequency of Chinese cyber intrusions could be a method to aid its economic development, an advantageous tool to uncover adversarial vulnerabilities, an application to assist China's Communist Party's (CCP) foreign policy objectives, or a purely commercial endeavor conducted by private actors outside of significant central government authority.

Amid the ambiguity, however, Department of Defense (DOD) and government-sponsored reports (like U.S.-China Economic and Security Review Commission publications, DOD reports, and U.S. think tank studies) compare the upsurge in Chinese cyber espionage with the PLA's rapid twenty-first century modernization and make a key assumption that cyber espionage is the primary force behind the PLA's rapid advancement—often without establishing the basis for that claim.[8] For example, a U.S.-

---

[6] Jon R. Lindsay, "The Impact of China Cybersecurity: Fiction and Friction," *International Security* 39, no. 3 (Winter 2014–2015): 7–9, http://belfercenter.hks.harvard.edu/files/IS3903_pp007-047.pdf; Jon R. Lindsay, "Inflated Cybersecurity Threat Escalates Mistrust," *Huffington Post*, May 18, 2015, http://www.huffingtonpost.com/jon-r-lindsay/cybersecurity-threat-escalates-us-china-mistrust_b_7302282.html; Lawrence J. Cavaiola, David D. Gompert, and Martin C. Libicki, "Cyber House Rules: On War, Retaliation and Escalation," *Survival: Global Politics and Strategy* 57, no. 1 (February-March 2015): 81, http://www.iiss.org/en/Topics/chinas-cyber-policy/57-1-07-cavaiola-gompert-and-libicki-3ab8.

[7] "Document: China's Military Strategy," *USNI News*, May 26, 2015, http://news.usni.org/2015/05/26/document-chinas-military-strategy#BDC; Franz-Stefan Gady, "China to Embrace New 'Active Defense' Strategy," *Diplomat*, May 26, 2015, http://thediplomat.com/2015/05/china-to-embrace-new-active-defense-strategy/; *Annual Report to Congress: 2015*, I; Neil Robinson, "Cybersecurity Strategies Raise Hopes of International Cooperation," RAND Review, RAND, last modified July 11, 2013, http://www.rand.org/pubs/periodicals/randreview/issues/2013/summer/cybersecurity-strategies-raise-hopes-of-international-cooperation.html.

[8] U.S.-China Economic and Security Review Commission, "Section 2: China's Cyber Activities," *2013 Annual Report to Congress* (Washington, DC: USCC), 244–45, 259, http://origin.www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%202%3B%20Section%202%20China%27s%20Cyber%20Activities.pdf; *Annual Report to Congress: 2015*, 22, 35; *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2014* (Washington, DC: Office of the Secretary of Defense, Department of Defense, 2014), 35, http://www.defense.gov/pubs/2014_DOD_China_Report.pdf; Eric Heginbotham et al., *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power 1996–2017* (Santa Monica, CA: RAND, 2015), 24–25, http://www.rand.org/pubs/research_reports/RR392.html.

China Economic and Security Review Commission publication asserts that, "China's cyber espionage…of U.S. military contractors likely improves China's insight in U.S. weapons systems…and shortens China's research and development timelines for military technologies."[9] An excerpt from the 2015 Annual Report to Congress on the "Military and Security Developments Involving the [PRC]" also demonstrates this assumption: "China is using its cyber espionage capabilities to support intelligence collection against U.S. diplomatic, economic, and defense industrial base sectors…The information targeted could potentially be used to benefit China's defense industry."[10] While there are likely classified analyses on the subject, there are not widely accessible, open-source assessments that directly address these assumptions.

Consequently, this thesis addresses China's increased use of exploitive cyber methods with regard to PLA modernization to demonstrate how they are related. The major research question for this thesis is: How do suspected Chinese cyber espionage campaigns fit into the PLA military's modernization strategy? Using exclusively open-source information, this thesis seeks to understand China's interpretation of its own cyber strategy and determine the historical, internal, and external motivating factors that drive China's use and employment of cyber espionage. Through a study of PLA modernization initiatives and exploitive Chinese cyber operations, this thesis investigates if cyber espionage plays a central, limited, or complementary role in accelerating China's military advancement.

This thesis employs case studies of Chinese cyber intrusions, virtually exploited U.S. military technologies, developmental timelines of modern PLA military technology, and alternate PLA procurement methods, to show that government-sanctioned cyber espionage is a complementary (not a primary) acquisition method. This thesis first examines 24 cases of noted, historical Chinese cyber espionage operations (*Byzantine Hydes*, *Ghost Net*, *Shady Rat,* etc.) and their respective military, government, or private industry targets. Based on this, it is shown that approximately 33 percent (one-third) of the cyber intrusions on military and defense objectives likely assisted PLA military

[9] U.S.-China Economic and Security Review Commission, "Section 2: China's Cyber Activities," 258.

[10] *Annual Report to Congress: 2015,* 39.

modernization; approximately 42–44 percent (a little over one-third) of the cyber espionage operations likely assisted China's domestic development goals; and approximately 38–42 percent (a little over one-third) percent of the cyber intrusions likely aided CCP foreign policy objectives. The percentages vary based on the wide range of exploited targets in individual computer network exploitation (CNE) operations: some cyber espionage campaigns exploited military, economic, and diplomatic objectives under the same operation, and some campaigns only exploited one or two categories at a time.[11] The evidence of China's relatively equal cyber exploitation record across three developmental categorical target areas highlights the divided focus of the Chinese government's sponsored cyber espionage operations.

Focusing on the first of these categories, this thesis then examines the PLA's alternate acquisitions methods—negotiated military technology purchases from foreign governments, negotiated trade agreements, traditional espionage operations, and indigenous research and development (R&D) programs—and compares them with the PLA's developmental timelines of critical, modern military technologies. This study identifies 21 modernized PLA military platforms (study pulls examples from the PLA Air Force [PLAAF], PLA Navy [PLAN], and PLA Army), their U.S. equivalent model, and their developmental timelines to determine if the means of their production were primarily due to cyber espionage. It concludes approximately 19 percent of these military platforms were likely exclusively developed from cyber espionage exploits; approximately 48 percent of the military platforms were likely developed from exclusively non-cyber acquisition methods (whether by reverse engineering, overt purchases, technology trade agreements, or traditional espionage); and approximately 33 percent were likely developed from a combination of cyber espionage and non-cyber procurement methods. Put another way, over 80 percent of the 21 cases involve non-cyber acquisition methods, while only 52 percent of the cases include cyber espionage.[12]

[11] Cyber espionage operations, or campaigns, can last several days, weeks, months, or years without the affected entity knowing. A single cyber espionage campaign constitutes one cyber actor exploiting one target, or the same target, for information no matter the length of the exfiltration operation.

[12] The variance in the percentages is due to the inclusion of cases that employed both cyber and non-cyber means.

This study confirms that cyber espionage assists PLA modernization efforts, but it also shows that non-cyber espionage procurement methods are used in the majority of PLA modernized military platform cases. The PLA's use of robust alternate procurement methods on the majority of its modernized PLA equipment suggest that government-sponsored cyber espionage complements existing PLA procurement processes to modernize the PLA military. Since this thesis relies exclusively on publicly available information, the research findings could need to be modified if classified information released in the future or other future research presents information that contradicts this study's conclusions.

B. SIGNIFICANCE

The world is exploding with rapid technology changes, cyber network interoperability, and proliferated Internet access across the globe. The interconnected nature of the Information Age has introduced a host of new cyber exploitation areas on which governments, industries, and cyber criminals capitalize.[13] Due to their advanced technological capabilities, Russia and the United States have been the frontrunners in cyber warfare. Within the last decade, however, the PRC was added to the list as a frequent suspect in cyber espionage cases.[14] Primarily among U.S. defense reports, one area of agreement is that PRC-sponsored cyberattacks are increasing at an enormous rate, which may provide long-term advantages for PLA military capabilities.[15] From DOD cyber missions to President Barak Obama's foreign policy priorities, cybersecurity has become a top concern for the United States; as Obama explained:

---

[13] *U.S. International Strategy for Cybersecurity, Before the Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, Senate Foreign Relations Committee*, Cong. (March 14, 2015) (statement of James A. Lewis, Director for Strategic Technologies Program at the Center for Strategic and International Studies), 1, http://www.foreign.senate.gov/imo/media/doc/051415_REVISED_Lewis_Testimony.pdf; Timothy L. Thomas, "China's Cyber Incursions: A Theoretical Look at What They See and Why They Do It Based on a Different Strategic Method of Thought," *OE Watch* (March 2013): 1–2, http://fmso.leavenworth.army.mil/documents/China's-Cyber-Incursions.pdf; Paul Cornish, "Governing Cyberspace through Constructive Ambiguity," *Survival: Global Politics and Strategy* 57, no. 3 (June-July 2015): 153, http://www.iiss.org/en/Topics/chinas-cyber-policy/57-3-09-cornish-a772.

[14] Robinson, "Cybersecurity Strategies Raise Hopes"; James A. Lewis, "To Protect the U.S. Against Cyberwar, Best Defense is a Good Offense," *U.S News and World Report*, March 29, 2010, http://www.usnews.com/opinion/articles/2010/03/29/to-protect-the-us-against-cyberwar-best-defense-is-a-good-offense; Cavaiola, Gompert, and Libicki, "Cyber House Rules," 81.

[15] U.S.-China Economic and Security Review Commission, "China's Cyber Activities," 259.

> America's economic prosperity, national security, and our individual liberties depend on our commitment to security cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property…the threats are serious and they constantly evolve.[16]

As President Obama's statement implies, the United States faces many challenges in cyberspace—specifically the challenge of how to defend against the increased cyber exploitation of its critical technologies.[17] Testimony at U.S. Senate hearings also upholds the White House's emphasis on cybersecurity, but concludes that the growing concern lies with Chinese-sponsored, "cyber-enabled theft of intellectual property for commercial gain."[18] How can the United States and other countries protect their military technology from PRC-sponsored cyber spying if they do not understand China's cyber strategy?[19] What are the drivers for China's cyber espionage targets; why does it continually direct attacks toward companies like Northrup Grumman, Lockheed Martin, or U.S. Internet search engines?[20] These questions demonstrate the voiced confusion and lack of understanding among top political, defense, and government officials about the upward

---

[16] Barak Obama, "Cybersecurity," Foreign Policy, U.S. Whitehouse, accessed May 19, 2015, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity#section-engage-internationally.

[17] Richard B. Andres, "The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 89–90, https://muse.jhu.edu.libproxy.nps.edu/books/9781589019195/9781589019195-12.pdf.

[18] *Cybersecurity: Setting the Rules for Responsible Global Behavior, Before the Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy*, Cong. (May 14, 2015) (statement of Christopher M. E. Painter, U.S. Department of State Coordinator for Cyber Issues), 4, http://www.foreign.senate.gov/imo/media/doc/051415_Painter_Testimony.pdf; George Leopold, "China's Military Calls for 'Online Great Wall,'" Defense Systems, Public Sector Media Group, last modified May 21, 2015, http://defensesystems.com/articles/2015/05/21/china-pla-online-great-wall.aspx.

[19] Timothy L. Thomas, "China's Concept of Military Strategy," *Parameters* 44, no. 4 (Winter 2014–2015): 39, http://strategicstudiesinstitute.army.mil/pubs/parameters/Issues/Winter_2014-15/7_ThomasTimothy_ChinasConceptofMilitaryStrategy.pdf.

[20] Dmitri Alperovitch, "Revealed: Operation Shady RAT," McAfee, 3–4, accessed June 3, 2015, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf; Timothy L. Thomas et al., "A PLA Cyber 'Rules of the Road' Proposal," *OE Watch* 3, no. 7 (July 2013): 48, http://fmso.leavenworth.army.mil/OEWatch/201307/201307.pdf; Bill Gertz, "NSA Details Chinese Cyber Theft of F-35, Military Secrets," *Washington Beacon*, January 22, 2015, http://freebeacon.com/national-security/nsa-details-chinese-cyber-theft-of-f-35-military-secrets/; Michael Joseph Gross, "Enter the Cyber-dragon," *Vanity Fair*, September 2011, http://www.vanityfair.com/news/2011/09/chinese-hacking-201109.

trend of Chinese cyber operations. Global anxiety over the PRC's cyber tactics and language outlined in its forward-leaning Defense White Papers bring forth the importance of interpreting China's cyber methodology.[21] A better understanding of the motivations behind PRC cyber espionage and its relationship with the PLA's modernization is crucial; this thesis addresses those general questions and anticipates the broad international implications of China's cyberspace behavior.[22]

C. LITERATURE REVIEW

The debates in the literature that address China's cyber strategy, PLA cyber methods, and rapid PLA modernization span across a range of intricate, rapidly evolving cyber and technological discussions. What is China's current cyber strategy? Does China employ a coordinated or fragmented cyber strategy? Is China's cyber strategy offensive, defensive, military-target focused, or private industry-focused, and why? These representative questions address key groups of literature topics that attempt to explain the reason for the PLA's accelerated modernization, China's increased virtual presence, and the growth in frequency of Chinese cyberattacks on foreign targets. Additionally, these questions are used to help distinguish the categories of debates in the literature in this section.

Despite the contributions these publications make toward explaining China's cyber actions and the course of PLA modernization, there is not enough unclassified literature devoted to exploring how China's cyber espionage directly relates to PLA modernization: specifically, the degree to which cyber exploitation assists the military's advancement. Of the literature on both PLA modernization and cyber warfare published since the late 1990s, many scholars try to interpret China's strategic thinking on both: Is

[21] "Document: China's Military Strategy."

[22] Thomas et al., "PLA Cyber 'Rules of Road,'" 48.

it offensive, defensive, or a combination of the two?[23] This group of authors is broken up into two categories: U.S. and Western scholars who argue China's cyber strategy is oriented in an offensive manner, and Chinese scholars who argue the strategy is a defensive, modernized version of traditional warfare—similar to developed cyber strategies employed throughout the world.

U.S. Army analyst Timothy L. Thomas and James C. Mulvenon, Director for the Center of Intelligence Research and Analysis (CIRA) at the Defense Group Inc. (DGI), are two key authors who are representative of the majority of studies on China's modern cyber strategy from U.S. and Western perspectives. Western perspectives often reference the "cult of the offensive,"[24] because they advocate that China's cyber strategy is offensive in nature, and the only way for the United States to combat that strategy is with a similarly aggressive stance.[25] Other key contributors to this literature include U.S. government, defense, and news reports. These reports argue that China's cyber strategy is

[23] Allen A. Friedman, "Cyber Theft of Competitive Data: Asking the Right Questions," Center for Technology Innovation, Brookings Institute (September 2013), 1, http://www.brookings.edu/~/media/research/files/papers/2013/09/25-cyber-theft-competitive-data-friedman/brookingscybertech_revised.pdf; James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in *Beyond the Strait: PLA Missions Other Than Taiwan*, ed. Roy Kamphausen, David Lai, and Andrew Scobell (Carlisle, PA: U.S. Army War College, 2009), 257–58; Kevin Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), 141.

[24] P.W. Singer and Allen Friedman, "Cult of the Cyber Offensive: Why belief in the First-Strike Advantage is as Misguided Today as it was in 1914," Foreign Policy, last modified January 15, 2014, http://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/

[25] Heginbotham et al., *U.S.-China Military Scorecard*, 273; Mulvenon, "PLA Computer Network Operations," 258–59.

also offense-oriented and use the case of one PLA unit's cyber compromise of more than 140 Western targets over seven years as supporting evidence.[26]

Mulvenon and Thomas represent a group of authors who address China's increased cyber theft of sensitive technology with respect to its impact on PLA modernization.[27] Thomas and Mulvenon provide detailed explanations of current Chinese cyber operations, and the factors that influence China's stance on cyber warfare to describe why China's strategy is aggressive and offense-centric.[28] Their works (through analyses of Chinese language sources) provide useful descriptions of current PLA cyber operations and cyber terminology to clearly outline the parameters of China's cyber strategy.[29] Ultimately, Thomas and Mulvenon's literature describe the nature of China's grand cyber strategy, why China employs certain cyber methods, and

[26] "APT 1: Exposing One of China's Cyber Espionage Units," Mandiant (February 2013), 2–4, http://intelreport.mandiant.com; Adam M. Segal, "Cyberspace: The New Strategic Realm in U.S.-China Relations," *Strategic Analysis* 38, no.4 (2014): 577, http://dx.doi.org/10.1080/09700161.2014.918447; Gertz, "NSA Details Chinese Cyber Theft"; "Chinese Military Experts Slam U.S. Defence Report Alleging Cyber Attacks," *BBC Worldwide Monitoring*, May 8, 2013, http://www.lexisnexis.com.libproxy.nps.edu/hottopics/lnacademic/; James A. Lewis, "Five Myths about Chinese Hackers," *Washington Post*, March 22, 2013, http://www.washingtonpost.com/opinions/five-myths-about-chinese-hackers/2013/03/22/4aa07a7e-7f95-11e2-8074-b26a871b165a_story.html; *Cyber Threats from China, Russia, and Iran: Protecting American Critical Infrastructure Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security, House of Representatives*, 113th Cong., 1 (2013), 11 (statement of Frank J. Cilluffo, Director of the Homeland Security Policy Institute at George Washington University), https://www.hsdl.org/?view&did=755309; "China's Cyber-theft Jet Fighter," *Wall Street Journal*, November 12, 2014, http://www.wsj.com/articles/chinas-cyber-theft-jet-fighter-1415838777.

[27] Mulvenon, "PLA Computer Network Operations," 253–54; James Mulvenon, interview by Ray Suarez, "U.S. Government, Industry Fed up with Chinese Cyber Theft; What's Being Done?" *PBS News Hour*, July 8, 2013, http://www.pbs.org/newshour/bb/military-july-dec13-cybercrime_07-08/; Mark A. Stokes and L.C. Russell Hsiao, *Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests* (Project 2049 Institute, October 29, 2012), 3–5, http://www.project2049.net/documents/countering_chinese_cyber_operations_stokes_hsiao.pdf.

[28] Richard Parker, "Trojan Alert! It's Not Just the Russians Who are Spying on America," *Nation* (Thailand), July 6, 2010, http://www.lexisnexis.com.libproxy.nps.edu/hottopics/lnacademic/; Adam Segal, *Advantage: How American Innovation Can Overcome the Asian Challenge* (New York: W. W. Norton & Company, 2011).

[29] Thomas, "China's Cyber Incursions," 2–5; Thomas, "China's Concept of Military Strategy," 41–43.

recommend effective counterstrategies.[30] The two authors differ, however, in their methods of approach and conclusions.[31]

Mulvenon makes his observations of China's employment of current computer network operations (CNO) to argue that China's cyber strategy is oriented in an offensive, aggressive manner because it seeks to both deter the U.S. and maintain a semblance of control over Taiwan. Mulvenon contends the best U.S. response is to cultivate a similarly aggressive, offense-centric cyber strategy.[32] This thesis finds Mulvenon's work helpful and relies on his detailed analyses of China's modern CNO to engage in an accurate study of how China employs cyber espionage.

In contrast, Thomas's analyses interpret Chinese perspectives on military strategy and transfer that view over to China's cyber operations to discuss the orientation and methods of China's modern cyber strategy.[33] Thomas uses case studies of China's modern strategic cyber language as evidence to show the influence of Sun Zi's historical principles on its cyber strategy: deception and obtaining a strategic advantage over the enemy through offense will help achieve victory.[34] This thesis also finds Thomas's work useful since he dissects China's cyber strategy from a Chinese cultural perspective—instead of relying on traditional Western views. Consequently, this thesis utilizes Thomas and Mulvenon's works since they represent the majority of publications on China's cyber strategy and approach the subject from a Chinese viewpoint.

Thomas and Mulvenon's discussions on China's modern cyber operations and the nature of China's cyber strategy are helpful for this thesis but lack the foundational information on the origins of that strategy. Hence, rather than enter their debate over whether China's cyber strategy is inherently offensive or defensive, this thesis builds on

---

[30] Mulvenon, "PLA Computer Network Operations," 280; Stokes and Hsiao, *Countering Chinese Cyber Operations*, 2–5; Thomas et al., "PLA Cyber 'Rules of Road,'" 48.

[31] Thomas, "China's Cyber Incursions," 1–5; Thomas, "China's Concept of Military Strategy," 39–40; Mulvenon, "PLA Computer Network Operations," 253–54.

[32] Parker, "Trojan Alert"; Mulvenon, "PLA Computer Network Operations," 267, 279–80.

[33] Thomas, "China's Cyber Incursions," 3–11; Timothy L. Thomas, "The Chinese Military's Strategic Mind-set," *Military Review* 87, no. 6 (November-December 2007): 47–49, http://fmso.leavenworth.army.mil/documents/chinese-mind-set.pdf.

[34] Thomas, "China's Cyber Incursions," 5–11.

their studies to establish the foundation for China's cyber strategy and demonstrate how the PLA's use of certain cyber methods—cyber espionage and CNE—fits into that strategy.[35] In opposition to Thomas and Mulvenon's work, the Chinese military and strategic cyber literature denies this view that China's cyber strategy is primarily offensive in nature.

Chinese-native language literature frequently disagrees with U.S. and Western perceptions that China's cyber strategy is aggressive and offense-centric. Chinese authors argue that China's cyber strategy is oriented in a defensive, cooperative, operational manner.[36] "China's Military Strategy," as *The Science of Military Strategy* claims, "is to protect national sovereignty and territorial integrity, resist aggression and subversion from outside, and safeguard people's labor in peace."[37] Chinese government, military, and media outlets frequently uphold the position that China is heavily victimized by CNE and cyberattacks, so the cyber intrusions it launches are part of its defense approach to cyber strategy.[38]

This Chinese-native literature emphasizes China's "Peaceful Development and Five Principles of Peaceful Coexistence" as evidence of China's nonaggressive cyber intentions.[39] China's Defense White Papers maintain that China uses its developed cyber capabilities for its own peaceful development and in response to U.S. hacks on Chinese

---

[35] Thomas, "China's Cyber Incursions," 1; Thomas, "China's Concept of Military Strategy," 39–40.

[36] Thomas, Hurst, Kim et al., "PLA Cyber 'Rules of Road,'" 48.

[37] Guangqian Peng and Yao Youzhi, ed., *The Science of Military Strategy* (Beijing: Military Science Publishing House, 2005), 13.

[38] "Foreign Gov't Backed Forces Hack into Chinese Agencies: Report," *Xinhua*, May 29, 2015, trans. Open Source Center (Washington, DC, May 29, 2015), https://www.opensource.gov/portal/server.pt/gateway/PTARGS_0_0_200_203_121123_43/content/Display/CHR2015052953397017#index=1&searchKey=19171295&rpp=10; "Document: China's Military Strategy"; Dongping Han, "U.S., not China, Involved in Cyber Espionage," *China Daily*, February 13, 2015, http://www.lexisnexis.com.libproxy.nps.edu/hottopics/lnacademic/; Lindsay, "Impact of China on Cybersecurity: Fiction and Friction," 8, 44; Lewis, "Five Myths"; Austin, "What the U.S. Gets Wrong"; "China Ramps Up Public Cyber Security Awareness," *Xinhua*, June 1, 2015, trans. Open Source Center (Washington, DC, June 1, 2015), https://www.opensource.gov/portal/server.pt/gateway/PTARGS_0_0_200_203_121123_43/content/Display/CHR2015060135582672#index=1&searchKey=19171242&rpp=10.

[39] Yamei Wang, "Full Text: China's Peaceful Development," *Xinhua*, September 6, 2011, http://news.xinhuanet.com/english2010/china/2011-09/06/c_131102329.htm; Fu Peng, ed., "The Diversified Employment of China's Armed Forces," *Xinhua*, April 2013, http://news.xinhuanet.com/english/china/2013-04/16/c_132312681.htm.

networks.[40] As another example, Chinese author Han Dongping directly disputes China's so-called unlawful cyber acquisition of F-35 schematics by stating the United States repeatedly launches cyberattacks against PRC networks—as evident by the Edward Snowden-released information.[41] While it is important to introduce Chinese literature that offers an alternate perspective to U.S. views and addresses the nature of China's cyber strategy, the publications could have biased foundations for Chinese government purposes that do not accurately portray the nature of China's cyber strategy. This thesis incorporates these Chinese perspectives to provide an accurate depiction of China's modern strategic thought and Chinese views on the employment of cyber espionage. As previously mentioned, however, this thesis does seek to enter the debate on whether the orientation of China's cyber strategy is offensive or defensive in nature.

The next category of literature also examines China's cyber strategy but takes a different approach to earlier debates to determine the quality of China's cyber strategy compared to other nations: Is China's cyber strategy coordinated and organized, or is it an unsystematic, *ad hoc* strategy?[42] This group of literature does not discuss the historical, domestic, or international drivers that impact the orientation of China's modern strategy. These publications operate under the key assumption that China has an established cyber strategy. On one side of this debate, publications contend that the CCP's delegation of China's cyber mission to the disorganized Chinese-state bureaucracy has left the implementation of China's cyber strategy disjointed and fragmented.[43]

Authors that evaluate China's cyber strategy as underdeveloped, argue that Chinese cyber operations are too fragmented to pose a legitimate threat to U.S. national security. Authors in this debate substantiate their arguments through comparisons of U.S.

---

[40] Peng, "Diversified Employment of China's Armed Forces," 7; Wang, "China's Peaceful Development."

[41] Han, "U.S., not China"; Zhiming Xin, "China's Cyber Move in the Right Direction," *China Daily*, May 14, 2014, http://www.lexisnexis.com.libproxy.nps.edu/hottopics/lnacademic/; Jing De Jong-Chen, "U.S.-China Cybersecurity Relations: Understanding China's Current Environment," *Georgetown Journal of International Affairs*, September 15, 2014, http://journal.georgetown.edu/u-s-china-cybersecurity-relations-understanding-chinas-current-environment/.

[42] Ball, "China's Cyber Warfare Capabilities," 81–82.

[43] Lindsay, "Inflated Cybersecurity Threat."

and Chinese cyberattacks: they argue that U.S. cyber capabilities are more sophisticated than the basic technical skills China employs.[44] This literature also cites numerous domestic and territorial concerns China prioritizes over its cyber strategy to argue that those concerns prevent China from cultivating robust, sophisticated cyber capabilities that would severely damage U.S. networks.[45] In particular, as an authoritarian regime, strict control over its population's access to information is vital to the survival of the CCP at the top of the PRC state.[46] Doing this, in turn, requires strict control over the Internet, which State Department and commercial actors promoting "open Internet" threatens.[47] These publications also argue that U.S. defense reports' evaluations of China's cyber strategy as developed, organized, and a threat to U.S. national security are inaccurate because of their lack of foundational evidence.[48]

U.S. government- and defense-sponsored reports represent the alternate side of this debate because they maintain the perception that China possesses advanced cyber capabilities; they contend that their analyses are correct and even under-evaluated.[49] U.S. security commission reports draw support for their claims from studies of wide-scale Chinese CNE operations: the Mandiant-reported information highlighting one PLA units' largely undetected record of cyber intrusion operations of 141 targets from 2006–2013.[50] Defense reports also compare China's ambiguous cyber capabilities with transparent U.S. cyber missions to make this point. These reports contend that China employs a high

[44] Lindsay, "Inflated Cybersecurity Threat"; *Cyber Threats from China, Russia, and Iran*, 11.

[45] Franz-Stefan Gady, "Does China Really Know How to Wage Cyber War," *Diplomat*, February 20, 2015, http://thediplomat.com/2015/02/does-china-really-know-how-to-wage-cyber-war; Lindsay, "Inflated Cybersecurity Threat."

[46] Lindsay, "Impact of China on Cybersecurity: Fiction and Friction," 14–16.

[47] Ibid; Inkster, "China in Cyberspace," 191–92; Lindsay, "Inflated Cybersecurity Threat" ; Jon R. Lindsay, "Introduction—China and Cybersecurity: Controversy," in *China and Cybersecurity" Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), 10–11.

[48] Gady, "Does China Really Know."

[49] *Annual Report to Congress: 2015*, 54.

[50] Nakashima, "Chinese Hackers Breach Federal Government"; "APT 1," 2–4.

degree of secrecy in their operations because their cyber capabilities are continually advancing.[51]

Government- and defense-sponsored reports also conclude that China's increased cyber espionage points to a larger trend: the cyber threat from China spans much wider than the United States knows.[52] This thesis agrees with these studies that China does in fact employ a coherent, observable cyber strategy. This thesis also draws information from these studies to establish the foundation and parameters for China's cyber strategy. This thesis does not, however, provide an evaluation on the quality of China's cyber strategy. This thesis uses defense-reported information to establish the basis that China has a cyber strategy that employs cyber espionage but does not comment on whether that strategy employs advanced cyber capabilities or rudimentary technical skills.

Broadening the scope of research, there is literature that examines Chinese cyber espionage operations in relation to U.S. national security and cybersecurity concerns.[53] Is cyber espionage of U.S. military data or U.S. trade secrets more damaging to U.S. national security? This literature divides cyber espionage targets into categories and explores how CNE of each category impacts U.S. foreign policy decisions.[54] These publications distinguish between military and economic cyber espionage to argue that the exploitation of certain targets is more damaging than others. While there is disagreement

---

[51] U.S.-China Economic and Security Review Commission, "China's Cyber Activities," 244–45, 259; *Annual Report to Congress: 2015*, 22, 35.

[52] U.S.-China Economic and Security Review Commission, "China's Cyber Activities," 244–45, 259; *Annual Report to Congress: 2015*, 22, 35.

[53] Derek S. Reveron, "An Introduction to National Security and Cyberspace," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 6; Jason Harmala, "Cyber Experts Weigh in on Threat of Chinese Cyber Espionage," discussion with Franklin D. Kramer, Dmitri Alperovitch, James Mulvenon, and Gregory J. Rattray (Washington, DC: Brent Scowcroft Center on International Security, Atlantic Council), http://www.atlanticcouncil.org/events/past-events/cyber-experts-weigh-in-on-threat-of-chinese-cyber-espionage.

[54] Adam Segal, "Shaming Chinese Hackers Won't Work because Cyber-espionage is here to Stay," *Guardian*, May 30, 2013, http://www.theguardian.com/commentisfree/2013/may/30/china-hacking-cyber-espionage-obama; John D. Negroponte et al., "Defending an Open, Global, Secure, and Resilient Internet," *Independent Task Force Report*, no.70 (Washington, DC: Council on Foreign Relations, 2013), ix, http://www.cfr.org/cybersecurity/defending-open-global-secure-resilient-Internet/p30836; Adam Segal, "The Challenge of China as a Science and Technology Superpower," *Guardian*, October 11, 2013, http://www.theguardian.com/science/political-science/2013/oct/11/china-science-superpower.

on which category is more damaging to U.S. national security, both debates agree that increased Chinese cyber intrusion on U.S. networks is a concern the United States needs to mitigate.[55] Defense reports cite the damage cyber espionage of U.S. military and defense information causes; scholarly articles and private industry publications list the impact industrial trade secret CNE has on U.S. national security. This thesis agrees with these publications' categorical separation of cyber espionage targets and uses them to conduct a precise study of how cyber espionage fits in to PLA modernization.

On one side of the debate, scholars Derek S. Reveron and Adam Segal, advocate that China's cyber exploitation of U.S. private industries and intellectual property is a damaging, unsanctioned form of warfare.[56] Publications in this debate argue that China focuses on using CNE to acquire key foreign industrial secrets and technologies because the economic information rapidly increases the rate at which China's domestic economy grows, China's outdated infrastructure improves, China's global economic standing rises, and China's economic edge over the United States increases.[57]

In contrast, U.S. defense and military reports contend that the theft of military system designs is more damaging to U.S. national security.[58] U.S. defense- and military-sponsored reports agree with the premise that cyber espionage of U.S. trade secrets is damaging, but they place more weight on the damaging effects CNE has on modern military platforms.[59] The reports list the PRC's compromise of U.S. F-35 fighter technology and China's subsequent tests of its strikingly similar J-31 fighter jet as cases

[55] Negroponte et al., "Open, Global, Secure, and Resilient Internet," 4–5.

[56] Segal, "Shaming Chinese Hackers"; Segal, "Cyberspace: New Strategic Realm," 578–79.

[57] Segal, *Advantage: American Innovation Overcome Asian Challenge*, 109–13.

[58] Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security* 4, no. 2 (2011): 2–3, doi: 10.5038/1944-0472.4.2.1; U.S.-China Economic and Security Review Commission, "Section 2: China's Cyber Activities," 243–48.

[59] U.S.-China Economic and Security Review Commission, "Section 2: China's Cyber Activities," 247.

of indisputable evidence.[60] These reports also expand their argument to comment on the rapid pace of China's and the PLA's development.

Defense reports also make a key assumption that China's elevated economic and advanced military development are products of Chinese cyber espionage.[61] This thesis rejects that assumption because there is frequently no foundational evidence presented to support that claim. This thesis finds these publications' distinction between military and economic CNE targets useful to discover trends in Chinese cyber espionage campaigns; however, the major goal of this study is to address the assumption that cyber espionage is the primary explanation for the PLA's rapid modernization. This thesis also establishes the evidentiary basis for the role cyber espionage plays in accelerating PLA modernization. But this thesis does not evaluate which cyber espionage target category—military or economic—is more damaging to U.S. national security.

Another debate in the literature related to this thesis, discusses the effects China's underdeveloped domestic innovation has on the PLA's advancement.[62] Tai Ming Cheung, Jon R. Lindsay, and Segal are key authors representing these publications. They investigate the connection between PLA modernization, increased Chinese cyber espionage, and indigenous Chinese innovative and R&D capacities.[63] These publications surmise that China's rudimentary domestic innovative capabilities force its dependence

---

[60] U.S.-China Economic and Security Review Commission, "Section 2: China's Cyber Activities," 247; Segal, "Cyberspace: New Strategic Realm," 577; Gertz, "NSA Details Chinese Cyber Theft"; "Chinese Military Experts Slam U.S. Defence Report"; Lewis, "Five Myths"; Cilluffo, *Cyber Threats from China, Russia, and Iran*, 11; "China's Cyber-theft Jet Fighter."

[61] George J. Gilboy, "The Myth Behind China's Miracle," *Foreign Affairs* 83, no. 4 (2004): 38, http://www.jstor.org/stable/2003404534-35; Jon R. Lindsay and Tai Ming Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), 56, 73–74.

[62] Gary L. Pembleton, "Assessing Technology Innovation in the PLA" (master's thesis, Naval Postgraduate School, Monterey, CA, March 2015), v, http://hdl.handle.net/10945/45238; John T. Oakley, "Cyber Warfare: China's Strategy to Dominate in Cyber Space" (master's thesis, Fort Leavenworth, Kansas, 2011), 16, http://www.dtic.mil/dtic/tr/fulltext/u2/a547718.pdf.

[63] Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, "Will China and America Clash in Cyberspace?" *National Interest*, April 12, 2015, http://nationalinterest.org/feature/will-china-america-clash-cyberspace-12607; Anthony H. Cordesman, Ashley Hess, and Nicholas S. Yarosh. *Chinese Military Modernization and Force Development: A Western Perspective* (Washington, DC: Center for Strategic & International Studies, August 2013), 59–61, http://csis.org/files/publication/130725_chinesemilmodern.pdf; Segal, "Challenge of China as Science and Technology Superpower."

on foreign technology acquisitions to modernize the PLA.[64] These publications compare the high amount of China's foreign technology acquisitions (whether through trade agreements, cyber espionage campaigns, traditional espionage operations, or reverse engineering) with its limited domestically produced innovative technology to support their argument. These publications assert that China's accessibility to foreign technology through various procurement means has diminished its urgency to develop China's private R&D industries and innovation-focused infrastructure.[65] Ultimately, these reports advocate that China needs to develop domestic technological innovation rather than depend primarily on espionage to maintain a modernized military whose capabilities rival Western nations.[66]

While the evidence in the above-referenced articles associates cyber espionage with PLA modernization, it does not provide a comprehensive description of how cyber espionage fits into the PLA's advancement. The difference between this thesis' focus and the domestic innovation publications is that the publications imply cyber espionage is one of several coping mechanisms the PLA uses to modernize its equipment. The articles do not discuss the role cyber espionage plays in advancing PLA modernization as this thesis does. This study finds the publications' identification of China's alternate procurement

---

[64] Gilboy, "Myth Behind China's Miracle," 34–35; Lindsay and Cheung, "Exploitation to Innovation," 56, 73–74.

[65] Ibid.

[66] Tai Ming Cheung, "China's Emergence as a Defense Technological Power: Introduction," The *Journal of Strategic Studies* 34, no. 3 (June 2011): 296, http://www.tandfonline.com/doi/pdf/10.1080/01402390.2011.583155; Tai Ming Cheung, "Rejuvenating the Chinese Defense Economy: Present Developments and Future Trends," *The Study of Innovation and Technology in China Policy Brief* No. 19 (University of California Institute on Global Conflict and Cooperation, September 2011), 1, https://escholarship.org/uc/item/60z7p0kp; Cindy Hurst, "China's Digital Destroyers: Striving for Information Dominance," Foreign Military Studies Office, Ft. Leavenworth, U.S. Army, accessed May 28, 2015, 3, http://fmso.leavenworth.army.mil/documents/China's-digital-destroyers.pdf; Segal, *Advantage: American Innovation Overcome Asian Challenge*, 80; Kathleen A. Walsh, "China's Defense Technology Acquisition System, Processes, and Future as an Integrator and Supplier," *The Study of Innovation and Technology in China Policy Brief 2014* (University of California Institute on Global Conflict and Cooperation, January 2014), 1, http://escholarship.org/uc/item/82r7r1nj; Maggie Marcum and Aliaksandr Milshyn, "Changing Trends in Global Research, Development, and Acquisition Process," *The Study of Innovation and Technology in China Policy Brief 2014* (University of California Institute on Global Conflict and Cooperation, January 2014), 2–3, http://escholarship.org/uc/item/7s48w1ck; Maggie Marcum, "Assessing High-Risk, High-Benefit Research Organizations: The 'DARPA Effect,'" *The Study of Innovation and Technology in China Policy Brief* 2014 (University of California Institute on Global Conflict and Cooperation, January 2014), 1, http://escholarship.org/uc/item/7n49c638.

methods for specific military technologies very useful and draws from their examples to support the research findings. This thesis also utilizes these examples to draw correlations between the frequency each method is used and to distinguish if one method is used more heavily than others. This thesis finds the description of China's underdeveloped innovative capacities helpful, as a potential explanation: it suggests why the PLA employs CNE versus alternate procurement methods. This thesis does not discuss the finer details of China's innovative capacity to recommend improvement areas.

Taking an alternate approach to PLA modernization and Chinese cyber espionage, James A. Lewis, Strategic Technologies Director at the Center for Strategic and International Studies (CSIS), represents a literature category that debates cyberspace definitions. Specifically, do China's cyber operations warrant retaliation because they are defined as cyberattacks, or are they just employing benign virtual methods of traditional espionage? Lewis highlights U.S. government and military officials' interchangeable use of "cyber espionage" and "cyberattack" to highlight his point: cyberattacks cause physical damage, so if China conducted cyberattacks on the United States—instead of cyber espionage—the United States could respond with kinetic force because those attacks would be considered virtual acts of war.[67] Lewis also contends that while China sanctions cyber espionage on U.S. targets, virtual spying does not cause damage and is not tantamount to a cyberattack.[68]

Lewis's representative work establishes precise definitions of cyber warfare, cyberattacks, and cyber espionage, but does so to comment on the overall threat level Chinese hackers pose to U.S networks.[69] Lewis defends his point by arguing that China would not instigate cyberattacks because China recognizes the U.S.'s virtual superiority and the importance of peacefully operating within existing international cyber norms.[70] This thesis draws directly from Lewis's cyber definitions because they allow this study to

---

[67] Lewis, "Five Myths."

[68] Ibid.

[69] Lewis, "Protect U.S. Against Cyberwar."

[70] Zhu Feng, "China's Rise Will Be Peaceful: How Unipolarity Matters," in *China's Ascent: Power, Security, and the Future of International Politics*, ed. Robert S. Ross and Zhu Feng (Ithaca: Cornell University Press, 2008), 37, 54; Lewis, "Five Myths."

give a precise determination of how state-sponsored cyber espionage fits into PLA modernization. Lewis's work is also helpful to this thesis because it identifies cases of Chinese cyber espionage that potentially assisted PLA modernization.

Along similar lines, another group of scholars seeks to establish the standards for warfighting domains: Can China's actions in the cyberspace be categorized as cyber warfare if virtual reality is not a warfighting domain?[71] This group examines land, sea, air, and space domains in the context of wartime operations and discusses whether classifying cyberspace as a warfighting domain is plausible or unrealistic. U.S. government and DOD publications assert that cyberspace is a warfighting domain, while scholarly articles disagree.[72] Martin C. Libicki is one author who argues against the idea that cyberspace is a legitimate domain for information warfare operations.[73] Libicki concludes that while control over adversarial networks can disrupt communication channels and cause inconveniences to government operations, it does not constitute an act of war; therefore negating the claim that warfare can be conducted in cyberspace. Libicki supports his point by arguing that if cyberspace were a warfighting domain, then nations would respond to cyberattacks with kinetic strikes—but that has not happened.[74]

Libicki also argues that physical control over another nations' territory, as occurs in conventional warfighting domains, cannot be achieved through disruptive, data-damaging cyber operations.[75] But the important role of cyber espionage in China's warfighting capacity established in this thesis challenges the judgment that "cyberspace is not a warfighting domain."[76] Cyber espionage employs the same concepts, principles,

---

[71] Martin C. Libicki, "Cyberspace is not a Warfighting Domain," *Journal of Law and Policy for the Information Society* 8, no. 2 (2012): 321–22, http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4. Libicki.pdf; Segal, "Cyberspace: New Strategic Realm," 577.

[72] Catherine A. Theohary and Anne I. Harrington, *Cyber Operations in DOD Policy and Plans: Issues for Congress* (CRS Report No. R43848) (Washington, DC: Congressional Research Service, 2015, 1–2, fas.org/sgp/crs/natsec/R43848.pdf.

[73] Libicki, "Cyberspace is not Warfighting Domain," 322.

[74] Ibid., 321–22, 327, 332–333, 335.

[75] *Managing September 12th in Cyberspace: Hearing Before the Committee on Homeland Security, House of Representatives*, Cong., 1–2 (March 20, 2013) (statement of Martin C. Libicki, RAND, Office of External Affairs).

[76] Libicki, Cyberspace in not a Warfighting Domain," 321–22.

and objectives as traditional espionage; the only variance is in the application method. Consequently, to engage in a more precise analysis of the major research question, this thesis treats cyber espionage is a form of warfare, and the domain it is conducted in (cyberspace) as a warfighting domain.

Another category of literature examines China's cyber ambiguity to discuss the feasibility of deterrence in cyberspace: Is the ambiguity in China's cyber strategy China's virtual method of deterrence against Western nations, or is deterrence in the virtual realm even possible?[77] This thesis does not explore the intricacies of deterrence, in relation to the orientation of China's cyber strategy; however, this thesis does present ideas from this literature to bolster the study's interpretation of China's strategic cyber principles (ambiguity, deception, denial, etc.). Within cyber deterrence literature, one category of authors argues that the secrecy surrounding China's modern cyber strategy and military cyber operations is necessary for China to maintain standard military operations and deterrence against foreign adversaries.[78]

In contrast to the first debate, another group of scholars contends that foreign adversaries cannot be deterred if they do not have an idea of the potential capabilities a nation employs: in essence giving their cyber capabilities a level of credibility that they could inflict significant damage on an adversary.[79] Consequently, the ambiguity of Chinese cyber operations does not afford China a cyber-deterrent against adversarial nations because there are no indications of its true cyber capabilities. Scholars on this debate expand their argument to suggest the opaqueness of China's cyber strategy is just

---

[77] Mulvenon, "PLA Computer Network Operations," 257–58.

[78] Jian Zhang, "China's Defense White Papers: A Critical Appraisal." *Journal of Contemporary China* 21, no. 77 (May 2012): 884,892, doi: 10.1080/10670564.2012.684969; Phillip C. Saunders and Andrew Scobell, "Introduction: PLA Influence on China's National Security Policymaking," in *PLA Influence on China's National Security Policymaking*, ed. Phillip C. Saunders and Andrew Scobell (Stanford: Stanford University Press, 2015), 8; Stokes and Hsiao, *Countering Chinese Computer Operations*, 6.

[79] Jeffrey R. Cooper, "A New Framework for Cyber Deterrence," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 108–09, https://muse.jhu.edu.libproxy.nps.edu/books/9781589019195/9781589019195-13.pdf.

an inherent characteristic of the authoritarian Chinese communist government.[80] Additionally, within this literature, authors argue against cyber deterrence by highlighting the inherently ambiguous nature of the virtual domain. Authors contend that in order for nations to adequately deter other nations, they must have some idea of an adversary's intentions and motivations. Due to cyberspace's remote, disconnected nature, it disguises nations' intentions and motivations, which makes cyber deterrence unfeasible.[81]

The last group of literature broadly examines China's increased cyber espionage and rapid PLA modernization in the context of international relations and power transition theories: Are China's aggressive cyber intrusions indications for its future foreign policy objectives to overtake the United States as a world power? Or will China rise peacefully within existing international norms? Author Maria Hsia Chang notes, "The PLA is a growth industry, already the largest in the world in manpower."[82] There is no debate that China and the PLA's physical power bases are growing.[83] The extent of the PRC's rise, the PLA's long-term modernization strategy, China's strategic cyber orientation, and the ensuing ripple effects on the international order, are contested areas among international relations (IR) scholars.

This group of publications argues that China's foreign policy intentions aim to aggressively rise as a world power and cites cases of Chinese government-sponsored

---

[80] Beina Xu and Eleanor Albert, "The Chinese Communist Party," CFR Backgrounders, Council on Foreign Relations, last updated August 27, 2015, http://www.cfr.org/china/chinese-communist-party/p29443; Lindsay, "Impact of China on Cybersecurity: Fiction and Friction," 7–8.

[81] Jian, "China's Defense White Papers: Critical Appraisal," 883–84; Nan Li, "The PLA's Evolving Campaign Doctrine and Strategies," in *The People's Liberation Army in the Information Age* (Santa Monica, CA: RAND, 1999), 160, http://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF145/CF145.chap8.pdf.

[82] Maria Hsia Chang, *Return of the Dragon: China's Wounded Nationalism* (Boulder, CO: Westview Press, 2001), 7.

[83] Ashley J. Tellis, "The United States and Asia's Rising Giants," in *Strategic Asia 2011–2012: Asia Responds to its Rising Powers China and India*, ed. Ashley J. Tellis, Travis Tanner, and Jessica Keough (Seattle: The National Bureau of Asian Research, 2011), 4; Chang, *Return of the Dragon*, 7; John J. Mearsheimer, "China's Unpeaceful Rise," *Current History* 105, no. 690 (April 2006): 160, http://archives.cerium.ca/IMG/pdf/Chinas_Unpeaceful_Rise.pdf; M. Taylor Fravel, *Strong Borders, Secure Nation: Cooperation and Conflict in China's Territorial Disputes* (New Jersey: Princeton University Press, 2008), 1–2; Susan Shirk, China Fragile Superpower: How China's Internal Politics Could Derail its Peaceful Rise (Oxford: Oxford University Press, 2007), 39–41.

cyber espionage as evidence.[84] Realists like John W. Mearsheimer express one view on China's future international goals: China's rise to power will be aggressive and accompanied with conflict—to include cyber conflict.[85] Realists conclude that cyber espionage is an advantageous tool that gives China the edge in future power struggles. Additionally, realists argue that the increase in Chinese CNE and the PLA's offensive cyber orientation clearly support their claims.[86] Through the course of investigating the central research question, it is possible that evidence supporting certain IR theories may emerge and will subsequently be addressed in the conclusion.

D. POTENTIAL EXPLANATIONS AND RESEARCH DESIGN

In the last decade, numerous U.S. government- and DOD-sponsored reports have cited the overwhelming number of Chinese cyber espionage cases and the PLA's simultaneous, rapid modernization as evidence that China is aggressively rising as an international power.[87] These reports additionally outline the assumption that cyber espionage is the clear mechanism thrusting forward the PLA's advancement. As the literature review details, however, there are many potential explanations for China's aggressive CNE and cyber network attack (CNA): the forward leaning posture is because China's cyber strategy is "death by 1,000 cuts," so its high-volume aggressive attacks both damage U.S. power and increase China's power base; China's use of cyber espionage is not as damaging as U.S. reports suggest because China's cyber strategy is fragmented and decentralized; and China relies on cyber espionage as a central pillar of its cyber strategy because its domestic R&D and innovation are underdeveloped.

---

[84] Wylie McDade, "Attribution, Delayed Attribution and Covert Cyber-attack. Under What Conditions Should the United States Publicly Acknowledge Responsibility for Cyber Operations" (master's thesis, Naval Postgraduate School, Monterey, CA, March 2014), V, http://hdl.handle.net/10945/41417.

[85] Mearsheimer, "China's Unpeaceful Rise,"160; Chang, *Return of the Dragon*, 8.

[86] Anthony Capaccio and Terry Atlas, "China Advances Threaten Erosion of U.S. Edge, Pentagon Says," *Bloomberg Report*, May 8, 2015, http://www.bloomberg.com/news/articles/2015-05-08/china-advances-threaten-erosion-of-u-s-advantage-pentagon-says; Cordesman, Hess, and Yarosh, *Chinese Military Modernization*, 59–61; Leopold, "China's Military Calls for 'Online Great Wall.'"

[87] U.S.-China Economic and Security Review Commission, "Section 2: China's Cyber Activities," 244–45, 259; *Annual Report to Congress: 2015*, 22, 35; *Annual Report to Congress: 2014*, 35; Heginbotham et al., *U.S.-China Military Scorecard*, 24–25.

This potential explanation challenges U.S. Economic and Security Review Commission reports, DOD reports on "Military and Security Developments" in China, and U.S. think tank reports that make the key assumption that cyber espionage is the driver behind PLA modernization. Those reports do not provide the basis for their assumptions, and this study provides evidence to the contrary. This thesis investigates the role cyber espionage and CNE plays in advancing PLA modernization efforts: Does it have a central, complementary, or limited role in driving PLA modernization forward?

The resulting explanation from that question is that Chinese cyber espionage plays an observable role in PLA modernization. Its role, however, is complementary to other preexisting PLA acquisitions methods because China's cyber capabilities are not developed to the level at which they could consistently return intricate system details on military designs. There are also noted cases of modernized PLA military equipment that were purchased or reverse engineered through indigenous R&D efforts that support this explanation. Furthermore, this thesis expands on the original hypothesis to suggest that cyber espionage is not a primary tool for PLA modernization objectives.

To investigate this potential explanation, the research is presented in three phases. The first phase examines PLA modernization and how it progressed from 1978–2015; the second phase investigates China's cyber strategy, Chinese cyber actors, and the nature of China's cyber actions; and the third phase identifies specific examples of Chinese cyber espionage campaigns, and their potential connections to PLA modernization in order to determine how they are related. Additionally, the majority of this thesis's research relies on a comparison of PLA and U.S. military data due to the countries' similarity in size, cyber capabilities, and modern military functions.[88] Apart from Russia, there is no other nation with a relatively similar size, phase of development, modern military equipment,

[88] Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Virginia: Northrup Grumman, March 2012), 97–98, http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-066.pdf.

and cyber skills that would provide a useful comparison to China.[89] As a result, this thesis uses case studies of Chinese cyber intrusions on U.S. systems.

Since this thesis focuses on determining how government-sponsored cyber espionage fits into PLA modernization, the research and research findings differentiate between military cyber espionage and economic cyber espionage. Military cyber espionage, for the purpose of this thesis, refers to cyber espionage or virtual exploitation of military- and defense-related equipment, technology, or data.[90] In contrast, economic espionage primarily refers to cyber theft of economic, industrial, private corporation, or individual intellectual property and technologies.[91] This thesis concentrates on military cyber espionage. Throughout the course of the study, however, examples of economic espionage are cited as evidentiary support for this study's findings.

Comprehensively addressing how cyber espionage fits into PLA military modernization while relying exclusively on open-source information is a multifaceted challenge in the research. Historical, declassified government-accounts of military tactics in previous wars have been crucial for the insight they provide into countries' military strategies. Detailed current and future military strategies, however, typically remain classified above general public release for several decades, and cyber strategy is no exception. The inherently secretive and unsanctioned manner in which cyber espionage is conducted suggests, if there is literature regarding China's cyber espionage strategy, it will likely be several years before it is declassified for study.[92] Due to the classification constraints on first-hand sources, this thesis relies heavily on secondary sources for research. Additionally, first-hand Chinese-native, sources are often produced with the added influence of China's authoritarian conditions, which suggests their comparative value for this study would not be useful due to the high amount of propaganda they

---

[89] Cilluffo, *Cyber Threats from China, Russia, and Iran*, 12, 15; "Countries Ranked by Military Strength (2015)," Global Fire Power, last modified April 1, 2015, http://www.globalfirepower.com/countries-listing.asp.

[90] Cilluffo, *Cyber Threats from China, Russia, and Iran*, 12.

[91] Ibid.

[92] Jeffrey Engstrom et al., *China's Incomplete Military Transformation: Assessing the Weaknesses of the People's Liberation Army* (PLA) (Santa Monica, CA: RAND, 2015), 86, http://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR893/RAND_RR893.pdf.

contain. This study's research findings could need modification if the Chinese government-released information this thesis relies on is also inaccurate as part of government deception campaigns to disrupt adversary operations.[93] An additional limiting factor in this thesis is the language barrier. The author has limited knowledge and ability to translate Chinese language sources. Consequently, the thesis relies on translated Chinese works or scholarly secondary U.S. sources to provide the necessary information.[94]

Due to the relatively new and rapid evolution of cybersecurity and cyber warfare methods, this thesis primarily references recent publications (published from 2010–2015), to ensure the relevancy, accuracy, and timeliness of the information. Additionally, as a result of research design constrains, this thesis cites a majority of its research material through Annual Congressional Reports, think tank publications, Chinese Defense White Papers, and authors such as Lewis, Lindsay, Cheung, and Mulvenon.[95] This thesis also pulls quantitative data from recently published sources, to include Master's theses and U.S. government websites, due to the information being the most up-to-date.[96] Since this thesis addresses hypotheses primarily using military and security language, the previously listed sources also best support that effort. To obtain a comprehensive picture of modern PLA cyber capabilities versus cyber espionage operations, this thesis uses U.S. and Chinese media articles, government reports, and international publications to compile the data.

E. THESIS ORGANIZATION

In order to investigate how government-sponsored cyber espionage fits into PLA modernization, this thesis triangulates three areas for discussion: the path of China's cyber development throughout the course of PLA modernization, China's cyber strategy,

---

[93] Oakley, "China's Strategy to Dominate in Cyber Space," 14.

[94] Ibid., 15.

[95] Lindsay, "Introduction" 13–14; Lindsay and Cheung, "Exploitation to Innovation," 57–59, 61.

[96] Pembleton, "Assessing Technology Innovation in the PLA," v; Oakley, "China's Strategy to Dominate in Cyber Space," 16; Shannon Tiezzi, "China's Growing Defense Budget: Not as Scary as You Think," *Diplomat*, February 5, 2014, http://thediplomat.com/2014/02/chinas-growing-defense-budget-not-as-scary-as-you-think/; Krekel, Adams, and Bakos, *Occupying Information High Ground*, 97–98.

and how China employs cyber espionage. Consequently, Chapter II of this thesis provides the definitions for key cyber terminology—cyber warfare, cyber espionage, and cyberattack—to foster a common, foundational understanding for the rest of the thesis. Chapter III establishes the basis for China's cyber strategy by discussing PLA modernization in four distinct waves: this chapter outlines specific PLA modernization initiatives, developmental cyber programs, and the drivers behind them.

Chapter III sets the foundation for Chapter IV, which details the organization, tenents, and modes of operation the PLA uses to operate China's current CNO strategy. Chapter V gives an in-depth examination of case studies that detail historical Chinese cyber espionage operations, PLA acquisition methods, and developmental timelines of modernized PLA military equipment. Ultimately, Chapter VI discusses the implications Chinese cyber intrusions have on bilateral cyber agreements and discusses potential courses of action the United States could use to cultivate an appropriate counterstrategy. Finally, Chapter VI also presents avenues for future research that this thesis did not explore.

II. DEFINING KEY CYBER TERMS

A. TRADITIONAL ESPIONAGE VERSUS CYBER ESPIONAGE

The Oxford's English Dictionary defines espionage as "the practice of spying or of using spies, typically by governments, to obtain political and military information."[97] Nations have engaged in traditional espionage since the beginning of conventional warfare. Traditional espionage can be conducted physically by an agent of the government, a proxy, or a co-opted individual.[98] Those individuals use any means necessary to acquire data, information, or state secrets for an external entity. A notable example from U.S. history was former Central Intelligence Agency (CIA) employee Aldrich Ames who provided covert U.S. agent information to the Soviet Union in the Cold War.[99] Espionage is split into categorical types like military, political, or economic.

The U.S. Federal Bureau of Investigations (FBI) defines economic espionage as an individual consciously targeting, stealing, or acquiring trade secrets to intentionally aid a foreign individual, entity, or government.[100] Since the creation of the U.S. Economic Espionage Act (EEA), of 1996, the United States prosecuted over 124 cases of economic espionage.[101] One such example occurred over the course of 25 years: a Chinese-born citizen became an employee of the U.S. Aerospace Company Boeing and exfiltrated an enormous amount of technical data, schematics, and designs for U.S. military-contracted airframes back to China.[102] Even though the espionage target was

---

[97] "Espionage," Oxford Dictionaries, accessed October 7, 2015, http://www.oxforddictionaries.com/definition/english/espionage.

[98] Peter Toren, "A Look at 16 Years of EEA Prosecutions," Law 360, Portfolio Media, last modified September 19, 2012, http://www.law360.com/articles/378560/a-look-at-16-years-of-eea-prosecutions.

[99] Tim Weiner, "Why I Spied; Aldrich Ames," *New York Times*, July 31, 1994, http://www.nytimes.com/1994/07/31/magazine/why-i-spied-aldrich-ames.html.

[100] "Economic Espionage: Protecting American's Trade Secrets," Federal Bureau of Investigation, U.S. Department of Justice, accessed October 7, 2015, https://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage; Lindsay and Cheung, "Exploitation to Innovation," 57; Toren, "16 Years of EEA Prosecutions."

[101] "Economic Espionage: Protecting American's Trade Secrets"; Lindsay and Cheung, "Exploitation to Innovation," 57.

[102] Lindsay and Cheung, "Exploitation to Innovation," 57.

military data, the case was considered economic because the individual targeted a private U.S. corporation's trade secrets. While espionage is an offense punishable by death in many countries, it is not an act that can be used to initiate war. Studies of notable espionage cases in U.S. history have served to increase physical security measures, bolster background check requirements, proliferate employee training on espionage indicators, and make traditional espionage attempts more difficult. Consequently, a new, more accessible form of espionage has risen in the Information Age—cyber espionage.

Due to its ease-of-use, variance of applications, anonymity, and degree of separation for its users, cyber espionage is a popular substitute for traditional espionage.[103] Cyber espionage and traditional espionage have the same end goal: obtain, acquire, or steal information, data, or technology from a foreign entity to use the acquired information against the entity for personal, military, or economic gains. The difference in traditional and cyber espionage, however, comes down to practical application. Cyber espionage is conducted in the virtual domain using Internet, network, and cyber connections to acquire or steal critical information from foreign nations.

In other words, cyber espionage, cyber intrusions, and cyber spying are all acts of an adversarial power (whether government-sanctioned, military, private, or terrorist), stealing or acquiring another country's sensitive information, technology, or trade secrets through cyber means.[104] In contrast to traditional espionage, cyber espionage can be state-sponsored or conducted by individual actors, hacker groups, or private corporations with non-state-aligned goals. For example, China's non-government hacktivists conduct cyber espionage against domestic targets, foreign governments, military networks, and private businesses to benefit their personal and national objectives.[105]

Cyber espionage has brought about a new sense of fear in many nations across the world because of the inherent ambiguity of adversarial intentions, difficulty of

---

[103] Andres, "Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence," 91, 93–94.

[104] James A Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War, and Other Cyber Threats* (Washington, DC: Center for Strategic and International Studies, December 2002), 9, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

[105] Lindsay, "Introduction," 18.

attribution, and lack of legal framework to prosecute suspected cyber criminals.[106] With traditional espionage, if a spy is captured, there is an individual and often a host-nation to hold accountable. With cyber espionage, however, that is not always the case. Cyber hackers can conduct cyber espionage from any location outside of the targeted cyber objective. Skilled hackers can disguise their Internet Protocol (IP) addresses to prevent a targeted entity from attributing the attack to them or from discovering their location.

The high degree of anonymity in the virtual realm also increases the motivation for governments to conduct cyber espionage, because states cannot prosecute offenders without physical evidence and developed legal standards. An example demonstrating this point was the U.S. DOJ's indictment of five PLA officers for conducting CNE on U.S. industrial targets.[107] The PLA officers conducted the cyber intrusions outside the United States and were not extradited to the United States by China.[108] Similar to traditional espionage, cyber espionage can be broken down into different target categories.

In contrast to the United States, China has traditionally not acknowledged separate categories of cyber espionage targets. Cyber analyses have cultivated a common view on China, based on numerous government, defense, and media reports of increasing Chinese CNE on U.S. military, economic, and government targets without regard for economic sanctions or political blowback: that China views all data and information (whether military, political, or industrial) obtained from cyber espionage campaigns as acceptable and sanctioned targets under modern cyber warfare.[109] China does not have a similar record as the United States of upholding individual intellectual or private property

---

[106] Eugene Kaspersky, "The Most Sophisticated Cyber Espionage Campaign Ever—But Who's Behind it?" *Forbes,* February 25, 2015.

[107] "DOJ Brings first-ever cyber espionage case against Chinese Officials," *Fox News*, May 19, 2014, http://www.foxnews.com/politics/2014/05/19/doj-bringing-cyber-espionage-case-against-chinese-officials/; *Annual Report to Congress: 2015*, 54–55; Austin, "What the U.S. Gets Wrong."

[108] Ibid.

[109] Arthur Herman, "Edward Snowden enables Chinese Hack Attacks," *New York Post,* February 24, 2014, http://nypost.com/2014/02/24/chinas-military-hackers-can-thank-edward-snowden/; *Annual Report to Congress: 2015*, 39; U.S.-China Economic and Security Review Commission, "Section 2: China's Cyber Activities," 257–59.

rights because the majority of public holdings are state-owned.[110] The United States distinguishes between categories of cyber espionage targets, however, because it has a history of protecting U.S. citizen and private industry intellectual property rights.[111] Military cyber espionage exploits military applications, equipment schematics, personnel data, or strategic doctrines; economic cyber espionage targets private citizen, corporate, or intellectual property; political espionage manipulates government personnel, data, and operations information.[112] U.S. private industries make up a significant portion of the U.S.'s economic activity; increased cyber exploitation of their trade secrets has lowered the United States' overall domestic profits.[113] For this reason, the United States condemns economic espionage attacks and uses the EEA to indict individuals who commit economic cyber espionage.[114] This thesis distinguishes between military, economic, and political cyber espionage but primarily examines the effects of military cyber espionage under the umbrella of cyber warfare.

B. UNDER CYBER WARFARE'S UMBRELLA: COMPARING THE SPECTRUM OF CYBER APPLICATIONS

CSIS cyber expert James A. Lewis takes a firm stance on the differences between definitions of cyber espionage and cyberattacks, "China has not used force against the United States in cyberspace. What it has been doing is spying. And spying, cyber or otherwise, is not an attack or grounds for war."[115] This thesis takes a similar stance on Lewis's judgement toward the difference between cyber espionage and cyberattack. As Lewis suggests, however, cyber terms—cyber warfare, cyberattack, cyber espionage, and

---

[110] Peter K. Yu, "From Pirates to Partners: Protecting Intellectual Property in China in the Twenty-First Century," *American University Law Review* 50, no. 131 (2001): 133, https://www.wcl.american.edu/journal/lawrev/50/yu.pdf; Daniel C. Fleming, "Intellectual Property Rights in China," Wong-Fleming Attorneys at Law, accessed December 13, 2015, http://wongfleming.com/intellectual-property-rights-in-china/.

[111] Peter Toren, *Intellectual Property and Computer Crimes*, 4th ed. (New York: Law Journal Press, 2005), 1-2–1-6.

[112] Negroponte et al., "Open, Global, Secure, and Resilient Internet," ix.

[113] Ibid., 22; Obama, "Cybersecurity"; Obama, "Remarks by Obama and Xi"; Toren, "16 Years of EEA Prosecutions."

[114] Segal, "Shaming Chinese Hackers"; Negroponte et al., "Open, Global, Secure, and Resilient Internet," 5, 22; Obama, "Cybersecurity"; Obama, "Remarks by Obama and Xi."

[115] Lewis, "Five Myths." 37; Zhu, "China's Rise Will Be Peaceful," 37, 54.

cybersecurity—are used interchangeably in popular discourse, but the terms occupy different ends of the spectrum under cyber warfare.[116]

Cyber warfare is an important term to distinguish because it encompasses all exploitive cyber activities: cyber espionage, computer hackings, cyberattacks, computer network intrusions, information operations, and information deception.[117] Cyber warfare is a virtual method of warfighting that relies of cyber tools to carry out wartime or state objectives against an adversarial power. The U.S. Joint Chiefs of Staff define cyber warfare as, "An armed conflict conducted in whole or in part by cyber means."[118] Even though "armed conflict" is designated as a criteria of cyber warfare, the parameters for cyberattacks that would constitute "armed" cyber conflicts are not defined.

The United States frequently categorizes Chinese cyber espionage or cyberattacks on U.S. networks as punishable crimes, not warfare. For example, the United States attributed several CNE campaigns on U.S. industries to five PLA officers and pursued criminal indictments for them rather than taking military action against China.[119] Analyses on the subject suggest the United States employs that specific definition of cyberattack in order to avoid entering retaliatory conflicts.[120] This thesis, however, does not use "armed conflict" as a measure for cyber warfare. Cyber warfare is used as a term to discuss the range of exploitive cyber methods and applications employed by government or non-government entities to achieve a desired outcome. The key word in this definition is "exploitive." For this thesis, exploitation (in regards to cyber espionage)

---

[116] Lewis, *Assessing Risks of Cyber Terrorism*, 1; Jon R. Lindsay and Derek S. Reveron, "Conclusion: The Rise of China and the Future of Cybersecurity," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), 345–46.

[117] Lewis, *Assessing Risks of Cyber Terrorism*, 7–8.

[118] James E. Cartwright, *Attachment 1: Cyberspace Operations Lexicon*. DOD Memorandum on Joint Terminology for Cyberspace Operations. Washington, DC: Vice Chairman of the Joint Chiefs of Staff, 2010, 8, http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20 Cyberspace%20Operations.pdf.

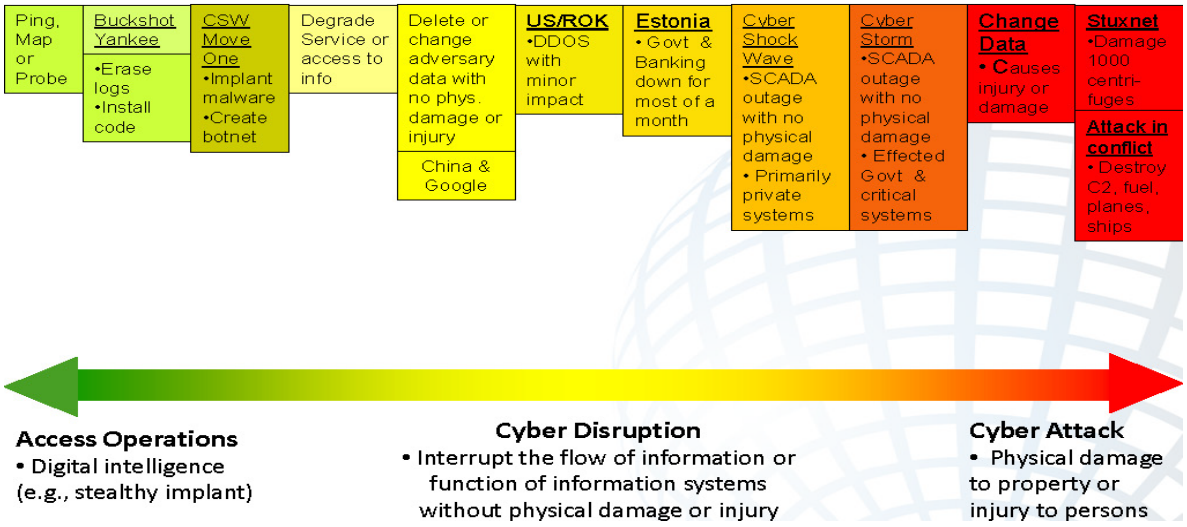
[119] Shannon Tiezzi, "U.S. Indicts 5 PLA Officers for Hacking, Economic Espionage," *Diplomat*, May 20, 2014, http://thediplomat.com/2014/05/us-indicts-5-pla-officers-for-hacking-economic-espionage/.

[120] "A New Kind of Warfare," *New York Times*, September 9, 2012, http://www.nytimes.com/2012/ 09/10/opinion/a-new-kind-of-warfare.html?_r=0.

refers to the unwilling, unknowing, and unauthorized targeting and subsequent exfiltration of objectives, information, or data by a hacker using cyber warfare means.

Within the range of activities included under cyber warfare (listed in the U.S. Cyber Command's Cyber Warfare Spectrum in Figure 1), cyber espionage is considered a benign intrusion and cyberattacks are considered kinetic strikes.[121] In this thesis, both cyberattacks and cyber espionage are considered subsets of cyber warfare operations.

Figure 1. The Spectrum of Cyber Warfare with Historical Examples Demonstrating the Range and Effectiveness of Cyber Activities



Source: "U.S. Cyber Command Presentation: Assessing Actions along the Spectrum of Cyberspace Operations," Public Intelligence, last modified August 26, 2013, https://publicintelligence.net/uscc-cyber-spectrum/.

Cyberattacks are the intentional use of networks, cyber applications, or malware to disrupt, deny, or physically harm to another individual's, entity's, or government's networks, servers, or cyber operations.[122] Cyberattacks can be singular, annoying

[121] "U.S. Cyber Command Presentation: Assessing Actions along the Spectrum of Cyberspace Operations," Public Intelligence, last modified August 26, 2013, https://publicintelligence.net/uscc-cyber-spectrum/.

[122] Cartwright, *Cyberspace Operations Lexicon*, 5–7.

instances like credit card, banking, or personal information theft; they can also be long-term malware attacks that are devastating to a foreign entity's electronics.[123]

Cyberattacks are distinguished by their severity and damage they cause to a target.[124] Since this thesis uses "exploitive" to define cyber warfare applications, cluttered annoyances like Spam emails do not exploit a target and therefore are not considered cyber warfare. Cyber intrusions, cyber espionage, and data exfiltration are on the lower, benign level of cyber warfare.[125] Cyber disruption—distributed denial of service (DDOS) or spearphishing—are mid-level cyber warfare operations.[126] CNA—like the Stuxnet computer virus—is on the higher level of cyber warfare.[127] In this thesis, cyberattacks refers to both cyber disruption and severely damaging attacks. Apart from distinguishing cyber tools' severity, it is also crucial, when referencing China's CNE, to differentiate between the actors that employ those applications.

C. CATEGORIZATIONS OF CYBER ACTORS: HACKER GROUPS AND INDIVIDUALS

1. Advanced Persistent Threats

In 2006, the U.S. Air Force coined the term "advanced persistent threat" (APT) to categorize suspected Chinese hacking groups that targeted U.S. servers.[128] Since cyber hacking proliferated across international borders, APT's meaning has also expanded across the world. APT now refers to any state or non-state sponsored hacking groups that have established records of exploitive, large-scale cyberattacks against particular targets—whether from Russia, China, or the United States.[129] Hacking groups are also

---

[123] Lewis, *Assessing Risks of Cyber Terrorism*, 8.

[124] Theohary and Harrington, *Cyber Operations in DOD Policy*, 3–5.

[125] "U.S. Cyber Command: Assessing Cyberspace Operations."

[126] Ibid.

[127] Ibid.; Theohary and Harrington, *Cyber Operations in DOD Policy*, 3–5.

[128] Lindsay and Cheung, "Exploitation to Innovation," 61; Lindsay, "Impact of China on Cybersecurity: Fiction and Friction," 20–21.

[129] Theohary and Harrington, *Cyber Operations in DOD Policy*, 6–7; Lindsay and Cheung, "Exploitation to Innovation," 57, 61; Cilluffo, *Cyber Threats from China, Russia, and Iran,* 12, 15; "APT 1," 2.

categorized as APTs when they employ developed, tailored malware coding in their cyberattacks that allows them to exploit a specific objective.[130] In 2013, Mandiant produced a cyber threat report that named Chinese PLA Unit 61398 (also known as the *Comment Crew)* as APT 1 based on its record of cyberattacks conducted against Western countries over several years.[131] Apart from non-state organized hacking groups, small paramilitary hacking organizations also play a role in cyber warfare operations.

2. Cyber and Information Warfare Militias

Standard military and cyber militias are formal, specialized, civilian-integrated units that are unique to the PLA and to China.[132] These contrast to the *ad hoc,* informal, non-military-affiliated reputation U.S. militias have had historically. The PLA is reliant on militias to supplement its general military functions.[133] Chinese militias operate under the PLA's command.[134] The militias are comprised of non-military volunteers and citizens in order to integrate the Chinese people into PLA affairs.[135] Additionally, militia members bolster PLA cyber, R&D, commercial, and educational development areas because a majority of the militia's civilians are recruited from private institutions.[136] PLA militias are further distinguished by their mission sets: "ordinary and primary."[137]

---

[130] Theohary and Harrington, *Cyber Operations in DOD Policy*, 7.

[131] "APT 1," 1–3, 7, 20; Nigel Inkster, "The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), 44; U.S.-China Economic and Security Review Commission, "Section 2: China's Cyber Activities," 243; Theohary and Harrington, *Cyber* Operations in DOD Policy, 7.

[132] Robert Sheldon and Joe McReynolds, "Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain,* ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), 186–90; Lindsay, "Introduction," 15, 18–19.

[133] Information Office of the State Council of the People's Republic of China, *China's National Defense* (Beijing: State Council, December 2004), http://en.people.cn/whitepaper/defense2004/defense2004.html; Krekel, *Capability of People's Republic to Conduct Cyber Warfare*, 33–34.

[134] Sheldon and McReynolds, "Civil-Military Integration and Cybersecurity," 193–94; Information Office of the State Council, *China's National Defense.*

[135] Sheldon and McReynolds, "Civil-Military Integration and Cybersecurity," 192; Information Office of the State Council, *China's National Defense.*

[136] Sheldon and McReynolds, "Civil-Military Integration and Cybersecurity," 191–93; Krekel, *Capability of People's Republic to Conduct Cyber Warfare,* 33–34.

[137] Information Office of the State Council, *China's National Defense*.

Ordinary units augment general military operations (administration and communications); primary militias have specialized functions like the PLA's cyber; intelligence, surveillance, and reconnaissance (ISR); and information warfare operations.[138] PLA cyber militias assist the PLA with conducting CNO, but specifically engage in cyber espionage, hacking, and cyberattacks. Since PLA cyber militias are primarily composed of non-military civilians, militia members maintain access to cutting-edge government and non-government malware, cyber warfare applications, and cyber hackers.[139] This thesis highlights the PLA's cyber militias to demonstrate the range of actors that contribute to China's government and non-government-sanctioned cyber espionage. Chinese underground hackers are additional cyber actors that must be distinguished because of their elevated presence in China and the virtual domain.

3. The Underground Hacking Economy

China's "underground hacking economy"[140] refers to unsanctioned cyber actions undertaken in secret by non-government entities for personal gain; it also references underground hacking's mass proliferation and profitability across China.[141] Since underground hackers are often unendorsed by the government, the individuals are considered cyber criminals; however, the Chinese government occasionally recruits underground hackers to bolster the PLA's cyber forces.[142] Hackers associated with China's underground hacking conduct CNA against government, military, and corporate objectives. Underground hackers (or "black hat hackers") do not all maintain a standard

---

[138] Information Office of the State Council, *China's National Defense*.

[139] Sheldon and McReynolds, "Civil-Military Integration," 192–93; Krekel, *Capability of People's Republic to Conduct Cyber Warfare*, 33–34.

[140] Ibid.

[141] Ibid.; Gao Yuan, "Good Guys Who Can Hack Like Internet Criminals," *China Daily*, September 25, 2014, http://www.lexisnexis.com.libproxy.nps.edu/lnacui2api/results/docview/docview.do?docLinkInd=true&risb=21_T22838833327&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T22838833331&cisb=22_T22838833330&treeMax=true&treeWidth=0&csi=401290&docNo=1; Omkar Sapre, "Cyber Underworld is on Path to Corporatisation," *Economic Times*, September 23, 2011, http://www.lexisnexis.com.libproxy.nps.edu/hottopics/lnacademic/; Libicki, Ablon, and Golay, *Markets for Cybercrime Tools*, ix, x.

[142] Jong-Chen, "U.S.-China Cybersecurity Relations"; Krekel, *Capability of People's Republic to Conduct Cyber Warfare*, 45–46.

level of capabilities because they utilize whatever means they can access.[143] Underground hackers are not always the perpetrators of cyberattacks: some exclusively design CNA malware, viruses, or coding and sell them to other hackers.[144] Since China's underground hacking has rapidly expanded, it is likely that underground entities also have a contribution to China's CNE—whether sanctioned or not. Apart from various hacking group terms, there are also terms that distinguish individual hackers.

4. Individual Hackers as Hactivists, Patriotic Hackers, White-Hat Hackers, and Cyberterrorists

Hactivists, patriotic hackers, white-hat hackers, and cyberterrorists are types of non-government and government-sanctioned individual hackers. Hactivist is a general term that describes hackers who—absent of government or military pressure—conduct cyber operations for their own utility, personal motivations, or political biases.[145] Hactivists choose their targets (sometimes at random) primarily based on their own preferences.[146] The next two terms (patriotic hackers and white-hat hackers) are considered types of hactivists because of the personal motivations that drive their cyber operations. The difference in the two lies in their employer.

Patriotic hackers ("netizens" in China) are hactivists attributed to a specific nation.[147] Patriotic hackers are typically not formally associated governments but can be government-employed. The primary motivation driving patriotic hackers is

---

[143] Krekel, *Capability of People's Republic to Conduct Cyber Warfare*, 41.

[144] Bien Perez, "Internet Attacks Raise Alert; Malware Strikes Mainland, Other Fast-moving Economies," *South China Morning Post*, September 18, 2007, http://www.lexisnexis.com.libproxy.nps.edu/hottopics/lnacademic/; Gao, "Good Guys Who Can Hack."

[145] Theohary and Harrington, *Cyber Operations in DOD Policy*, 6–7.

[146] "Virus Alert in Hacker War," *Herald Sun*, April 23, 2001, http://www.lexisnexis.com.libproxy.nps.edu/hottopics/lnacademic/.

[147] Sarah McKune, "'Foreign Hostile Forces': The Human Rights Dimension of China's Cyber Campaigns," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), 272; Mulvenon, "PLA Computer Network Operations," 277; Theohary and Harrington, *Cyber Operations in DOD Policy*, 9; Nigel Inkster, "China in Cyberspace," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 194–95, http://muse.jhu.edu/books/9781589019195/9781589019195-19.pdf.

nationalism.[148] Consequently, patriotic hackers' cyber targets are chosen based on their correlation to national security and development objectives. At times, these hackers' extreme nationalism drives them to conduct retaliatory cyberattacks against nations that threaten their home country's security.[149] An example of a patriotic hacking was the high volume Chinese government and non-government cyberattacks on U.S. and Taiwanese government servers following the Taiwan Straits Crisis in 2004.[150] Apart from patriotic hackers, there is also a designator for government-sponsored hackers.

"White-hat" hackers are so named because of their affiliation with a specific national government. In contrast to underground, non-sanctioned "black-hat" hackers, white-hat hackers are government employees who conduct government-sanctioned cyber operations.[151] White-hat hackers can be military, bureaucratic, or government-employed. Similar to patriotic hackers, white-hat hackers' targets are in line with domestic government, military, and national security objectives. Specific motivational themes do not necessarily drive their cyber operations because the government directs them. In China, white-hat hackers are frequently used to assist domestic cybersecurity, bolster information censorship controls, and combat hactivists targeting China's networks.[152]

The last form of individual hackers—cyberterrorists—are similar to traditional terrorists but employ cyber applications to accomplish their objectives. Lewis defines cyberterrorism as, "the use of computer network tools to shut down critical national infrastructures…or to coerce or intimidate a government or civilian population."[153] Cyberterrorists are motivated by religious or ideological purposes and conduct cyberattacks to recruit for their organizations and spread propaganda.[154] This thesis does not touch on cyberterrorism, but cyberterrorists are important to distinguish because of

---

[148] Mulvenon, "PLA Computer Network Operations," 253, 277–78.

[149] Ibid., 277–78.

[150] Ibid., 255–56, 277–78.

[151] Gao, "Good Guys Who Can Hack."

[152] Ibid.

[153] Lewis, *Assessing Risks of Cyber Terrorism*, 1.

[154] Ibid.; Theohary and Harrington, Cyber Operations in DOD Policy, 7.

their prominence on global networks. Of the various types of hackers noted in this section, China routinely employs patriotic hackers to assist with PLA modernization and informationization goals. Since China's cyber strategy is largely modeled around the core tenet of "informationization," it is also crucial to define this term for this study.

D. INFORMATIONIZATION

"Informationization" and "informationized" are terms widely used by the CCP and to describe China's transition into a modern technologically capable country. "Informationization" references the incorporation of communications and information technology (IT) equipment into the domain that it concerns.[155] For example, if a report discusses the informationization of public education, it signifies the integration of communication and IT into public education sectors. The term does not just represent physical equipment: it also represents the technical skills and expertise needed to operate that equipment.[156] Informationization is not exclusive to military, government, or bureaucratic domains. It can be (and has been) used to reference developmental objectives in Chinese economic, education, business, and corporate enterprise domains as well.[157] An example that demonstrates this definition is when the CCP announces that it will informationize its military forces as part of PLA modernization. This statement means the CCP aims to equip the PLA with high-tech military weapons, advanced cyber capabilities, and modern technical training.[158] In order to determine the role cyber warfare and cyber actors play in PLA modernization, the next chapter discusses how PLA modernization and China's cyber missions have progressed since 1978.

---

[155] Stokes and Hsiao, *Countering Chinese Computer Operations*, 3–4.

[156] Jianbin Jin and Chengyu Xiong, "Digital Divide in National Informationization Quotient: The Perspective of Mainland China" (paper, International Conference on the Digital Divide: Technology & Politics in the Information Age, Beijing, PRC, 2002), 1–2, http://unpan1.un.orgintradoc/groups/public/documents/apcity/unpan046441.pdf.

[157] "Full Text: White Paper on the Internet in China," *China Daily*, June 8, 2010, http://www.lexisnexis.com.libproxy.nps.edu/hottopics/lnacademic/.

[158] Ibid.; "China Sets Strategic Plans for National Defence, Armed Forces," *BBC Worldwide Monitoring*, January 20, 2009, http://www.lexisnexis.com.libproxy.nps.edu/hottopics/lnacademic/.

III. PLA MODERNIZATION MEETS INFORMATIONIZATION

Since 1978, domestic and international events have affected the scope, pace, and focus of PLA modernization; these events guided the PLA away from its traditional focus on conventional forces, toward informationized military branches. China's responses to internal and external incidents are observable through specific time periods and waves of the PLA's development. The first wave of modernization occurred from 1978–1988; the second wave followed from 1989–1996; the third wave happened in 1997–2003; and the fourth wave occurred from 2004–2015. Each wave demonstrated unique fundamental shifts in the CCP's and PLA's strategic thinking, national priorities, and postures toward the international community. The PLA modernization periods built upon each other to transform the PLA from an underdeveloped military into a semi-modern force.[159] This chapter discusses the path of development for China's modern cyber strategy and also shows China's establishment of distinct cyber missions—like cyber espionage. This chapter establishes the foundation for China's cyber strategy (discussed in Chapter IV). This chapter's examination of modernization initiatives during key time periods—to include fielding a modern cyber strategy—also highlights the correlation between China's introduction of modern military applications and increased CNO.

A. THE FIRST WAVE: PLA MODERNIZATION FROM 1978–1988

The years 1978–1988 saw the initial wave of PLA modernization that introduced important foundational concepts that future modernization waves built upon: technological acquisitions processes, conventional force reductions, technical skill and professional development training, and an indigenous R&D platforms for military technologies.[160] In 1978, Chinese Premier Deng Xiaoping agreed PLA modernization

[159] Saunders and Scobell, "Introduction: PLA Influence," 2, 24, 26–27.

[160] Ibid., 6.

was critical, but prioritized it beneath China's domestic economic development.[161] From 1978–1988, Deng made significant cuts to the PLA's conventional force numbers and reduced the PLA's spending by approximately four percent of China's gross domestic product (GDP).[162] Deng's decreased emphasis on the military and the military's reduced budget actually became an advantage to the PLA in its modernization endeavors: the PLA had to develop a cost-effective, robust acquisitions system to update the military and supplement its previous government assistance.[163]

The early PLA modernization initiatives of the 1970s that stressed force restructuring, indigenous R&D development, and military training reform, continued into the 1980s.[164] Initial modernization efforts not only assembled a leaner, cost-effective force but also created an autonomous, business-like atmosphere in the PLA.[165] In order for the PLA to follow the CCP's orders and modernize amidst its second-hand prioritization, it had to join China's economic vigor and become an independent player in China's economy. The PLA's self-sufficient, new economic role kept its advancement on par with China's rapid economic growth until the late 1980s.[166] From 1985–1990, however, the PLA's modernization slowed. There were key events from 1989–1996 that revived the CCP's urgency to modernize the military at a rapid rate: these events highlighted the PLA's inferiority and underdevelopment force—compared to nations across the world.

---

[161] Andrew J. Nathan and Andrew Scobell, *China's Search for Security* (New York: Columbia University Press, 2012), 280–82, 284–86; Kenneth Allen, "Introduction to the PLA's Administrative and Operational Structure," in *The People's Liberation Army as Organization: Reference Volume v1.0*, ed. James C. Mulvenon and Andrew N. D. Yang (Santa Monica, CA: RAND, 2002), 20, http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2008CF182part1.pdf; Dennis J. Blasko, *The Chinese Army Today: Tradition and Transformation for the 21st Century* (New York: Routledge, 2006), 4–5.

[162] Heginbotham et al., *U.S.-China Military Scorecard*, 24–25; Saunders and Scobell, "Introduction: PLA Influence," 5, 8, 24.

[163] Saunders and Scobell, "Introduction: PLA Influence," 5.

[164] Ibid., 2.

[165] Ibid., 31, 34, 37; Nathan and Scobell, *China's Search for Security*, 282–88, 291–93; Allen, "Introduction to the PLA's Administrative," 12.

[166] June Teufel Dreyer, "Washington Contemplates the Chinese Military," Foreign Policy Research Institute, last modified September 2015, http://www.fpri.org/docs/dreyer_-_chinas_military.pdf.

B. THE SECOND WAVE: PLA MODERNIZATION FROM 1989–1996

The second wave of PLA modernization from 1989–1996 was significant because its international events shifted the CCP's priorities from economic-based to dual military- and economic-focused. The Soviet Union's collapse in 1989, the Gulf War in 1991, and the Taiwan Straits Crisis in 1996 were critical events that reasserted PLA modernization as a central pillar in China's developmental agenda.[167] In the second wave, there was also a noticeable change in PLA doctrines: military strategy shifted from conventional land battles to informationizing warfighting. The collapse of the Soviet Union in 1989–1991, deeply impacted PLA modernization because the Soviet Union offered China a great amount of assistance during its developmental decades.

During periods in 1950–1980, the Soviet Union provided the PLA aid, training, and technical advisement.[168] The CCP knew it could request military assistance from the Soviet Union at any time, so there was no urgency to modernize while China had the Soviet Union as a key resource.[169] The Soviet Union's dismantlement ended that type of CCP thought. The Soviet collapse introduced an insecurity to the CCP that foreign assistance had been a crutch for the PLA. The PLA's overreliance on Soviet assistance had left its forces underdeveloped. The CCP also believed that its communist rule could just as easily be overturned (like the Soviets) if the party did not strengthen its standing in the international community with a strong military force.[170] The Gulf War only added to

---

[167] Nathan and Scobell, *China's Search for Security*, 279, 288–89; Dorothy E. Denning, *Information Warfare and Security* (Massachusetts: ACM Press Books, 1999), 8–9, 193; Heginbotham et al., *U.S.-China Military Scorecard*, 25; Inkster, "Chinese Intelligence Agencies," 35.

[168] Nathan and Scobell, China's Search for Security, 278, 280–85; Allen, "Introduction to the PLA's Administrative," 18–19; Inkster, "Chinese Intelligence Agencies," 30; Kenneth W. Allen, Glenn Krumel, and Jonathan D. Pollack, *China's Air Force Enters the 21st Century* (Santa Monica, CA: RAND, 1995), 156–61, http://www.rand.org/pubs/monograph_reports/MR580.html.; Heginbotham et al., *U.S.-China Military Scorecard*, 23–24; Andrew Scobell, Michael McMahon, and Cortez A. Cooper III, "China's Aircraft Carrier Program: Drivers, Developments, Implications," *Naval War College Review* 68, no. 4 (Autumn 2015): 70, https://www.usnwc.edu/getattachment/c96be200-d3a9-4b6f-9114-179169fa844e/China-s-Aircraft-Carrier-Program--Drivers,-Develop.aspx.

[169] Heginbotham et al., *U.S.-China Military Scorecard*, 23–24.

[170] Ibid., 25–26.

the CCP's insecurities. The United States' weaponry in the Gulf War demonstrated just how technologically inferior the PLA was compared to advanced Western militaries.[171]

In the 1991 Gulf War, the U.S. military's technology, interventionism, and immediate defeat of Saddam's large conventional force were factors that caused significant concern for the CCP. One example of superior U.S. military technology in Iraq was the United States' preemptive installation of malware programs onto Iraqi air-defense systems prior to the war's outbreak.[172] After the war began, the United States triggered the malware allowing the U.S. military to bypass Iraq's malfunctioning air-defense system and defeat Iraqi troops.[173] The CCP also perceived the U.S.'s decisive defeat of Saddam's army as a warning that the U.S. military could do the same to the PLA.[174] The PLA had not yet encountered exploitive cyber warfare applications like the United States used in Iraq. Consequently, the PLA had no modern cyber defenses against the United States if it did go to war with China. The U.S. military's cyber tactics in the Gulf War accentuated the PLA's technological inferiority to the United States. The Gulf War also highlighted the cyber warfighting capabilities the PLA needed to develop. As a result, the CCP put pressure on the PLA to rapidly modernize its technological skills, which would decrease its vulnerability to cyberattacks.[175]

In response to the Gulf War, the CCP and PLA made outwardly visible changes that showed their shift in focus from conventional forces to modernized capabilities. In 1994, the CCP allowed the Internet into China, and sanctioned public Internet access in 1996.[176] The Internet's vast store of information had the ability to erode the CCP's

---

[171] Ye Zheng, "From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), 127; Pollpeter, "Chinese Writings on Cyberwarfare," 145–46; Li, "PLA's Evolving Campaign," 146.

[172] Ye, "Cyberwarfare to Cybersecurity in Asia-Pacific," 127; Pollpeter, "Chinese Writings on Cyberwarfare," 145–46.

[173] Ye, "Cyberwarfare to Cybersecurity," 127.

[174] Heginbotham et al., *U.S.-China Military Scorecard*, 36; Inkster, "Chinese Intelligence Agencies," 36; Ye, "Cyberwarfare to Cybersecurity," 127.

[175] Lindsay, "Introduction," 8.

[176] Nina Hachigian, "China's Cyber-Strategy," *Foreign Affairs* 80, no. 2 (March-April 2001): 119, http://www.jstor.org/stable/20050069; Inkster, "China in Cyberspace," 191.

single-party rule but modern technology development and electronic integration in the military became more important. Additionally, in 1995, Chinese Premier Jiang Zemin introduced a key doctrinal shift in the PLA's warfighting strategy, which is still used with minor variation in modern PLA writings: the PLA must prepare "to fight and win local wars under modern, high-tech conditions."[177] Jiang's doctrinal guidance necessitated that the PLA develop information warfare strategies—like those used by the United States in the Gulf War.[178] Those initial developments also thrust forward the rapid development of domestic Internet censorship, which added further complexity to PLA modernization.[179]

The Taiwan Straits Crisis in 1996 was arguably the most influential event in the second wave because it invigorated the CCP's urgency to modernize the military. The crisis also emphasized the U.S.'s global reach, willingness to intervene in international affairs, and superior technological capabilities.[180] Since 1949, the CCP has viewed political reunification with Taiwan and Taiwanese dissidence as top domestic issues.[181] The Taiwan Straits Crisis in 1996 also fell under that category. Taiwan pursued independent elections, which complicated its diplomatic situation with mainland China.[182] China sought to unilaterally prevent this signal of Taiwanese dissidence by intervening with the PLAN.[183] The United States, however, previously guaranteed Taiwan protection against Chinese aggression and used U.S. naval forces to intervene in the conflict.[184] China's naval capabilities (specifically ballistic missile technology) could

---

[177] The term "high-tech" was replaced with "Informationization"; David M. Finklestein, "China's National Military Strategy: An Overview of the 'Military Strategic Guidelines,'" *Asia Policy*, no. 4 (July 2007): 69, 71–72, http://muse.jhu.edu/journals/asia_policy/v004/4.finkelstein.pdf.

[178] Ball, "China's Cyber Warfare Capabilities," 81–82.

[179] Hachigian, "China's Cyber-Strategy," 119.

[180] Heginbotham et al., *U.S.-China Military Scorecard*, 25–27.

[181] Gary D. Rawnsley, "Old Wine in New Bottles: China-Taiwan Computer-based 'Information Warfare' and Propaganda," *International Affairs* 81, no. 5 (October 2005): 1062, http://www.jstor.org/stable/3569075.

[182] Lindsay, "Introduction," 17–18.

[183] Ibid.; Heginbotham et al., *U.S.-China Military Scorecard*, 25.

[184] Heginbotham et al., *U.S.-China Military Scorecard*, 25.

not compete with that of the United States.[185] Consequently, the CCP could not discredit U.S. naval forces and unilaterally handle an event it viewed as a domestic priority—Taiwan. The crisis demonstrated to China and the rest of the world how underdeveloped the PLA was—causing the CCP to emphasize multifaceted military, economic, and technological development, versus its previous economic-focused initiatives.[186]

During the second wave, the CCP also made minor strides in physical implementation of PLA modernization. These strides reemphasized early modernization themes of reduced force numbers, rapid development, and advanced technologies.[187] The CCP's Information Office also created the strategic parameters for what would be the PLA's modern cyber strategy.[188] In addition, the PLA's defense budget rose from one percent to 1.3 percent of China's annual GDP.[189] The PLA also introduced joint-branch mission execution strategies to supplement lacking technological capabilities in any force. The release of joint mission doctrines was a key development because it moved the PLA away from its traditional, compartmentalized top-down organization.[190] The international events that occurred during the second wave accelerated the PLA's development of modern military technology and robust cyber warfighting capabilities because China needed defenses against the U.S.'s superior technology.

C. THE THIRD WAVE: PLA MODERNIZATION FROM 1997–2003

The third wave was a critical period for the PLA's rapid modernization strategies, robust acquisition methods, and initial cyber strategy because these initiatives were the CCP's solution to PLA vulnerabilities exposed during the second wave.[191] In contrast to

---

185 Ibid., 25–27.

186 Heginbotham et al., *U.S.-China Military Scorecard*, xx, 16, 25–26, 28, 129.

187 Blasko, "Maritime Missions Require a Change," 3–4.

188 "Document: China's Military Strategy"; Dennis J. Blasko, "The 2015 Chinese Defense White Paper on Strategy in Perspective: Maritime Missions Require a Change in the PLA Mindset," *China Brief* 15, no 12 (June 2015): 3, 6, http://www.jamestown.org/uploads/media/China_Brief_Vol_15_Issue_12_1.pdf.

189 Heginbotham et al., *U.S.-China Military Scorecard*, 24–26.

190 Ibid., 25–26.

191 Ibid., 24–27.

the first and second waves, the third wave had a wider span of modernization implementation across the entire PLA. This section divides third wave developments into categorical types to discuss the PLA's transition into an informationized force.

1. Defense White Papers as Doctrinal Guidance for PLA Modernization

The release of China's biannual Defense White Papers (DWP) in 1998 was the first indication to the international community that the CCP adopted modern strategic thought.[192] Even though the white papers do not provide details on PLA missions, the papers give insight into China's national defense goals, the CCP's international priorities, and the PLA's path of advancement.[193] In the 1998 white papers, the CCP introduced the PLA's "active defense" strategy.[194] The strategy asserts that the PLA will use R&D and acquisitions to cultivate a technically skilled force that can accomplish two core objectives: be able to retaliate against enemies that attack China first and use a first-strike policy to gain an advantage over enemies.[195] The Active Defense Strategy appeared to be a subtle response to the Taiwan Straits Crisis in 1996. It also acted as a notification to foreign naval forces in the Pacific that China would assert control over the South China Sea.[196] The DWPs demonstrated the CCP's commitment to reinforce PLA modernization efforts. Additionally, much like the second wave of PLA modernization, there were key events that fueled the development of other PLA initiatives during the third wave.

---

192 Jian, "China's Defense White Papers: Critical Appraisal," 881, 883–84; Blasko, "Maritime Missions Require a Change," 3, 6.

193 "Document: China's Military Strategy"; Blasko, "Maritime Missions Require a Change," 3, 6; Nathan Beauchamp-Mustafaga and Peter Wood, "In a Fortnight," *China Brief* 15, no. 12 (June 2015): 1, http://www.jamestown.org/uploads/media/China_Brief_Vol_15_Issue_12_1.pdf; Jian, "China's Defense White Papers: Critical Appraisal," 886.

194 Jian, "China's Defense White Papers: A Critical Appraisal," 881, 883; Blasko, "Maritime Missions Require a Change," 3–4, 6.

195 Ibid.

196 James R. Holmes, "Island Chains Everywhere," *Diplomat*, last modified February 11, 2011, http://thediplomat.com/2011/02/island-chains-everywhere/; Robert D. Kaplan, "The Geography of Chinese Power: How Far Can Beijing Reach on Land and at Sea?" *Foreign Affairs* 89, no. 3 (2010): 33, http://www.jstor.org/stable/25680913.

2. International Events Thrusting forward Modernization Efforts

The 1999 U.S.-led North Atlantic Treaty Organization (NATO) bombing campaign in Yugoslavia, and the 2001 EP-3 aircraft collision were key third wave events that affected PLA modernization because they reinforced the CCP's decision to rapidly develop PLA cyber capabilities.[197] In 1999, the United States unintentionally bombed a Chinese Embassy in Belgrade—using precision-guided bombs—during NATO intervention in Yugoslavia.[198] This event fueled the CCP's insecurities (much like the Gulf War and U.S. intervention in the Taiwan Straits Crisis) that the United States would continually undermine the CCP's authority.[199] In response to the incident, Chinese government, military, and individual hackers conducted high volume, overlapping cyber intrusions on U.S. and NATO networks.[200] The retaliatory nature of the cyber operations highlighted the PLA's implementation of its modern strategic guidance, and the PLA's experimentation with modern information warfighting operations.

In 2001, the collision of a U.S. EP-3 reconnaissance aircraft into a Chinese fighter jet was another event that thrust forward the physical development of all PLA branch missions—to include cyber.[201] This incident was critical to PLA modernization because it demonstrated the PLA's inferior cyber capabilities in relation to that of the U.S. military. In response to the EP-3 crash, Chinese hackers again flooded U.S. government networks; the difference in this situation, however, was that the United States conducted retaliatory cyber intrusions.[202] The CCP and the PLA recognized the U.S.'s superior technical skills and molded their modern cyber strategy to defend against it. The PLA would use inferior cyber means with a modern cyber strategy, cyber espionage, and ISR

---

[197] Lindsay, "Introduction," 18; Heginbotham et al., *U.S.-China Military Scorecard*, 25.

[198] Lindsay, "Introduction," 18; Mulvenon, "PLA Computer Network Operations," 255; Krekel, *Capability of the People's Republic*, 67–68.

[199] Krekel, *Capability of the People's Republic*, 67–68.

[200] Ibid.; Ball, "China's Cyber Warfare Capabilities," 81–82, 95.

[201] Krekel, *Capability of the People's Republic*, 68–69; Mulvenon, "PLA Computer Network Operations," 255.

[202] Krekel, *Capability of the People's Republic*, 38, 68–69.

to overcome U.S. superiority in the virtual domain.[203] To bolster PLA defenses against future cyber confrontations, China's Academy of Military Sciences (AMS) also adopted a forward-leaning stance toward advancing the PLA's cyber capabilities.

3. Adopting a Modern Chinese Cyber Strategy

a. The Chinese Academy of Military Sciences' Cyber Experimentation

During the third wave, AMS researched and established the foundation for China's cyber strategy and cyber operations.[204] AMS is China's premier military institution, responsible for cutting-edge research on emerging strategic trends and military operations.[205] The shift in relative emphasis AMS research from conventional to cyber strategies also demonstrated the spread of modernized strategic thinking throughout the PLA. Prior to 1999, AMS military experts used their studies on Western military cyber operations to theorize about potential Chinese cyber strategies. After 1999, however, AMS began to put those theories into practice by testing CNA methods under China's Information Warfare doctrine.[206] AMS expanded its research to field-test military cyber units for the PLA.[207] Additionally, from 1999–2000, AMS simultaneously introduced government-sponsored cyber hackers and integrated civilian cyber militias to conduct a range of internal and external cyber missions.[208] AMS's experimentation was critical because the PLA's continues to employ similar entities with overlapping cyber missions as part of China's modern cyber strategy.

---

[203] Jian, "China's Defense White Papers: Critical Appraisal," 884, 892; Li, "PLA's Evolving Campaign," 146–47.

[204] Mulvenon, "PLA Computer Network Operations," 254, 275.

[205] Ibid.

[206] Pollpeter, "Chinese Writings on Cyberwarfare," 145; Ball, "China's Cyber Warfare Capabilities," 81–82.

[207] Sheldon and McReynolds, "Civil-Military Integration and Cybersecurity," 194–95; Lindsay, "Introduction," 10, 18–19.

[208] Ibid.; Information Office of the State Council, *China's National Defense.*

AMS's cyber research efforts even progressed the PLA's personnel recruitment methods.[209] Once AMS's initial testing and cyber application research was complete, AMS recommended that the PLA recruit technically capable, computer-savvy individuals from Chinese universities.[210] These individuals filled the fundamental positions for the PLA's modern cyber strategy and pioneered the use of modernized cyber tactics (cyber espionage and cyberattack) in the PLA.[211] By 2001–2002, the first reports emerged detailing Chinese cyberattacks against U.S. government servers, Chinese dissidence organizations, neighboring East Asian countries, and Tibetan networks.[212] Available information on early Chinese cyber intrusions suggests the targets were pursued primarily for political and national security purposes; however, that does not discount the notion that the obtained information could have also been used to supplement PLA modernization efforts.[213] The enormous strides the PLA made to cultivate modern cyber warfare abilities demonstrated the PLA's transition from a conventional-focused military to an informationized force.[214]

b. Document 27 Emerges as the Blueprint for China's Cyber Strategy

In 2003, China made a noticeable move to solidify its strategic views on cyber by publishing "Document 27" (also known as the State Informationization Leading Group [SILG] 2003 Opinion document).[215] Document 27 was China's first formal strategic cyber document and is still used today.[216] Document 27 is the blueprint for China's cybersecurity and provides the parameters for China's cyber strategy, cybercrime

---

[209] Krekel, Adams, and Bakos, *Occupying Information High Ground*, 51; Lindsay and Cheung, "Exploitation to Innovation," 64; Ball, China's Cyber Warfare Capabilities," 81–82, 94.

[210] Sheldon and McReynolds, "Civil-Military Integration and Cybersecurity," 194–95; Heginbotham et al., *U.S.-China Military Scorecard*, 34.

[211] Ibid.

[212] Ball, China's Cyber Warfare Capabilities," 96; Doug Naime, "State Hackers Spying on Us, Say Dissidents," *South China Morning Post*, September 18, 2002, http://www.scmp.com/article/391734/state-hackers-spying-us-say-dissidents.

[213] Ball, "China's Cyber Warfare Capabilities," 96.

[214] Sheldon and McReynolds, "Civil-Military Integration and Cybersecurity," 194–95.

[215] Lindsay, "Introduction," 8.

[216] Ibid.

investigations, and the Multilevel Protection Scheme (MLPS) for critical infrastructure.[217] Since Document 27's release, the SILG has not published a new cybersecurity documents, despite advancements in IT and the international environment: they only supplemented the document with policy updates that were responsive to national security issues or CCP priorities.[218] In 2003, Document 27 was not fully developed (compared to similar documents in Western nations), but its emergence demonstrated the targeted cyber modernization efforts the PLA made in the third wave.

4. Physical Modernization Developments

Even though the third wave was primarily dedicated to modernizing the PLA's warfighting strategies and cyber capabilities, there were still physical developments in the realm of informationized modernization that took effect. In 1997 and 2003 the PLA undertook massive personnel reductions to lower its conventional force numbers and create budgetary room for the PLA to refine its cyber and R&D platforms.[219] In 1999, the PLA also began to exercise modern acquisitions methods: the PLA attempted to procure an Israeli Airborne Early Warning system (AEW).[220] Consequently, the United States blocked the sale of the AEW to China, and the PLA used indigenous R&D to produce an AEW system.[221] In 1999, China also opened procurement channels with Russia to acquire four destroyer ships that could fire long-range cruise missiles that depended on overcoming significant command and control (C2) and ISR challenges.[222] The PLA's attempts to purchase modern AEW and naval technology demonstrated its development of non-cyber acquisitions systems—which helped the PLA modernize its military equipment in the fourth wave

---

[217] Lindsay, "Introduction," 8.

[218] Adam Segal, "China Moves Forward on Cybersecurity Policy," *Diplomat*, July 25, 2012, http://thediplomat.com/2012/07/china-moves-forward-on-cybersecurity-policy/; Lindsay, "Introduction," 8, 11–12.

[219] Saunders and Scobell, "Introduction: PLA Influence," 2, 16, 26–27; Blasko, "Maritime Missions Require a Change," 4.

[220] Heginbotham et al., *U.S.-China Military Scorecard*, 98.

[221] Ibid.

[222] Ibid., 30.

D. THE FOURTH WAVE: PLA MODERNIZATION FROM 2004–2015

The fourth wave of PLA modernization was the rapid, multifaceted physical implementation phase for the PLA's transition into a modern military force. By 2004, the PLA had already fielded a functional cyber mission, conducted successful cyber intrusions, and altered its strategic cyber warfare guidance to reflect the high-tech posture other militaries adopted around the world. Immediately in the beginning of the fourth wave, however, international events again served as an accelerant for the pace of the PLA's equipment modernization initiatives.

Similar to the previous waves of modernization, the fourth wave saw three international events simultaneously thrust forward PLA modernization and China's robust cyber strategy. In 2004, another Taiwan Straits Crisis erupted with Taiwan's introduction of independent elections.[223] The CCP did not support Taiwan's independence campaigns, or the U.S.'s diplomatic intervention that came with the 2004 elections.[224] As a result the CCP pushed forward PLAN technology, CNE, and military cyber intrusions to better prepare for any complications resulting from future Taiwanese independence demonstrations. Apart from the developments in the Taiwan Straits, the Stuxnet virus incident also had an effect on the course of PLA modernization.[225]

The 2010 Stuxnet virus was critical for China (and the entire world) because it was the first demonstration of cyber warfare that could remotely inflict physical damage on another country.[226] The Stuxnet virus impaired an entire Iranian uranium enrichment plant, which had not been done before.[227] Similar to the malware the United States

---

[223] Lindsay, "Introduction," 18; International Crisis Group (ICG), "China and Taiwan: Uneasy Détente," *Asia Briefing*, no. 42 (September 2005): 1, 3–4, http://www.crisisgroup.org/~/media/Files/asia/north-east-asia/taiwan-strait/b042_china_and_taiwan_uneasy_detente.pdf.

[224] International Crisis Group, "China and Taiwan: Uneasy Détente," 3–4.

[225] Lindsay, "Introduction," 12; Jon R. Lindsay, "Stuxnet and the Limits of Cyberwarfare," *Security Studies* 22, no. 3 (2013): 365, doi: 10.1080/09636412.2013.816122.

[226] Libicki, "Cyberspace is not Warfighting Domain," 329; Lindsay, "Stuxnet and the Limits of Cyberwarfare," 365–66; "Significant Cyber Incidents Since 2006," Center for Strategic International Studies, last modified July 13, 2015, 6, http://csis.org/files/publication/150714_Significant_Cyber_Events_List.pdf.

[227] Libicki, "Cyberspace is not Warfighting Domain," 329; Lindsay, "Stuxnet and the Limits of Cyberwarfare,"365–66; "Significant Cyber Incidents Since 2006," 6.

employed during the Gulf War, the CCP viewed Stuxnet in the same manner. In contrast, however, by 2010, China built up cyber warfare tactics, cyber defenses, and multifaceted cyber strategies.[228] The CCP interpreted Stuxnet as a signal that the PLA needed to refine its computer network defense (CND) and CNA capabilities: the PLA had to maintain its ability to preemptively strike, retaliate, and defend against damaging cyberattacks. In addition to Stuxnet, the 2013 release of classified U.S. government cyber operations information also impacted the pace and scope of PLA modernization.

In 2013, Edward Snowden's release of sensitive, classified National Security Administration (NSA) information to foreign governments was the last fourth wave event that significantly influenced PLA modernization. Snowden intentionally released information detailing the NSA's deep virtual infiltration of Chinese government, university, and communications networks.[229] The information Snowden provided only reinforced the CCP's inclinations that the United States conducted continual CNE on Chinese networks.[230] The leaked information also detailed how inferior China's cyber capabilities were—relative to the United States—and revitalized the PLA's urgency to field more aggressive cyber strategies.[231] Subsequent to the Snowden incident, the PLA's cyber functions were reorganized directly under the control of the CCP, and the PLA's cyber strategy was postured to combat the U.S.'s superior skills.[232]

1. Public Characterization of Strategic Cyber Modernization

The Defense White Papers published in 2004–2015 set the tone for fourth wave modernization efforts because they emphasized the PLA's development of robust cyber missions. The 2004 white papers referenced a key excerpt, "Revolution in Military

[228] Lindsay, "Stuxnet and the Limits of Cyberwarfare," 365.

[229] Lindsay, "Impact of China on Cybersecurity: Fiction and Friction," 7, 27.

[230] Jong-Chen, "U.S.-China Cybersecurity Relations."

[231] Lindsay, "Stuxnet and the Limits of Cyberwarfare," 365.

[232] Lindsay, "Introduction," 3, 13; Ye Zheng, "Cyberwarfare to Cybersecurity," 126; Lindsay, "Impact of China on Cyber Security," 17.

Affairs [RMA] with Chinese Characteristics."[233] In essence, that excerpt plotted the PLA's course to completely transform the military's R&D infrastructure, science and technology (S&T) programs, training, weaponry, and military systems: a total revolution of the military.[234] The PLA's top priority was progression of each PLA branch's military mission, equipment, and platforms.[235] Subsequent white papers released in 2006, 2008, and 2010 stressed similar concepts and continually built upon the themes outlined in the 2004 white papers.[236] The 2015 DWPs also upheld the principles of the 2004 white papers but put more emphasis on developing modernized cyber strategies and virtual operations—like CNO, CNE, CND, and offensive CNA.

The 2015 white papers highlighted the PLA's modernization initiatives of multilayered cybersecurity, aggressive information warfare, and offensive CNA.[237] The white papers also outlined the consolidation of the PLA's military and cyber strategies under the CCP.[238] Many scholars conclude, however, that the white paper initiatives were not new, they were just openly disseminated to the public.[239] Upon comparing historical white papers with China's strategic moves from 1995–2015, the PLA's development matched the CCP's previously outlined developmental goals.[240] The lack of new initiatives suggests the PLA's military strategy achieved its modern, informationized objectives as the CCP intended.[241] The 2015 DWPs were also significant because they

---

[233] Blasko, "Maritime Missions Require a Change," 3, 6; Information Office of the State Council of the People's Republic of China, *China's National Defense* (Beijing: State Council, December 2004), http://en.people.cn/whitepaper/defense2004/defense2004.html.

[234] Information Office of the State Council, *China's National Defense.*

[235] Zhang, "China's Defense White Papers: Critical Appraisal," 893–94.

[236] Ibid., 894–96; Blasko, "Maritime Missions Require a Change," 3, 6.

[237] "Document: China's Military Strategy."

[238] Ibid.

[239] Joe McReynolds, "Network Warfare in China's 2015 Defense White Paper," *China Brief 15*, no. 12 (June 2015): 11–12, http://www.jamestown.org/uploads/media/China_Brief_Vol_15_Issue_12_1.pdf ; Blasko, "Maritime Missions Require a Change," 3–4; "Document: China's Military Strategy"; Thomas J. Christensen, "Windows and War: Trend Analysis and Beijing's Use of Force," in *New Directions in the Study of China's Foreign Policy*, ed. Alastai Iain Johnston and Robert S. Ross (Stanford, CA: Stanford University Press, 2006), 75–76; *Annual Report to Congress:2014*, 35.

[240] McReynolds, "Network Warfare in China's Defense," 11–12; Blasko, "Maritime Missions Require a Change," 3–4; "Document: China's Military Strategy"; *Annual Report to Congress: 2014*, 35.

[241] Ibid.

provided clues as to the driving forces that determine China's modern cyber strategy: Taiwan was listed as one of China's domestic "developmental" objectives.[242] In addition to the doctrinal parameters the DWPs outlined, the CCP also directed the PLA's focus toward renovating military equipment in each service branch.

2. Physical Modernization Initiatives across the PLA Branches

The PLA's 2015 military parade was a clear demonstration of the rapid physical modernization programs the PLA undertook in the fourth wave.[243] Phillip C. Sanders and Andrew Scobell, attempt to explain the drivers behind the PLA's swift, multifaceted modernization of physical platforms from 2004–2015: "PLA efforts to build more robust military capabilities, including more capable fighter aircraft, pilots with experience flying over water, and unmanned aerial surveillance vehicles have also expanded the military options available to Chinese decision makers."[244] This section explores cases of the PLA's physical modernization plans in order to compare them with previous modernization objectives set by the CCP.

The PLAN significantly expanded its ships, offensive missile capabilities, maritime defenses, and reach across the Pacific in the fourth wave.[245] Specifically, the PLAN modernized more than 60 percent of its frigates' offensive and defensive capabilities, produced its first littoral combat ship in 2012, and fielded its first large aircraft carrier in 2012.[246] The PLAN also developed naval vessels and submarines that

---

[242] "Document: China's Military Strategy."

[243] Saunders and Scobell, "Introduction: PLA Influence," 2; Chris Buckley, "Military Parade in China Gives Xi Jinping a Platform to Show Grip on Power," *New York Times*, September 3, 2015, http://www.nytimes.com/2015/09/04/world/asia/china-military-parade-xi-jinping.html.

[244] Saunders and Scobell, "Introduction: PLA Influence," 12.

[245] Heginbotham et al., *U.S.-China Military Scorecard*, 203–04.

[246] Ibid., 30–31, 89; Andrew Erickson, Abraham M. Denmark, and Gabriel Collins, "Beijing's 'Starter Carrier' and Future Steps: Alternatives and Implications," *Naval War College Review* 65, no. 1 (Winter 2012): 18–20, 32–34, http://www.andrewerickson.com/wp-content/uploads/2011/12/Erickson-Denmark-Collins_Beijings-Starter-Carrier_NWCR_2012-Winter.pdf; Meg Jones, "Navy's Vessel of Versatility," *Journal Sentinel*, November 5, 2008, http://www.jsonline.com/news/milwaukee/33947284.html; Robert Johnson, "This is China's Response to the U.S. Navy's Struggling Coastal Warship Program," *Business Insider*, June 25, 2012, http://www.businessinsider.com/chinas-type-056-corvette-and-the-lcs-2012-6; Liam Stoker, "Combat Ships do Battle: LCS versus Type 26," Naval Technology, Kable Intelligence Limited, last modified August 29, 2012, http://www.naval-technology.com/features/featurecombat-ships-battle-lcs-type-26/.

could combat modern submarine warfare.[247] To bolster its new maritime platforms, the PLAN subsequently introduced the J-15 carrier landing-capable fighter and modern long-range helicopter models.[248] The PLAN's completion of fourth wave physical initiatives earned it the designation as one of the few developed, modern navies.[249] From 2004–2015, the PLAAF also made enormous strides in updating its airframes.

Over the course of nine years (2004-2015), the PLAAF became the epitome of the PLA's physical modernization initiatives: it introduced new fighters, stealth aircraft, heavy aircraft, helicopters, air defense systems, and sophisticated missile technologies.[250] In 2010, the PLAAF produced fourth generation multirole fighter jets (the J-10 and J-11 models) that rivaled U.S. F-15 and F-16 fighters.[251] In 2011 and 2014, the PLAAF tested stealth-models of fifth generation multirole fighters (the J-20 and J-31).[252] In addition to the modernized fighters, in 2006, the PLAAF produced AEW-capable aircraft.[253] In the area of unmanned aerial vehicles (UAV), the PLAAF manufactured a range of medium-altitude, weaponized, long-endurance, and ISR capable UAVs.[254] Apart from new aircraft, the PLA also advanced its long-range surface-to-air missile (SAM) capabilities

---

[247] Heginbotham et al., *U.S.-China Military Scorecard*, xxvi.

[248] Ibid., xxvi, 30–31, 33–34, 208–09.

[249] Ibid., 34.

[250] Ibid., xxvi, 13, 16, 27, 30–31, 33–34, 208–09, 327, 338.

[251] Ibid., 30–31.

[252] Maggie Marcum, "A Comparative Study of Global Fighter Development Timelines," *The Study of Innovation and Technology in China Policy Brief 2014* (University of California Institute on Global Conflict and Cooperation, January 2014), 1–5, http://escholarship.org/uc/item/1wm202sh; "CAC J-10 Meng Long," Jane's All the World's Aircraft, IHS: Aerospace, Defence & Security, last modified July 20, 2015, https://janes.ihs.com.libproxy.nps.edu/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=+++1342293; Heginbotham et al., *U.S.-China Military Scorecard*, 99–100, 172; Zhao Yan, "China's 'KJ-2000' AWACS Used the Technology that the U.S. and Russia Have Not Yet Used," China Military Report, accessed October 12, 2015, http://wuxinghongqi.blogspot.com/2009/10/chinas-kj-2000-awacs-used-technology.html.

[253] Heginbotham et al., *U.S.-China Military Scorecard*, 98–101.

[254] "Xi'an ASN-209," Jane's Unmanned Aerial Vehicles and Targets, IHS: Aerospace, Defence & Security, last modified September 24, 2015, https://janes.ihs.com.libproxy.nps.edu/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=+++1318867; "Predator RQ-1/MQ-1/MQ-9 Reaper UAV, United States of America," Air Force Technology, Kable Intelligence Limited, accessed September 29, 2015, http://www.airforce-technology.com/projects/predator-uav/; Joakim Kasper Oestergaard Balle III, "MQ-1 Predator/MQ-9 Reaper," Aeroweb, last modified May 28, 2015, http://www.bga-aeroweb.com/Defense/MQ-1-Predator-MQ-9-Reaper.html.

to reach further distances across the South China and East China Seas.[255] Those examples demonstrate the PLAAF's diversified development of its modern air force platforms. PLA land and space capabilities also progressed in the fourth wave.

From 2010–2015, the PLA Army introduced new battle tanks, armored infantry fighting vehicles (AIFV), and armored personnel carriers to implement modernization objectives across its ground forces.[256] The PLA Army upgraded its artillery systems from towed mechanisms to self-propelled, mechanized platforms.[257] Additionally, in 2015, Chinese leader Xi Jinping announced personnel reductions to build a lean, technically proficient, modernized military force.[258] The personnel reductions again allowed the PLA to allocate excess defense funds to CCP priority areas in PLA modernization: cyber abilities, R&D infrastructure, and indigenous innovation.[259]

Apart from the army's advancement, PLA space systems were also modernized in the fourth wave. From 2000–2015, China launched more than 70 satellites into orbit and built robust ground-based Over-the-Horizon (OTH) radar technology.[260] The majority of the satellite and radar systems were equipped with modern military reconnaissance capabilities.[261] The satellite launches and OTH technology development were significant because their tracking and ISR technology were for military use and solely dedicated to the PLA.[262] The satellite technology is also a notable modern development because it assists with tracking and identification of naval vessels, which allow China to follow foreign naval presences in the South and East China Seas.[263] Aside from examples of individual modernized PLA military equipment, the PLA's cyberspace operations also experienced significant progress in the fourth wave.

---

[255] Heginbotham et al., *U.S.-China Military Scorecard*, 98–100.

[256] Ibid., 32–33.

[257] Ibid., 33.

[258] Buckley, "Military Parade in China"; Saunders and Scobell, "Introduction: PLA Influence," 8.

[259] Saunders and Scobell, "Introduction: PLA Influence," 37.

[260] Heginbotham et al., *U.S.-China Military Scorecard*, xxv, 228–30.

[261] Ibid.

[262] Ibid., 154–55, 228–30.

[263] Ibid.

3. Refining China's Modern Cyber Strategy

Intelligence analyst Nigel Inkster observed the enormous strides the PLA made toward modernizing its cyber missions in the fourth wave: "The PLA has undergone a doctrinal evolution…[to pursue] a highly ambitious cyber warfare agenda that aims to link all service branches…and has created three new departments—Informationization, Strategic Planning, and Training—to bring this agenda into being."[264] By 2004, the PLA established strategic cyber guidelines (shown in the DWPs), structured operational cyber units, cyber militia units, and robust cyber recruitment methods.[265] The fourth wave saw enormous improvement to China's cyber strategy. Since there were many upgrades to PLA cyber missions during that time, this section discusses cases of modernized cyber initiatives. Additionally, since this thesis exclusively relies on open source information, its discussion of the nature of PLA cyber programs may be limited. Consequently, the information presented in this section is an example of China's and the PLA's openly publicized cyber advancements from 2004–2015.

a. Updates to Document 27

Even though Document 27 emerged prior to 2004, the SILG released document updates that were responsive to international events occurring in the fourth wave. From 2004–2015, Document 27 still served as the foundation for China's cybersecurity; however, during key periods the CCP and SILG released supplemental guidance to reinforce its core tenets.[266] In 2008, the CCP added provisions to Document 27 to adjust cybersecurity measures for the Beijing Olympics and global financial crisis.[267] Additionally, in 2012, the SILG released a new opinion stance to Document 27 that contained much of its original form but also improved on domestic encryption and critical infrastructure guidance.[268] The new 2012 SILG opinion was released in the wake

[264] Inkster, "Chinese Intelligence Agencies," 42.

[265] Gao, "Good Guys Who Hack Like Criminals"; Information Office of the State Council, *China's National Defense;* Sheldon and McReynolds, "Civil-Military Integration," 193–95.

[266] Segal, "China Moves Forward."

[267] Lindsay, "Introduction," 12.

[268] Ibid.; Segal, "China Moves Forward."

of the Iranian Stuxnet virus and sought to bolster China's CND against that type of damaging cyberattack.[269]

b. Enhancements to the PLA's Cyber Structure

During the fourth wave, the PLA implemented multifaceted improvements to its military cyber units, information-focused cyber militias, technical cyber training, and dedicated military technology R&D institutions. Despite the incremental personnel reductions in each wave of modernization, the PLA's cyber mission continued to expand its organization and employee base. In 2004 alone, the PLA had more than 10 million militia members at its disposal to conduct non-traditional information warfare operations and alternate PLA functions.[270] Since the PLA had also drastically improved its cyber capabilities and virtual global reach during this time, it categorized its cyber missions by type and area of focus (discussed in Chapter IV). PLA cyber units were spread across Chinese regions and compartmentalized based on their functions: domestic information censorship, cybersecurity, information warfare operations, CNO, or ISR—to name a few.

To support and continually refine those specific mission-sets, the PLA developed individual training and R&D institutions dedicated to each department's distinct cyber mission. For example, the PLA's Technical Reconnaissance Department has approximately 10 R&D institutions dedicated to providing training for its information security, communications intelligence (COMINT), reconnaissance, and cryptology missions.[271] The CCP also sought to improve its future PLA soldiers' technical skills and knowledge through mandated National Defense and military training courses in public school curriculums.[272] The forward leaning changes in the PLA's cyber structure, suggest that its modernized cyber strategy and mission sets (CNA, CND, and cyber espionage) were functioning and utilized during this time. There were other notable non-

---

[269] Segal, "China Moves Forward."

[270] Sheldon and McReynolds, "Civil-Military Integration," 193–94; Information Office of the State Council, *China's National Defense*.

[271] Stokes, "Chinese People's Liberations Army Computer Network," 175, 177–79; Lindsay, "Introduction," 18.

[272] Information Office of the State Council, China's National Defense.

military cyber developments—like the proliferation of China's underground hacking economy, patriotic hackers, and public Internet access—that occurred during the fourth wave; however, this chapter is primarily focuses on examining the role military developments and government cyber initiatives had on establishing China's modern cyber strategy.

c. Drawing from Western Cyber Strategies to Build China's Cyber Strategy

As Mulvenon observes, China's cyber strategy and strategic Chinese cyber terms contain significant Western influences: "If one tracks Chinese military terminology over time, it is possible to discern a short lag between…new cyber concepts in the United States and their eventual adoption in China."[273] China observed the United States' transformation into one of the first countries that developed sophisticated, cutting-edge technologies and subsequently adapted those technologies to engage in informationized warfare and cyber warfare. China knew it would have to assimilate those Western principles if it wanted to reach a similar level of technological superiority.[274]

Wang Baocun was an early contributor to China's modern cyber strategy for his studies on U.S. military cyber concepts and subsequent introduction of those concepts into Chinese strategic thought.[275] Wang was not a cyber expert; he was an expert on U.S. military strategies.[276] Wang observed the United States' early use of the cyber concept "information warfare" and subsequently incorporated it into China's early cyber strategy.[277] Similar Chinese experts on U.S. military strategy noticed the evolution of Western strategic cyber terms: "information warfare" became "information operations" and eventually converted into "network operations."[278] Adapting to the Western evolution, Chinese strategic cyber terms evolved in the same way. "Information warfare"

---

[273] Mulvenon, "PLA Computer Network Operations," 254.

[274] Jason Kelly, "A Chinese Revolution in Military Affairs?" Yale Journal of International Affairs 1, no. 2 (Winter-Spring 2006): 58–59, http://www.yale.edu/yjia/articles/Vol_1_Iss_2_Spring2006/kelly217.pdf; Heginbotham et al., U.S.-China Military Scorecard, 273.

[275] Mulvenon, "PLA Computer Network Operations," 254.

[276] Ibid.

[277] Blasko, Chinese Army Today, 2nd ed., 130–31.

[278] Mulvenon, "PLA Computer Network Operations," 254.

was used in early PLA writings, then moved to "information operations," and incorporated "network operations" in more recent publications.[279] "Network operations" underwent further revision until China's modern CNO strategy was formed.[280] While China's strategic thought on military and cyber operations incorporate U.S. and Western strategic concepts, China's modern cyber strategy is unique in the assimilated nature in which it employs this strategy, which is discussed further in Chapter IV.

E. SUMMARY

Since 1978, PLA modernization progressed in four distinct waves—with each wave emphasizing a specific theme in the PLA's advancement. The first wave from 1978–1988, introduced modern doctrinal concepts and transformed the PLA into an autonomous business-like force. The second wave from 1989–1996, was a lull period for actual modernization initiatives, but it significantly impacted the PLA's future advancement because of international events that occurred during that time. Second wave events forced the CCP to refocus domestic priorities toward dual economic and military development. In the third wave (1997–2003), the CCP's increased urgency toward PLA modernization forced the military to adopt an informationized cyber strategy. By the fourth wave (2004–2015), the PLA implemented the physical modernization of its military equipment.

Over the course of the four waves, the PLA developed new technologically focused doctrines, robust acquisitions systems, and multifaceted advanced military platforms. An examination of China's DWPs (released from 1998–2015), compared with the PLA's strategic moves during modernization suggest the PLA's modernization initiatives and cyber strategy developed in accordance with the CCP's objectives. This chapter presents evidence of the PLA's key, developed cyber missions and operations during the waves of modernization to address debates in the literature about China lacking an observable cyber strategy. The evidence indicates that China does in fact employ a coherent cyber strategy. Additionally, this chapter examines the CCP's and

[279] Mulvenon, "PLA Computer Network Operations," 254.

[280] Ibid.

PLA's deliberate development of specific cyber initiatives during key time periods of PLA modernization to suggest the PLA developed China's modern version of a cyber strategy. The next chapter provides an analysis of China's modern cyber strategy and discusses its core tenets.

IV. COMPUTER NETWORK OPERATIONS WITH "CHINESE CHARACTERISTICS"

Modern Chinese cyber strategy stresses ambiguity in its virtual operations and "[cyber warfare] victory through inferiority over superiority," which were warfighting principles adopted from Sun Zi and Mao Zedong.[281] Ambiguity in Chinese cyber operations allows Chinese operators to employ deception, information warfare, and "active [cyber] offense." "Victory through inferiority over superiority,"[282] refers to how China can creatively leverage its weaker cyber methods (in relation to that of the United States) to win cyber battles.[283] From those principles, Western analyses interpret China's modern cyber strategy as CNO that necessitates the use of CNA, cyber espionage, CND, and ISR in order for China to achieve military, economic, and developmental objectives.

Based on the information above, this chapter establishes that cyber espionage is a conscious, deliberate function of China's cyber strategy by identifying its structural features, the PLA's organizational methods, and the core concepts that are unique to this strategy. This chapter discusses the organizational structure of China's cyber mission under the PLA, individual case studies of PLA cyber units, and China's CNO principles to solidify this study's thesis. This examination of how the PLA directs and delegates its specific cyber missions also provides clues as to how the PLA employs cyber espionage against potential targets. This chapter ultimately studies the characteristics of China's modern cyber strategy and its implementation of cyber methods to provide clues on how cyber espionage fits into the PLA and its modernization efforts. As explored in the next section, the majority of China's CNO responsibilities are delegated from the CCP to the PLA and further organized from there.

---

[281] Pollpeter, "Chinese Writings on Cyberwarfare," 140–42; Jian, "China's Defense White Papers: Critical Appraisal," 892; Li, "PLA's Evolving Campaign," 146; "Document: China's Military Strategy."

[282] Hu Guangzheng et al., *Yingxiangdao ershiyi shiji de zhengming (Contention Affecting the 21st Century)*, (Beijing: Liberation Army Press, 1989), 113, quoted in Nan Li, "The PLA's Evolving Campaign Doctrine and Strategies," in *The People's Liberation Army in the Information Age* (Santa Monica, CA: RAND, 1999), 146, http://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF145/CF145.chap8.pdf.

[283] Li, "PLA's Evolving Campaign," 146.

A. DECONSTRUCTING THE ORGANIZATIONAL FEATURES OF CHINA'S CYBER STRATEGY

The CCP is situated at the top of the Chinese government and maintains a hierarchical structure over subordinate organizations (the Central Military Commission [CMC], State Council, and Leading Small Groups [LSG]) but especially China's cyber strategy. As shown in Figure 3, the chain of command for all organizations flows back to the party, underscoring its top-down authority structure.[284] The State Council is China's large bureaucracy; the CMC is the party's enforcement arm; the LSGs make national, military, and cyber policy recommendations to the CCP.[285] Prior to 2014, China's cyber mission, policies, and strategy were managed by the State Council.[286] Working in concert with the State Council, the SILG monitors China's cyber operations.[287] The organization of China's cyber mission under the large state bureaucracy has contributed to complications in China's strategic cyber implementation.

Jon R. Lindsay, Assistant Professor of Digital Media and Global Affairs at the Toronto Munk School of Global Affairs, highlights the difficulty China's rigid, authoritarian organization has on its cyber missions: "As in other areas of Chinese policy, the implementation of cybersecurity is disjointed functionally and regionally, rife with rent seeking bureaucratic agencies and enterprises."[288] The increasingly complicated bureaucratic over management of China's cyber operations has allowed multiple organizations to contribute to China's strategic cyber implementation.[289] Additionally, due to the closed nature of the Chinese government's authoritarian structure, cyber operational information is stovepiped, the many Chinese cyber organizations vary in their implementation of cyber strategies, and they overlap on similar cyber functions.[290] As

284 Lindsay, "Introduction," 7.

285 Inkster, "Chinese Intelligence Agencies," 38–39; Saunders and Scobell, "Introduction: PLA Influence," 2.

286 Lindsay, "Introduction," 7–8.

287 Stokes, "Chinese People's Liberation Army Computer Network," 163–64.

288 Lindsay, "Impact of China on Cybersecurity: Fiction and Friction," 16–18.

289 Ibid.

290 Ibid.

Lindsay details, the fragmented, decentralized nature in which China implements its overall cyber strategy, to include PLA cyber operations, is ultimately a function of China's bureaucratic mismanagement and rigid organization of its cyber units, which is discussed in further depth later in this chapter.

In an attempt to address this bureaucratic mismanagement, after 2014, President Xi Jinping added a new Cybersecurity Leading Small Group (CILG), which effectively shifted the policy arm of China's cyber strategy directly under his control.[291] Physical application and implementation of China's cyber strategy—cyber warfare, cyber operations, and cybersecurity—fall under the CMC. The specific delegation of Chinese cyber missions under the State Council and to the CCP, suggests China's robust cyber missions are central to the CCP's priorities, granting cyber special attention by state offices.

Since the CMC is the CCP's arm to manage the military, the CMC acts as an envoy between the party and the PLA—with China's president typically serving as the CMC Chairman.[292] Under the CMC, there are four General Departments (General Staff, Equipment, Logistics, and Administration) that carry out the PLA's policy guidance, training, and military strategic planning.[293] In addition to the General Departments exhibited in Figure 2, the PLA is also geographically divided into seven regions, shown

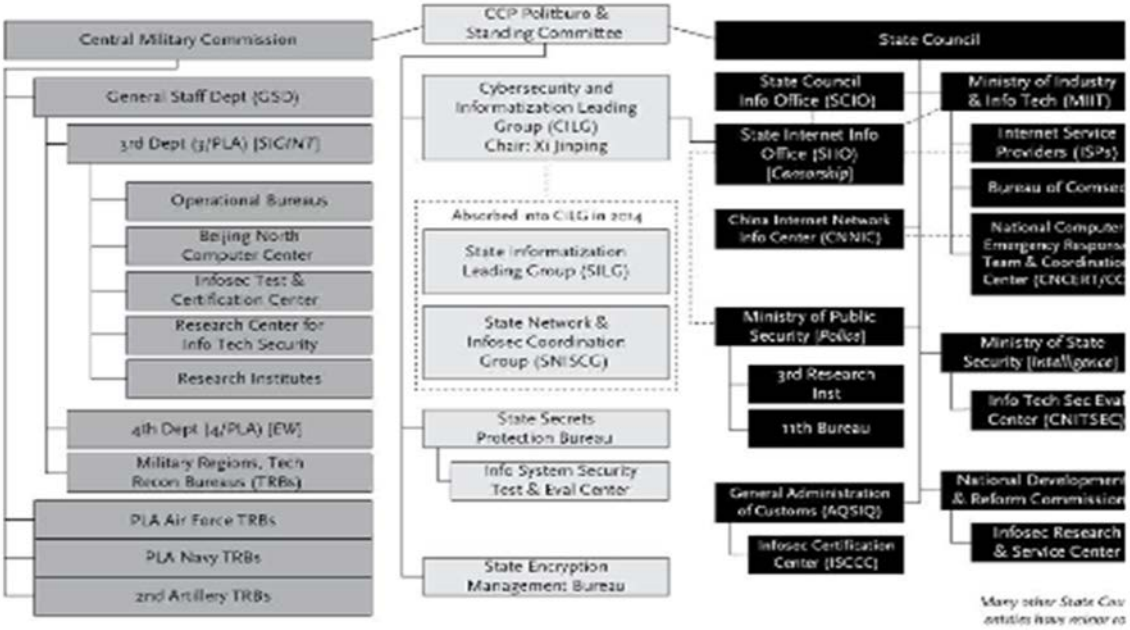
[291] Stokes, "Chinese People's Liberation Army Computer Network," 164; Lindsay, "Introduction," 7.

[292] Allen, "Introduction to the PLA's Administrative," 7, 28–29, 35, 38, 39–40; Nan Li, "The Central Military Commission and Military Policy in China," in *The People's Liberation Army as Organization: Reference Volume v1.0*, ed. James C. Mulvenon and Andrew N. D. Yang (Santa Monica, CA: RAND, 2002), 73–74, 82, 88–90, http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2008/CF182part1.pdf; "APT 1," 7–8; *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2014* (Washington, DC: Office of the Secretary of Defense, April 24, 2014), 23–24, http://www.defense.gov/pubs/2014_DOD_China_Report.pdf.

[293] Allen, "Introduction to the PLA's Administrative," 7–8, 19–21, 24, 35–36; David Finklestein, "The General Staff Department of the Chinese People's Liberation Army: Organization, Roles, & Missions," in *The People's Liberation Army as Organization: Reference Volume v1.0*, ed. James C. Mulvenon and Andrew N. D. Yang (Santa Monica, CA: RAND, 2002), 125, http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2008/CF182part1.pdf.http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2008/CF182part1.pdf.

in Table 1.[294] All PLA regions, divisions, bureaus, and units fall under the General Departments' command.[295]

Figure 2. Organization of China's Major Departments and Cyber Missions under the CCP



Source: Jon R. Lindsay, "Introduction—China and Cybersecurity: Controversy," in *China and Cybersecurity" Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), 8.

To maintain consolidated control across China, the CCP distributes PLA military groups across regions. PLA divisions are directly under military groups and are divided among Chinese districts: Beijing has *Hebei, Shanxi, and Nei Menggu* military districts.[296] Apart from location ordering principles, PLA bureaus and units are assigned numbered

[294] *Project Camerashy: Closing the Aperture on China's Unit 78020* (Arlington, VA: ThreatConnect and Defense Group Inc. [DGI], 2015), 16, https://www.threatconnect.com/camerashy/.

[295] Allen, "Introduction to the PLA's Administrative," 40–43; Li, "Central Military Commission and Military Policy," 46–47; Stokes, "Chinese People's Liberation Army Computer Network," 164–65; "APT 1," 7–8.

[296] Allen, "Introduction to the PLA's Administrative," 19–21; Stokes, "Chinese People's Liberation Army Computer Network," 166–67.

identifiers (Military Unit Cover Designators [MUCD])[297] to mask their true functions: PLA Unit 61398 is an example of an MUCD.[298] As shown in Table 1, the geographical separation and MUCD numbering system gives an added degree of anonymity to the PLA's already ambiguous missions.[299] The added degree of anonymity helps China to employ deception in cyberspace and accomplish cyber objectives without direct attribute, however, it also contributes to the fragmented implementation of China's cyber strategy as previously discussed. In addition to the physical organization features in the PLA's chain of command features are organized in a similar rigid manner.

Table 1. Technical Reconnaissance Bureaus by Region and MUCD

MILITARY REGION (MR)	UNIT DESIGNATOR	LOCATION	MILITARY UNIT COVER DESIGNATOR (MUCD)
Shenyang MR	Technical Reconnaissance Bureau	Shenyang, Liaoning Province	Unit 65016
Beijing MR	Beijing MR Technical Reconnaissance Bureau	Beijing	Unit 66407
Lanzhou MR	1st Technical Reconnaissance Bureau	Qilihe District, Gansu Province	Unit 68002
	2nd Technical Reconnaissance Bureau	Urumqi, Xinjiang Uyghur Autonomous Region	Unit 69010
Jinan MR	Technical Reconnaissance Bureau	Jinan, Shandong Province	Unit 72959
Nanjing MR	1st Technical Reconnaissance Bureau	Nanjing, Jiangsu Province	Unit 73610
	2nd Technical Reconnaissance Bureau	Fuzhou, Fujian Province	Unit 73630
Guangzhou MR	Technical Reconnaissance Bureau	Guangzhou, Guangdong Province	Unit 75770
Chengdu MR	1st Technical Reconnaissance Bureau	Chengdu, Sichuan Province	Unit 78006
	2nd Technical Reconnaissance Bureau	Kunming, Yunnan Province	Unit 78020

Source: *Project Camerashy: Closing the Aperture on China's Unit 78020* (Arlington, VA: ThreatConnect and Defense Group, Inc. [DGI], 2015), 78, https://www.threatconnect.com/camerashy/.

297 "APT 1," 9; ThreatConnect and DGI, *China's Unit 78020*, 16.

298 Stokes, "Chinese People's Liberation Army Computer Network," 181; Allen, "Introduction to the PLA's Administrative," 3, 11; ThreatConnect and DGI, *China's Unit 78020*, 16.

299 ThreatConnect and DGI, *China's Unit 78020*, 16.

Within the PLA, each unit has specified chain of command and mission functions that follow the CCP's rigid organizational theme. The geographical separation and one-directional flow of orders limits cross-talk between organizations and adds compartmentalization.[300] Similarly, the CCP delegates PLA mission sets to specific units. For example, cyber operations like offensive network sabotage and psychological operations exclusively belong to PLA Special Operations Forces.[301] The rigidity of PLA organizational features impacts the wide-scale implementation of China's cyber strategy and also suggests that the CCP and PLA employ cyber espionage in a conscious, deliberate manner much like their operational cyber structure.[302]

Since the 1980s, the PLA's General Staff Department (GSD) has carried out the practical application and physical implementation of China's cyber strategy—cyber warfare, CNO, and cybersecurity.[303] The GSD manages the implementation of China's physical cyber missions and directs cybersecurity for the PLA's networks.[304] Under the GSD, and across the PLA's regions, China's cyber missions are further delegated to Technical Reconnaissance Bureaus (TRB) that have service-specific and region-specific operational cyber missions.[305] Each PLA service—the PLAAF, the PLAN, and the PLA Army—has their own TRBs spread out China.[306] The TRBs engage in military-centric analysis, translation, and interpretation of Signals Intelligence (SIGINT), COMINT, and exploited cyber network information.[307] TRB missions are further distinguished by their

---

[300] Lindsay, "China and Cybersecurity"; "APT 1," 2–3; ThreatConnect and DGI, *China's Unit 78020*, 7.

[301] Kevin McCauley, "PLA Special Operations: Combat Missions and Operations Abroad," *China Brief* 15, no. 17 (September 2015), the Jamestown Foundation, http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=44336&tx_ttnews%5BbackPid%5D=789&no_cache=1#.VfBR7P_H_IU; Mulvenon, "PLA Computer Network Operations," 272–74; Lindsay, "Inflated Cybersecurity Threat."

[302] Allen, "Introduction to the PLA's Administrative," 6, 11–12; "APT 1," 9.

[303] Nathan and Scobell, *China's Search for Security*, 291; Finklestein, "General Staff Department, 156, 160; "APT 1," 7; Stokes, "Chinese People's Liberation Army Computer Network," 163–64; "APT 1," 7–8.

[304] Stokes, "Chinese People's Liberation Army Computer Network," 163–64.

[305] Ibid., 173–74; ThreatConnect, and DGI *China's Unit 78020*, 15–16.

[306] Stokes, "Chinese People's Liberation Army Computer Network," 173–74.

[307] Ibid., 174–75; ThreatConnect and DGI, *China's Unit 78020*, 7, 16.

branch-specific functions and global areas of focus. For example, PLAAF TRBs may focus on imagery analysis or SIGINT collection on Southeast Asian targets, while PLAN TRBs may focus on SIGINT collection of naval intelligence and foreign navies operating near China.[308] The TRB's noted and observed cyber, SIGINT, COMINT, and ISR collection missions through virtual means, further indicate that CNE is a key mission under China's CNO. In order to further establish how TRBs, and ultimately the PLA, employ cyber espionage, the next section conducts a case study of one PLA TRB.

1. Technical Reconnaissance Bureaus: A Case Study of PLA Unit 78020

PLA Unit 78020 is just one of the PLA's TRBs, and its cyber missions are a good example to study for the insight they provide into how the PLA units employ cyber espionage under its CNO. To maintain secrecy around PLA cyber missions, the CMC deliberately compartmentalizes PLA cyber bureau functions and uses MUCDs to maintain the clandestine nature of their missions. U.S. cybersecurity, high-technology and threat intelligence collection firms ThreatConnect and DGI, however, examine Chinese CNO, CNA, and CND trends over time and uses their originating source, personnel characteristics, employment requirements, and open source training information to determine the functions of individual Chinese cyber units—like PLA Unit 78020. ThreatConnect and DGI reported in 2015 that PLA Unit 78020 (known as *Naikon* APT) is a cyber exploitation unit in one of China's TRBs.[309] PLA Unit 78020 is located under the PLA Army's Second TRB in the Chengdu Region (reference Table 1).

ThreatConnect and DGI conclude that Unit 78020's mission is related to China's tensions in the South China Sea based on Unit 78020's CNE and SIGINT collection of Association of Southeast Asian Nations ([ASEAN] Singapore, Malaysia, Thailand, and the Philippines), government, private, and military entities with presences in Southeast Asia.[310] ThreatConnect and DGI also traced Unit 78020's cyber espionage activity back to the origination date of 2010, which was also the year the Sino-Japanese conflict over

[308] Stokes, "Chinese People's Liberation Army Computer Network," 173–75; ThreatConnect and DGI, *China's Unit 78020*, 7–10, 15–16, 20.

[309] ThreatConnect and DGI, *China's Unit 78020*, 7, 15–16, 69.

[310] Ibid., 8–10, 12, 15–16, 20, 23, 74.

the Diaoyu Islands began. Since then, Unit 78020 has exfiltrated cyber intelligence from countries that have also asserted claims in the South China Sea: like its cyber espionage campaigns on classified Filipino Naval intelligence following Sino-Filipino island contention.[311] Those examples further substantiate determinations that PLA Unit 78020's mission is concentrated on nations with dealings in the South China Sea.[312]

PLA Unit 78020's organization and cyber exploitation profile demonstrates the role TRBs play in China's cyber strategy and cyber mission implementation. Unit 78020's targeted cyber campaigns against Southeast Asian countries demonstrates the deliberate role in which cyber espionage is employed within the PLA—suggesting that cyber espionage is employed in a similar manner toward other PLA objectives. PLA Unit 78020's use of cyber espionage to collect intelligence on the CCP's domestic and international priority target areas (nations neighboring the South China Sea) highlights the foundational concept that cyber espionage plays a central role in China's overall cyber strategy. In contrast from the cyber intelligence collection and analysis missions the TRBs conduct, alternate GSD departments work in conjunction with the TRBs to execute China's offensive cyber strategy.

2. PLA Operational Cyber Departments

Adding to the complexity of China's cyber mission organization, the GSD is further broken down into three cyber operations departments, as Figure 4 shows.[313] The GSD departments that conduct China's CNO are the Third Technical Reconnaissance Department and the Fourth Electronic Countermeasures and Radar Department.[314] To supplement the PLA's cyber missions, the PLA also employs civilian-integrated PLA cyber militias and subject matter expert (SME) civilian hackers (white-hat, patriotic, and black-hat hackers) to ensure China's cyber strategy is executed in its entirety. The variance on military, government, and civilian hackers almost guarantees the completion

311 ThreatConnect, "Piercing Cow's Tongue."

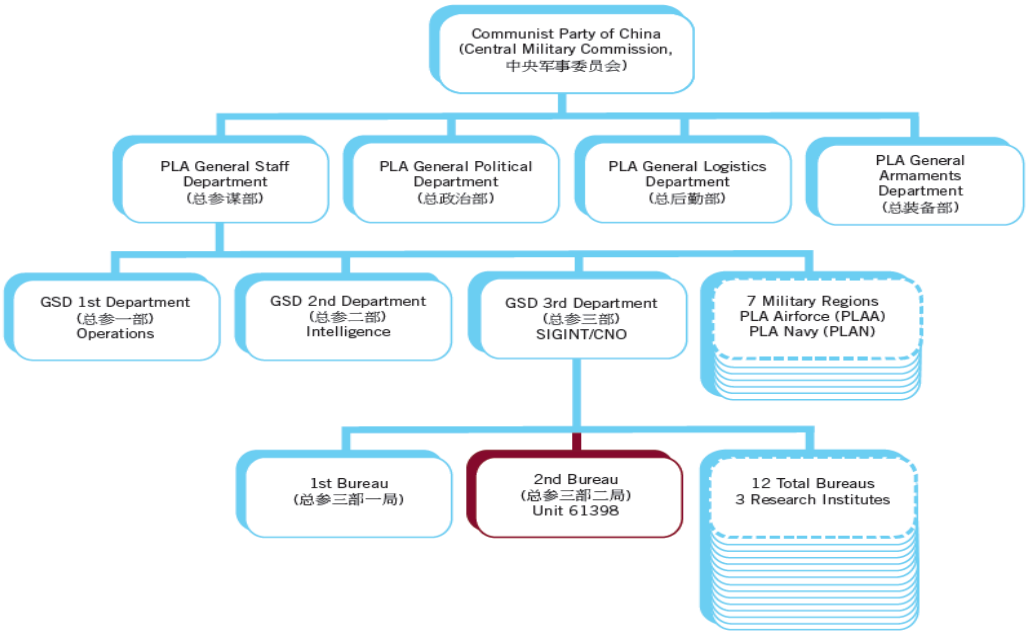
312 ThreatConnect and DGI, *China's Unit 78020*, 8–10, 15–16, 20, 23, 66, 68.

313 "APT 1," 7–8.

314 Stokes, "Chinese People's Liberation Army Computer Network," 163–65, 175; Finklestein, "General Staff Department," 158–61; Inkster, "Chinese Intelligence Agencies," 32–33.

of the CCP's national priorities because several competing entities engage in various CNE methods to ensure the missions' success.[315] Although the departments' and cyber militias' distinct functions are not publicly announced, open-source information suggests their functions include domestic cyber monitoring, COMINT, CNE, CNA, and CND.[316] Analyses of the PLA's Third and Fourth Department cyber missions liken their organization to U.S. organizations: the Third Department is similar to the U.S. military's Cyber Command, and the Fourth Department is comparable to the NSA.[317]

Figure 3. Organization of PLA Operational Cyber Departments under the CMC



Source: "APT 1: Exposing One of China's Cyber Espionage Units," Mandiant (February 2013), 7–8, http://intelreport.mandiant.com/.

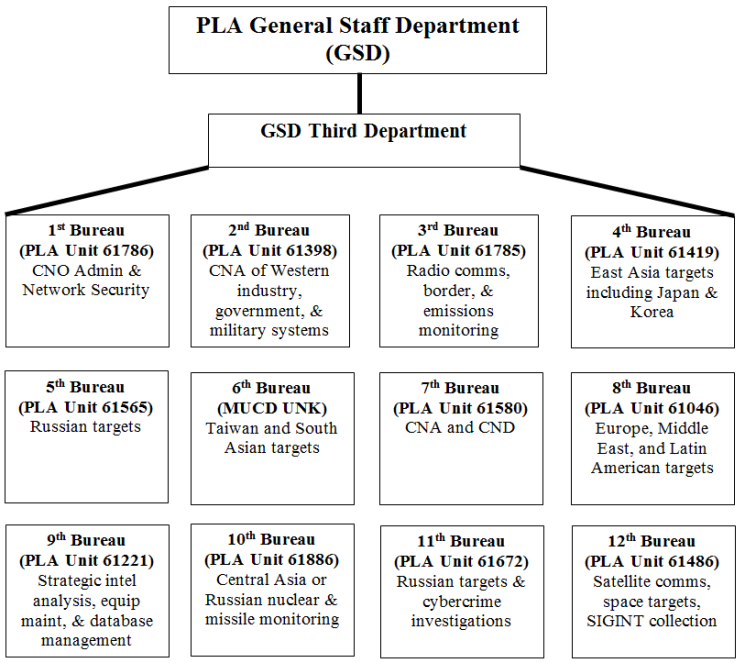
[315] Lindsay, "Introduction," 18–19; Lindsay and Reveron, "Conclusion," 345, 350; Krekel, Adams, and Bakos, *Occupying Information High Ground*, 39, 51–52.

[316] Mulvenon, "PLA Computer Network Operations," 259; Stokes, "Chinese People's Liberation Army Computer Network," 164–65.

[317] Lindsay, "Introduction," 8; McReynolds, "Network Warfare in China's Defense," 12; U.S. Department of Defense, *Task Force Report: Resilient Military Systems*, 9; Stokes, "Chinese People's Liberation Army Computer Network," 164–65.

The Third Department has 12 operational bureaus that are individually tasked with specific functions under China's CNO, further highlighting the deliberate manner in which the PLA's cyber operations are organized and executed.[318] The departments are separated by their functions and by countries of interest (as shown in Figure 5): the Fourth Bureau's (PLA Unit 61419) focus area is East Asia with a concentration on Japan and the Koreas.[319] Additionally, the Second Bureau (PLA Unit 61398) has been designated as China's CNA and exploitation bureau of Western industrial, military, and government targets.[320]

Figure 4. PLA Operational Cyber Bureaus under the Third Department



Adapted from: Mark A. Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), 168–72.

---

[318] These bureaus are distinctly separate from the PLA's Technical Reconnaissance Bureaus, which provide the CCP with domestic and external monitoring services—including Signals Intelligence, Communications Intelligence, and Internet monitoring; Stokes, "Chinese People's Liberation Army Computer Network," 170.

[319] Stokes, "Chinese People's Liberation Army Computer Network," 171.

[320] This information is based on Mandiant's 2006 report that provided an in-depth case study of PLA Unit 61398's (APT 1) suspected historical record of cyberattacks; "APT 1," 2–3, 5, 7.

The PLA does not openly publish each bureau's specific cyber missions, but conclusions on the bureaus' functions are built by Mark A. Stokes, a respected military analyst of the PLA who was also a former U.S. Air Force attaché, from contextual clues about the units: their location within China, how many offices they have, how much manpower is dedicated to them, the type of training their personnel receive, and the type of translators hired. For example, the Fourth Bureau is designated as a Japanese and Korean focus based on its use of Korean linguists and the central location of its offices in the Qingdao region—which falls in east-northeast China in close proximity to both Korea and Japan.[321]

3. PLA Operational Cyber Bureaus: A Case Study of PLA Unit 61398

Mandiant's 2013 cyber threat report on the cyber espionage group APT 1, or PLA Unit 61398, was the first significant in-depth look at how China and the PLA conduct CNO—namely cyber espionage.[322] Since 2006, Mandiant compiled enough data to link APT 1's cyber actions to the Chinese government-sponsored PLA Unit 61398.[323] Mandiant confirmed PLA Unit 61398 likely executes the PLA's CNA and CND missions as part of China's larger CNO strategy. Mandiant also based its conclusions on Unit 61398's operational functions based on the unit's organization under the GSD's Third Technical Reconnaissance Department and its physical offices' locations around China.[324] PLA Unit 61398 is centrally located in Shanghai, has thousands of employees, and primarily recruits employees with English speaking capabilities and formal technical computer training.[325]

Over 80 percent of Unit 61398's CNA and CNO operations (conducted from 2006–2013) were executed on Western targets, which further indicates that Unit 61398's

---

[321] Stokes, "Chinese People's Liberation Army Computer Network," 171.

[322] "APT 1," 1–2, 7–9, 20; Inkster, "Chinese Intelligence Agencies," 44; U.S.-China Economic and Security Review Commission, "Section 2: China's Cyber Activities," 243.

[323] "APT 1," 2–3, 7, 26, 31; Martinez et al., "Major U.S. Weapons Compromised."

[324] "APT 1," 2–3, 7–9; Stokes, "Chinese People's Liberation Army Computer Network," 163–65; Finklestein, "General Staff Department," 158–61; Inkster, "Chinese Intelligence Agencies," 32–33.

[325] "APT 1," 10–16, 19.

focus area is U.S., Canadian, and English-speaking industries and also suggests the deliberate nature in which China's CNO operations are employed.[326] PLA Unit 61398's list of cyber espionage exploitations range from specific U.S. military schematics, World Anti-Doping Agency information prior to the 2008 Beijing Olympics, and personal communications from the Coca-Cola Corporation. Even though China denies the legitimacy of Mandiant's report, Mandiant's concludes, "In a state that rigorously monitors Internet use, it is highly unlikely that the Chinese government is unaware of [a large cyber] attack group that operates from the Pudong New Area of Shanghai."[327] Previous discussions on the CCP's domestic Internet controls and its rigid, compartmentalized organization of the PLA also uphold the notion that the PLA's CNA, CNE, CND, and ISR operations are deliberate, government-sanctioned actions. The specific principles emphasized under China's CNO also provide clues on how and why the PLA employs targeted cyber espionage campaigns.

B. CHINA'S CYBER STRATEGY AS COMPUTER NETWORK OPERATIONS

China's current cyber strategy, described as CNO with "Chinese characteristics" by Chinese publications, incorporates core cyber warfare principles and situation-dependent scenarios and responses.[328] CNO is practiced by many nations in the world, and much like other nations, China's CNO principles are refined to make its cyber operations responsive to China's domestic and international needs, as this section discusses. As Table 2 shows, China's CNO is similar to the U.S.'s cyber strategy but is adapted to fit into China's cyber strategy.[329] The situation-dependent strategies built into China's cyber strategy are preemptive strategic choices that reflect the CCP's need to switch priorities based on the issues China faces.[330] One example of a situation-dependent scenario is Taiwan reunification: China's CNO necessitates the use of CNA

326 "APT 1," 3–4, 9.

327 Thomas, "China's Cyber Incursions," 13; "APT 1," 2.

328 Information Office of the State Council, China's National Defense.

329 Mulvenon, "PLA Computer Network Operations," 254, 258–61.

330 Ibid., 262–68.

against Taiwan if the island pursues an aggressive move toward independence; China's CNO also calls for CNA against the United States if it attempts to intervene in a Sino-Taiwanese conflict.[331] Each situation-dependent CNO strategy has several potential scenarios and outcomes that would allow for certain cyber methods and escalation tactics.[332]

Table 2. China's Computer Network Operations (CNO) Strategy Deconstructed

Core Concept	Description	Why?
1. DEFENSE FIRST	CND is the top priority. Once secure, develop "tactical counteroffensives"	*Because United States conducts high-volume CNE operations on Chinese servers*
2. PREEMPTIVE STRIKE ALWAYS	Use preemptive CNA to exploit an adversary's technological vulnerabilities (damaging their ability to respond) or to create more favorable conditions for offensive cyber operations	*Because China faces more technologically savvy adversaries (the United States) in cyber warfare and preemptive strike levels the playing field*
3. COMPUTER NETWORK ATTACK AS AN UNCONVENTIONAL WARFARE METHOD	CNA is used as an unconventional cyber method in the pre-stages of conflict to gain an advantage, but not for ongoing operations	*Because it helps China conduct quick decisive cyber actions in the case that an adversary cuts off China's access to the adversarial networks or fixes their network vulnerabilities*
4. PREEMPTIVE CNA FOR INFORMATION OPERATIONS	Use CNA to win in information warfare and limit or altogether eliminate the possibility of conventional war	*Because China's ability to monitor and conduct information campaigns is highly effective, China can use this skill in cyberspace to prevent war*
5. EXPLOIT AN ADVERSARIAL DEPENDENCE ON INFORMATION TECHNOLOGY IN C4I	Develop Command, Control, Communications, Computers, and Intelligence (C4I) capabilities that do not rely solely on information technology	*Because China believes it is not as technologically dependent as other countries (the United States)*

Adapted from: James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in *Beyond the Strait: PLA Missions Other Than Taiwan*, ed. Roy Kamphausen, David Lai, and Andrew Scobell (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2009), 259–60, 266, 269; Kevin Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press), 141–42, 145.

[331] Mulvenon, "PLA Computer Network Operations," 262–64.

[332] Ibid., 263–68.

Deliberate CNA and CNE allow China's CNO to target an adversary's IT and military network information.[333] Modern Chinese cyber strategists provide insight into why China emphasizes CNA, CNE, and CND in its CNO: "[CNA] is one of the most effective means for a weak military to fight a strong one."[334] This quote China's strategy of leveraging its inferior ("weak military") cyber and military capabilities, in reference to the U.S.'s, to gain advantage over stronger nations. The deconstruction of China's CNO principles and targets provides further insight into why and how the PLA employs certain cyber methods.

China's current CNO strategy relies on CNA and CNE for high priority targets: adversarial logistics information, computer network information, and military personnel data. An example of a CNO high priority target would be the infiltration and extraction of DOD unclassified Non-secure Internet Protocol Router Network (NIPRNET) information rather than Secret Internet Protocol Router Network (SIPRNET) data.[335] NIPRNET information is a primary target because a compromise of its personnel data, logistics operation information, and mission procedures could hinder or impede how the U.S. military conducts missions, operates in warfare, or even accomplishes routine tasks.[336] An example of a high priority target could potentially include the 2015 exploitation of millions of U.S. government employee files from OPM. Even though the United States has not determined the way in which the exfiltrated OPM data will be exploited, those OPM files contained personnel data and were stored on a relatively unsecure, easily accessible network. While it is not confirmed that OPM was a high priority target under Chinese CNO, the correlation between the breached OPM military and government personnel data and its placement on an unclassified network correlates to the previously

---

[333] Mulvenon, "PLA Computer Network Operations," 269.

[334] Foreign Ministry Press Conference, September 4, 2007, quoted in James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in *Beyond the Strait: PLA Missions Other Than Taiwan*, ed. Roy Kamphausen, David Lai, and Andrew Scobell (Carlisle, PA: U.S. Army War College, 2009), 257.

[335] Mulvenon, "PLA Computer Network Operations," 269–70.

[336] Ibid., 269–71.

mentioned Chinese CNO high priority target criteria.[337] Examples of Chinese cyber exploitation operations that parallel the CNO's high priority targets, like the OPM breach, also suggest that cyber espionage under China's CNO can be pursued in a deliberate manner.

Integrated Network Electronic Warfare (INEW) is also a key principle under China's CNO because it addresses China's cyber warfare actions. INEW was developed in 1999 but China evolved from its original form into a cyber principle that combines CNO with information censorship.[338] INEW differs from U.S. cyber operations in which the United States views information operations and CNA as independent missions and separates them under distinct electronic warfare (EW) and CNO subcategories. China's INEW advocates the simultaneous use of CNO and information operations to disrupt enemy networks.[339] Compared to Russia's and the U.S.'s developed skills, China's CNO and INEW cyber methods are often characterized as rudimentary and basic because INEW relies on user-friendly, cost-effective, quick-result methods—like DDOS and spearphishing.[340] The principles outlined under China's CNO and INEW indicate that the PLA deliberately employs cyber espionage against specific targets. The calculated nature in which cyber espionage is employed also establishes the key role cyber espionage plays in PLA operations—including PLA modernization.

C. SUMMARY

The rigid organization of China's cyber mission under the CCP and PLA indicates that the methods (CNA, CNE, cyber espionage, and CND) employed under China's CNO are deliberate missions delegated to specific PLA units. Two examples of how China's

337 Ellen Nakashima, "Hacks of OPM databases compromised 22.1 Million People, Federal Authorities Say," *Washington Post*, July 9, 2015, http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

338 Mulvenon, "PLA Computer Network Operations," 260–61; Pollpeter, "Chinese Writings on Cyberwarfare," 145; Ball, "China's Cyber Warfare Capabilities," 83.

339 Mulvenon, "PLA Computer Network Operations," 260–61.

340 DDOS attacks prevent a user's server from functioning by overloading the server with too many requests; Mulvenon, "PLA Computer Network Operations," 279–80; Lindsay, "Introduction," 18; Lindsay, "Inflated Cybersecurity Threat"; ThreatConnect and DGI, *China's Unit 78020*, 15; Heginbotham et al., *U.S.-China Military Scorecard*, 272.

CNO employs cyber espionage as a preferential, targeted, and established method under China's CNO strategy are PLA Unit 78020's TRB functions of ISR, SIGINT, and COMINT collection on Southeast and East Asian nations in the South China Sea; and PLA Unit 61398's aggressive, operational CNE of Western targets. Unit 78020's focused Southeast Asian cyber espionage campaigns also highlight the distinct role cyber espionage plays in PLA modernization. Additionally, the principles outlined in China's CNO speak directly to China's use of aggressive CNA, CNE, and CND methods to accomplish its military and national objectives.

This chapter outlines the organization of China's cyber functions under the CCP and PLA and discusses China's CNO principles to show that the PLA employs cyber espionage as a deliberate and conscious cyber method. Since this chapter establishes that cyber espionage assists the PLA in its domestic, regional, and target-specific cyber operations, Chapter V demonstrates that cyber espionage assists the PLA in its modernization—but not to an exclusive degree.

V. PLA CYBER AND NON-CYBER ACQUISITION METHODS

U.S. defense and news reports often compare noted examples of Chinese CNE with individual cases of modernized PLA equipment to explain the rapid pace at which the PLA advances.[341] These reports, however, discount the role alternate acquisitions—technology transfers, traditional espionage, and indigenous R&D—also play in PLA modernization.[342] While studies of China's CNE provide insight into how it implements CNO, the studies do not fully illustrate how cyber espionage fits into PLA modernization.

As demonstrated by PLA Unit 61398's increased CNE from 2006–2013 (Figure 6), China has an established, growing record of cyber espionage. Figure 6 shows China's pronounced CNE use but does not distinguish if these operations assist the PLA. This chapter engages in this discussion through comparing the following: examples of Chinese cyber espionage cases with their targets; the PLA's alternate acquisitions methods; and developmental timelines of the PLA's modernized platforms. This comparison establishes the role state-sponsored cyber espionage plays in PLA modernization.[343]

Figure 5. Timeline of PLA Unit 61398's CNE Incidents from 2006–2013

Source: "APT 1: Exposing One of China's Cyber Espionage Units," Mandiant (February 2013), 20, http://intelreport.mandiant.com/.

[341] *Annual Report to Congress: 2015*, 22, 35; *Annual Report to Congress: 2014*, 35; Heginbotham et al., *U.S.-China Military Scorecard*, 24–25.

[342] Martinez et al., "Major U.S. Weapons Compromised"; "A List of the U.S. Weapons Designs and Technologies Compromised by Hackers," *Washington Post*, May 27, 2013, http://www.washingtonpost.com/world/national-security/a-list-of-the-us-weapons-designs-and-technologies-compromised-by-hackers/2013/05/27/a95b2b12-c483-11e2-9fe2-6ee52d0eb7c1_story.html; U.S.-China Economic and Security Review Commission. "Section 2: China's Cyber Activities," 244–48, 259; Pierluigi Paganini, "Chinese Hackers Hit Forbes Visitors with Zero-day Exploits," *Security Affairs*, February 12, 2015, http://securityaffairs.co/wordpress/33417/cyber-crime/chinese-hackers-hit-forbes.html.

[343] The examples in this section are not all-inclusive, they are a sampling of information from unclassified sources.

The exploited cyber espionage targets this chapter discusses are broken up into three categories: military, domestic development, and diplomatic targets. In distinguishing between these three categories, this study engages in a more accurate analysis and identification of cyber espionage campaigns that have the potential to directly assist the PLA and PLA modernization efforts. To further categorize Chinese cyber espionage targets, "military targets" include CNE and network intrusions committed against military entities, the DOD, defense firms, defense-contracted companies, or specific military platforms. "Domestic development targets" include cyber intrusions against private industries (Google or energy companies) for communications technology, semi-conductors, developmental metals, and alternate energy data. "Diplomatic targets" include foreign governments, multinational firms, or non-government organizations that correlate to CCP policy objectives. An example of a diplomatic target is the Chinese-sponsored CNE of Taiwanese government servers or the Dalai Lama's networks following Taiwanese and Tibetan dissidence movements. Taiwan and Dalai Lama networks are diplomatic targets because maintaining Chinese territorial integrity is a top domestic policy concern for the CCP.

A. CYBER ESPIONAGE

China and the PLA entities engage in state-sponsored cyber espionage. Numerous cases reinforce that statement: Author Franz-Stefan Gady reports, "At least 30,000 hacking incidents, more than 500 significant intrusions in DOD systems, at least 1,600 DOD computers penetrated, and more than 600,000 user accounts compromised…the amount of data extracted (50 terabytes) to be equal to five Libraries of Congress."[344] Since early 2000, reports of suspected Chinese cyber espionage of U.S. military and U.S. defense contractors have increased in frequency and magnitude. U.S. defense reports often make the key assumption, without establishing the basis, that cyber espionage is the key driver behind the PLA's modernization efforts.[345] This section, however, establishes

[344] Franz-Stefan Gady, "New Snowden Documents Reveal Chinese Behind F-35 Hack," *Diplomat*, January 27, 2015, http://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/.

[345] U.S.-China Economic and Security Review Commission. "Section 2: China's Cyber Activities," 244–48; Ball, "China's Cyber Warfare Capabilities," 88; Krekel, *Capability of the People's Republic*, 51.

the foundation that defense reports do not. This section and Table 3 specifically, present examples of Chinese cyber espionage on U.S. targets and compares the responsible entity with the type of exploited target (military, economic, or diplomatic). A CNE target study and identification of responsible entities (whether government, military, or private) highlights how these cyber espionage potentially corresponds to PLA modernization or domestic developmental goals. This section's comparison demonstrates the role cyber espionage plays in CCP priorities and PLA modernization objectives.

1. A Study of Cyber Espionage Campaigns and Their Targets

The PLA cannot be singled out for CNE of foreign military targets because it is not the only Chinese entity that conducts cyber espionage: Chinese-attributed CNE entities range from the PLA, government entities, Chinese universities, individual non-government hackers, and corporate businesses. These entities, even if they are not government-sanctioned, also exploit military and defense information. As Table 3 shows, China's CNA, CNE, and CND missions are not exclusive to government or PLA entities: suspected PLA-sponsored cyber espionage does not always exploit military targets, and individual or university-sponsored hackers do not exclusively strike economic or private industry targets.[346] The correlations in the data, however, match the CCP's domestic and military developmental objectives shown in Tables 3, 4, and 5 and outlined in Figure 6. Yet it remains unclear how the specific data exfiltrated was subsequently utilized. These reports do not specifically detail if the information was put to use for PLA modernization or CCP domestic and foreign policy objectives.[347] If in the future new information emerges that details how the exploited information was employed, the findings of this section may need to be modified.

Table 3 has been created by synthesizing data from a wide range of sources that include government-sponsored studies, scholarly articles and books, private security firm publications, and media reports. The entries in this table are organized by their operation code name and the hacking group that exploited the target. Each listed CNE entry may be

[346] Ball, "China's Cyber Warfare Capabilities," 88–89.

[347] Krekel, *Capability of the People's Republic*, 69–70.

comprised of several campaigns or a singular campaign but are grouped into one entry to delineate them by their exploiting entity and code name. The "PRC-attributed entity" is compiled from multiple open-source references that list the same hacking group for the CNE operations. The "year of attack" is approximated from its open-source reported end date. Several of the listed CNE operations lasted several years, which is noted with a date range under "year of attack."

This table also makes the assumption that all listed cyber operations were, in one way or another, government-sanctioned campaigns—whether directly sanctioned before the event or endorsed after its completion. Consequently, this table also demonstrates the range of hacking entities in China. As discussed in Chapter II, there are many Chinese government-sponsored cyber entities and many "underground hacking" entities that also contribute to Chinese-originating cyber espionage. This table is organized to show the overlapping target areas that indirect non-government entities and government-attributed actors pursue. Cyber espionage campaigns that exploited military targets are highlighted in green; economic targets are highlighted in gray, and diplomatic targets are highlighted in orange.

Table 3. Chinese Government-sponsored Cyberattacks and their Origins

Target	Exploited Technology or Information	Year of Attack	Cyber Operation Name	PRC-Attributed Entity	Target Category
U.S. OPM	Current, former, and future federal employee background information	2015	N/A	Inconclusive	**Diplomatic**
Avago Technologies & Skyworks Solutions	Cellular technology	2015	N/A	Chinese Tianjin Professors and Chinese nationals	**Economic**
ASEAN nations and countries involved in the South China Sea	Classified and sensitive government and military operations and developmental information	2010 - 2015	*Naikon APT*	PLA Unit 78020	**Military**

Target	Exploited Technology or Information	Year of Attack	Cyber Operation Name	PRC-Attributed Entity	Target Category
Multiple U.S. Defense and Financial Firms: Through Forbes website	Personal and technical information through zero-day vulnerabilities	2014	*Sunshop Group or Codoso*	Likely PRC government or PLA-sponsored Group	**Military and Economic**
Six U.S. Companies: Alcoa World Alumina Westinghouse Electric U.S. Steel Corp Allegheny Technologies United Steelworkers Union SolarWorld	Nuclear power, metal, and solar power information	2014	N/A	PLA Unit 61398	**Economic**
U.S. DOD	U.S. Transportation Command (U.S. TRANSCOM) information	2014	N/A	PLA	**Military**
Multinational Financial Firms and G-20 Government Networks	Unspecific	2013	*Calc Team*	Likely PRC government or PLA-sponsored Group	**Diplomatic**
U.S. DOD, Lockheed Martin, Northrup Grumman, and Raytheon System Departments: F-35 Airframe V-22 Airframe C-17 Airframe UH-60 Black Hawk Helicopter Littoral Combat Ship Global Hawk	Blueprints, schematics and technical data for compromised equipment; technical data for satellite, radar, nanotechnology, electronic warfare systems, and personnel information	Mid-2000 to 2013	*Comment Crew*	Likely PLA	**Military**

Target	Exploited Technology or Information	Year of Attack	Cyber Operation Name	PRC-Attributed Entity	Target Category
Unmanned Aerial System Aegis Ballistic Missile Defense System Advanced Medium-Range Air-to-Air Missile (AMRAM) Patriot Advanced Capability Air Defense System					
Three U.S. Media Firms: *Wall Street Journal* *Washington Post* *New York Times*	Journalists research on PRC Government topics and leaders	2012	*Calc Team*	Likely PRC government or PLA-sponsored Group	**Diplomatic**
Multinational Defense and Commercial Firms	Defense Information and personal communications	2011	*Luckycat*	Sichuan University Individual and Group of Hackers	**Military and Economic**
48 Multinational Firms	Chemical and Defense Information and personal communications	2011	*Nitro*	Individual Hacker	**Economic**
American Superconductor (AMSC)	Source codes and AMSC software	2011	N/A	Chinese Energy Firm: Sinovel Wind Group	**Economic**
Multinational 100+ Financial and Defense Firms	Linked to *Operation Aurora:* Unspecific	2009	*Hidden Lynx*	Potentially PRC government-contracted Hacker Group	**Military and Economic**
U.S.-Taiwan Policy Think Tanks	U.S. Assistance Plans for Taiwan Airforce upgrades	2008	*Taidoor*	Inconclusive	**Diplomatic and Military**
Google + 34 Additional Internet Firms	Gmail and Internet email applications	2009	*Operation Aurora*	Potentially PRC government-contracted Hacker	**Diplomatic and Economic**

Target	Exploited Technology or Information	Year of Attack	Cyber Operation Name	PRC-Attributed Entity	Target Category
				Group	
U.S., Western, and Southeast Asian companies	Classified and sensitive government information from cloud-based media	2009	*Shadows in the Cloud*	Inconclusive	**Diplomatic and Economic**
Multinational Oil and Energy Companies	Oil Drilling Control Information and personal communications	2009	*NightDragon*	Likely Non-PLA Entity	**Economic**
71 Government and Corporate Entities (Including U.S. and International Organizations): International Olympic Committee World Anti-Doping Agency United Nations ASEAN South Korean Steel Firms U.S. Department of Energy U.S. Defense Contractors U.S. States and counties	Chinese Government Priority Targets: emails, legal documents, and design schematics, local government information, and intellectual property	2006-2009	*Shady Rat*	Likely PLA Unit 61398	**Diplomatic, Military, and Economic**
U.S. Lockheed-Martin and Northrup-Grumman; United Kingdom BAE Systems	U.S. F-35 Joint-Strike Fighter Technical Data	2007	N/A	Likely PLA Entity	**Military**
Multinational Firms and Government Networks in 103+ countries (Including a	Unspecific	2007	*Ghost Net*	Inconclusive	**Diplomatic**

Target	Exploited Technology or Information	Year of Attack	Cyber Operation Name	PRC-Attributed Entity	Target Category
cyberattack on the Dalai Lama)					
U.S. Office of the Secretary of Defense: Robert Gates	Computer applications and personal communications	2007	N/A	PLA	**Diplomatic and Military**
Approximately 141 Western Firms in 15+ countries: Coca-Cola	Exploited firms, technology, and information related to PRC national goals	2006	*Comment Crew*	PLA Unit 61398	**Economic**
U.S. Defense Firms and National Labs	Unspecific	2003	*Titan Rain*	Inconclusive	**Military and Economic**
U.S. DOD, U.S. Department of State, International Monetary Fund, World Bank, + Additional International and Non-governmental Firms	Personal communications, strategic planning, and personnel files	2002	*Byzantine Hydes*	PLA	**Military and Diplomatic**

Author's Table Created from the Following Sources: Dmitri Alperovitch, "Revealed: Operation Shady RAT," McAfee, 2–4, 6–9, accessed June 3, 2015, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf; "APT 1: Exposing One of China's Cyber Espionage Units," Mandiant (February 2013), 23–24, http://intelreport.mandiant.com/; "Beyond the Breach: 2014 Threat Report," M-Trends, Mandiant (2014), 16–18, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf; *Bird's Eye View Report,* no. 1, Novetta Threat Research Group (March 2015), 2, http://www.novetta.com/wpcontent/uploads2014/11/BirdsEyeView_001_March_2015.pdf; Joey Cheng and Kevin McCaney, "Cyber Charges against China Could Raise the Stakes for U.S. Command," Defense Systems, last modified May 19, 2014, https://defensesystems.com/articles/2014/05/19/us-china-cyber-charges.aspx; Christian de Looper, "Chinese Hackers Piggybacked Forbes.com to Attack U.S. Defense and Financial Industry Computers," *Tech Times,* February 11, 2015, http://www.techtimes.com/articles/32139/20150211/chinese-hackers-piggybacked-forbes-com-to-attack-us-defense-and-financial-industry-computers.htm; John E. Dunn, "Chinese 'Hidden Lynx' Hackers behind Major Cyberattacks on U.S., Claims Symantic," Tech World, last modified September 17, 2013, http://www.techworld.com/news/security/chinese-hidden-lynx-hackers-behind-major-cyberattacks-on-us-claims-symantec-3469248/; Michael Joseph Gross, "Exclusive: Operation Shady Rat-Unprecedented Cyber-espionage Campaign and Intellectual-Property Bonanza," *Vanity Fair,* September 2011, http://www.vanityfair.com/news/2011/09/operation-shady-rat-201109; Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (McLean, VA: Northrup Grumman, 2009),

67–74, http://online.wsj.com/public/resources/documents/chinaspy20091022.pdf; Jon R. Lindsay, "The Impact of China Cybersecurity: Fiction and Friction," *International Security* 39, no. 3 (Winter 2014–2015): 22–23, http://belfercenter.hks.harvard.edu/files/IS3903_pp007-047.pdf; Jon R. Lindsay and Tai Ming Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain,* ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), 58–59; "A List of the U.S. Weapons Designs and Technologies Compromised by Hackers," *Washington Post*, May 27, 2013, http://www.washingtonpost.com/world/national-security/a-list-of-the-us-weapons-designs-and-technologies-compromised-by-hackers/2013/05/27/a95b2b12-c483-11e2-9fe2-6ee52d0eb7c1_story.html; Luis Martinez et al., "Major U.S. Weapons Compromised by Chinese Hackers, Report Warns," *ABC News*, May 28, 2013, http://abcnews.go.com/Blotter/major-us-weapons-compromised-chinese-hackers-report-warns/story?id=19271995; Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies," *Washington Post*, May 27, 2013, https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html; Pierluigi Paganini, "Chinese Hackers Hit Forbes Visitors with Zero-day Exploits," *Security Affairs*, February 12, 2015, http://securityaffairs.co/wordpress/33417/cyber-crime/chinese-hackers-hit-forbes.html; "Significant Cyber Incidents Since 2006," Center for Strategic International Studies, last modified July 13, 2015, http://csis.org/files/publication/150714_Significant_Cyber_Events_List.pdf; *Project Camerashy: Closing the Aperture on China's Unit 78020* (Arlington, VA: ThreatConnect and Defense Group, Inc. [DGI], 2015), 8–10, 12, 15–16, 20, 23, 74, https://www.threatconnect.com/camerashy/; "Piercing the Cow's Tongue: China Targeting South China Seas Nations," ThreatConnect, last modified May 19, 2014, http://www.threatconnect.com/piercing-the-cows-tongue-china-targeting-south-china-seas-nations/;Timothy L. Thomas, "China's Cyber Incursions: A Theoretical Look at What They See and Why They Do It Based on a Different Strategic Method of Thought," *OE Watch* (March 2013): 12–13, 21–22, http://fmso.leavenworth.army.mil/documents/China's-Cyber-Incursions.pdf; U.S.-China Economic and Security Review Commission, "Section 2: China's Cyber Activities," 2013 Annual Report to Congress (Washington, DC: USCC), 244–48, http://origin.www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%202%3B%20Section%202%20China%27s%20Cyber%20Activities.pdf.

2. Cyber Intrusions that Likely Assisted PLA Modernization

This study identifies which CNE operations exploited which target types. The evidence shows that certain cyber espionage—those that were PLA-sponsored and employed against military targets—likely aided the PLA's modernization. Examples that exploited military targets that also came from Chinese government- or PLA-sponsored entities to represent the CNE that likely aided PLA operations and modernization efforts. Upon analyzing the targets in Table 3, eight[348] of the 24 total entries involved direct

[348] The percentages are approximate because some of the CNE operations could be classified under several categories due to the wide variance of targets pursued under individual attacks.

targeting of U.S. DOD and Defense Firms, and hence are listed as potential intrusions that assisted PLA modernization efforts: *Byzantine Hydes, Shady Rat,* 2007 F-35 exploit, *Hidden Lynx,* mid-2000-2013 *Comment Crew* military systems exploit, 2014 U.S. Transportation Command (TRANSCOM) exploit, *Sunshop Group, and Naikon APT*. For example, *Shady Rat* and *Byzantine Hydes* are classified as cyber intrusions that likely aided PLA modernization because their origination point came from a PLA entity, and their targets are U.S. Defense Firms and military contractors.

U.S. government information released after the Edward Snowden information leaks confirmed that the Chinese exfiltrated sensitive engine-functioning data, radar technology, missile guidance, and stealth technology from the U.S. F-22 and F-35 fighter aircrafts (fifth generation fighter jets).[349] Reports subsequently indicate the cyber exploitation of the U.S.'s fifth generation fighter critical program information (CPI) technology directly correlate to and resulted in the PLA's development of its fifth generation multirole J-31 and J-20 fighter aircrafts.[350] The overlapping cyber exploitation data also shows parallels to China's CNO doctrine and DWP objectives. The PLA-sponsored cyber exploitation of specific U.S. military platform technical data and schematics (F-22, F-35, Littoral Combat Ship, Global Hawk UAS) from mid-2000-2013, and the 2014 PLA's suspected cyberattack on TRANSCOM match the PLA's modernization goals: China's 2015 white papers stress building "a modern system of military forces" and a PLA capable of "mobile operations and multi-dimensional offense and defense."[351] Specifically, the DWPs stress improving the PLA Army's "trans-theater"[352] transportation capabilities; advancing the PLA's missile and precision-guided weaponry; refining the PLA's logistics and support systems; and "[optimizing] its nuclear force structure.[353] Although it is unclear how the targeted information was used, these

[349] Gady, "New Snowden Documents Reveal F-35 Hack."

[350] Ibid.

[351] "Document: China's Military Strategy."

[352] Ibid.

[353] Ibid.

DWP objectives suggests that if Chinese government or PLA entities exploited foreign military technical data, they would use it to further DWP goals.

The *Titan Rain* and *Luckycat* cyber intrusions targeted DOD networks and could have provided critical information about U.S. military systems that would aid the PLA's modernization progress; however, based on open source information, their origination point was a non-government or inconclusive entity, which was not directly tied to the PLA.[354] Consequently, since the originating source of the cyber intrusion is not directly linked to the PLA, a direct link cannot be drawn between the exploited defense information and its assistance in PLA modernization goals.

PLA-attributed CNE did not always exploit military or U.S. defense contractor systems. Cyber intrusions, like the PLA's cyber intrusions into U.S. Secretary of Defense Robert Gates' office computers are labeled as "diplomatic targets," rather than as "military targets" because they did not directly exploit modern U.S. military equipment: the cyber intrusion targeted Gates' personal communications and computer applications.

Apart from the military-related cyber espionage operations, there are also a similar percentage of economic development CNE-directed attacks. The relatively even breakdown between each CNE target area indicates that Chinese cyber espionage is not exclusively devoted to PLA modernization objectives; it also suggests that Chinese cyber espionage is potentially dedicated toward broader goals set by the CCP and not exclusively toward the PLA's advancement.

3. Cyber Intrusions that Likely Aided Chinese Domestic Development Objectives

To continually progress its domestic development, China uses Five-Year Plans (FYP) and Medium and Long Term Plans for Science and Technology Development (MLP) as developmental guidelines. These plans outline developmental focus areas that are responsive to domestic and international conditions China faces. The objectives in each plan also correlate to some of the exploited CNE targets in Table 3. In order to discuss the cyber espionage campaigns that likely aided China's domestic development

[354] Krekel, *Capability of the People's Republic*, 38, 68–69.

objectives, this section first provides an outline of the CCP's developmental priorities since 1990 to engage in an accurate comparison of the developmental objectives and Chinese CNE operations. Since the CCP is the premier authority in China, policies, plans, and developmental objectives are set at the top and delegated downward. This section examines the CCP's domestic policies that influence the targets and objectives pursued under China's CNO and also occupy a portion of China's state-sponsored cyber espionage agenda.

a. Five-Year Plans

China's FYPs set industrial, military, and societal development benchmarks for China to achieve every five years.[355] Earlier FYPs were geared toward major economic improvements, but recent plans are oriented toward PLA modernization and technological development.[356] While the variance in plans (as Table 4 shows) gives insight into the CCP's foreign and domestic policy priorities, the FYPs are also domestically unifying instruments. The CCP uses FYPs to motivate government, military, and private citizens toward shared goals that improve the quality of life, economy, and military in China.[357]

---

[355] Theodore Shabad, "Communist China's Five Year Plan," *Far Eastern Survey* 24, no. 12 (December 1955): 189–91, doi: 10.2307/3023788; Joseph Casey and Katherine Koleski, *China's 12th Five-Year Plan*, U.S.-China Economic & Security Review Commission, 1, last modified June 24, 2011, http://www.uscc.gov/sites/default/files/Research/12th-FiveYearPlan_062811.pdf.

[356] Inkster, "Chinese Intelligence Agencies," 42; Hachigian, "China's Cyber-Strategy," 119; C. Cindy Fan, "China's Eleventh Five-Year Plan (2006-2010): From 'Getting Rich First' to 'Common Prosperity," *Eurasian Geography and Economics* 47, no. 6 (2006): 716–17, http://www.sscnet.ucla.edu/geog/downloads/597/300.pdf.

[357] Casey and Koleski, *China's 12th Five-Year Plan*, 1–2, 14; Fan, "China's Eleventh Five-Year Plan"): 708.

Table 4. Comparison of Previous Five-Year Plans (1996–2015)

FYP Name	Years Covered	Release Date	China's Strategic Emerging Industries (SEIs) Identified for Development
12th Five-Year Plan	2010-2015	March 2011	- Clean Energy technology - Clean energy vehicles - Next generation information technology - Biotechnology - New materials - High-end equipment manufacturing - Alternative energy
11th Five-Year Plan	2006-2010	March 2006	- Biotechnology - Next-generation information technology - High-end equipment manufacturing - Alternative energy
10th Five-Year Plan	2001-2005	March 2001	- Next generation information technology - Communications technology - Telecommunications technology - High-end equipment manufacturing - Agricultural technologies
9th Five-Year Plan	1996-2000	March 1996	- Higher education institutions - Telecommunications technology - Next-generation information technology - Transportation methods

Adapted from: Joseph Casey and Katherine Koleski, *Backgrounder: China's 12th Five - Year Plan*, U.S.-China Economic & Security Review Commission, 8, 18–19, last modified June 24, 2011, http://www.uscc.gov/sites/default/files/Research/12th-FiveYearPlan_062811.pdf; "China Reports Investment figures for Ninth Five-Year Plan Period," *BBC Monitoring Worldwide*, October 3, 2000, ProQuest (454370371); "China: Summary of the Tenth Five-Year Plan (2001-2005) – Information Industry," APCO China, trans. Ministry of Industry and Information Technology (China), 5–6, 8, 10, 12–13, 18–19, 24–25, accessed August 21, 2015, http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan022769.pdf; "China's Twelfth Five Year Plan (2011-2015) – the Full English Version," China Direct, last modified September 11, 2011, http://cbi.typepad.com/china_direct/2011/05/chinas-twelfth-five-new-plan-the-full-english-version.html; C. Cindy Fan, "China's Eleventh Five-Year Plan (2006-2010): From 'Getting Rich First' to 'Common Prosperity," *Eurasian Geography and Economics* 47, no. 6 (2006): 708–09, 713, http://www.sscnet.ucla.edu/geog/downloads/597/300.pdf; National People's Congress and Chinese People's Political Consultative Conference (NPC&CPPCC), "The 8th Five-Year Plan (1991-1995)," last modified February 23, 2011, http://www.chinadaily.com.cn/china/2011npc/2011-02/23/content_12068062.htm; Mao Zhongying, ed., "China's New S&T Development Plan," *China Science and Technology Newsletter*, no. 456 (Beijing, China: Ministry of Science and Technology, November 10, 2006), http://www.most.gov.cn/eng/newsletters/2006/200611/t20061110_37960.htm; Zhu Rongji, "Report on the Outline of the Tenth Five-Year Plan for National Economic and Social Development (2001)" (speech, Fourth Session of the Ninth National People's Congress, China, March 5, 2001), http://www.gov.cn/english/official/2005-07/29/content_18334.htm.

As Table 4 highlights, FYP objectives have steadily evolved since 1996, from basic Internet development to high-end IT. Ever since the CCP welcomed the Internet into China, FYP objectives have shifted to incorporate technological development.[358] Upon comparing the 9th FYP's objectives with subsequent FYPs, a noticeable shift in CCP priorities can be seen—from heavy manufacturing to IT equipment, education, and applications.[359] China's 12th FYP celebrates China's successes in technological breakthroughs and software industries while simultaneously noting its lack of domestic innovation and R&D capacities.[360] One would expect that if China is having technological breakthroughs that it would also show progress in domestic innovation and R&D capacities—unless those breakthroughs were a result of cyber espionage.

As Table 4 and Figure 6 show, China's 12th FYP emerged in 2011 and emphasized modernizing the PLA, continuing China's economic growth, and developing China's cyber capabilities to protect China's core interests; these objectives subsequently affected the developmental pace and scope of China's cyber strategy.[361] The key development goals outlined in the 12th FYP are related to seven strategic emerging industries (SEI): aeronautical and space systems, IT, nanotechnology, and research, development, and acquisitions (RDA) processes (listed in Table 4 and Figure 6).[362] The 12th FYP objectives (and former FYPs) correlate to Chinese CNE targets, which indicates the high degree to which the FYPs also influence China's cyber espionage targets.

---

358 Hachigian, "China's Cyber-Strategy," 121.

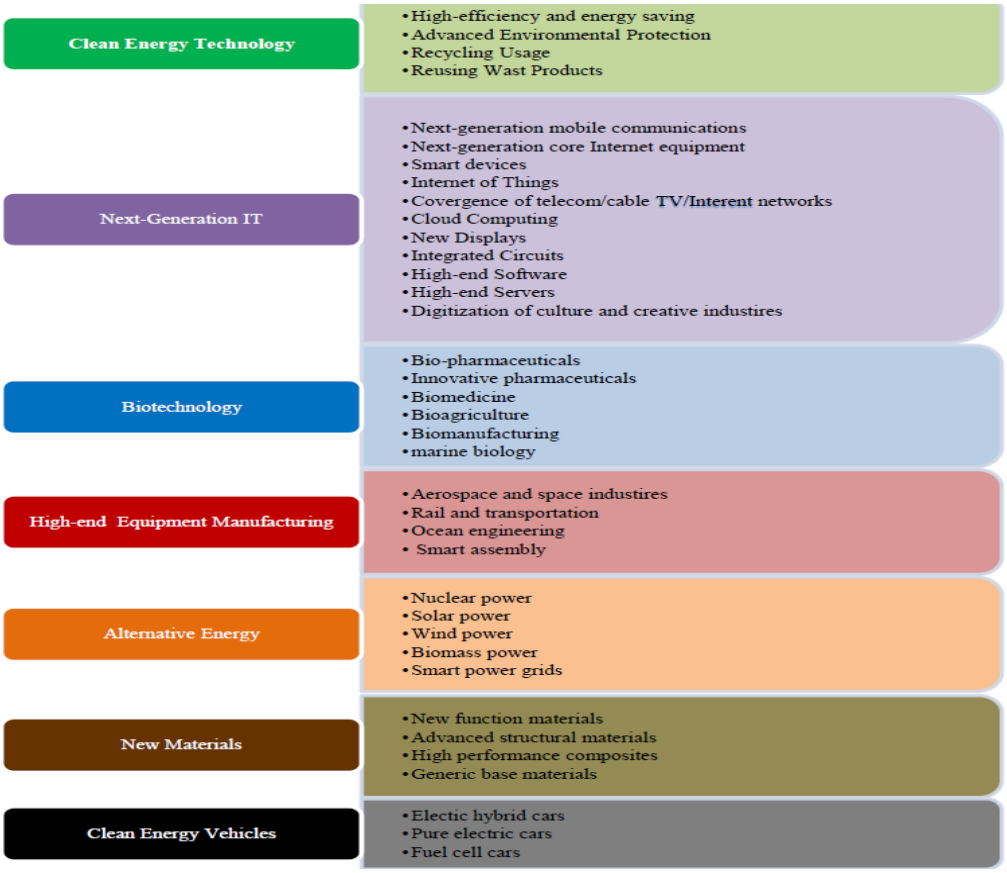
359 National People's Congress and Chinese People's Political Consultative Conference (NPC&CPPCC). "The 8th Five-Year Plan (1991-1995)," last modified February 23, 2011, http://www.chinadaily.com.cn/china/2011npc/2011-02/23/content_12068062.htm.

360 "The Tenth Five-Year Plan,," China Information Center, accessed August 22, 2015, http://www.china.org.cn/english/features/38198.htm; "China: Summary of the Tenth Five-Year Plan (2001-2005) – Information Industry," APCO China, trans. Ministry of Industry and Information Technology (China), 5–6, 8, 10, 12–13, accessed August 21, 2015, http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan022769.pdf; Zhu Rongji, "Report on the Outline of the Tenth Five-Year Plan for National Economic and Social Development (2001)" (speech, Fourth Session of the Ninth National People's Congress, China, March 5, 2001), http://www.gov.cn/english/official/2005-07/29/content_18334.htm.

361 Stokes, "Chinese People's Liberation Army Computer Network," 163; *Annual Report to Congress: 2014*, 32–33; Casey and Koleski, *China's 12th Five-Year Plan*, 1–2, 18.

362 *Annual Report to Congress: 2015*, 53; *Annual Report to Congress: 2014*, 15, 27–28, 30–31; Casey and Koleski, *China's 12th Five-Year Plan*, 8–9, 18–19.

Figure 6. 12th FYP Strategic Emerging Industries Targeted for Development



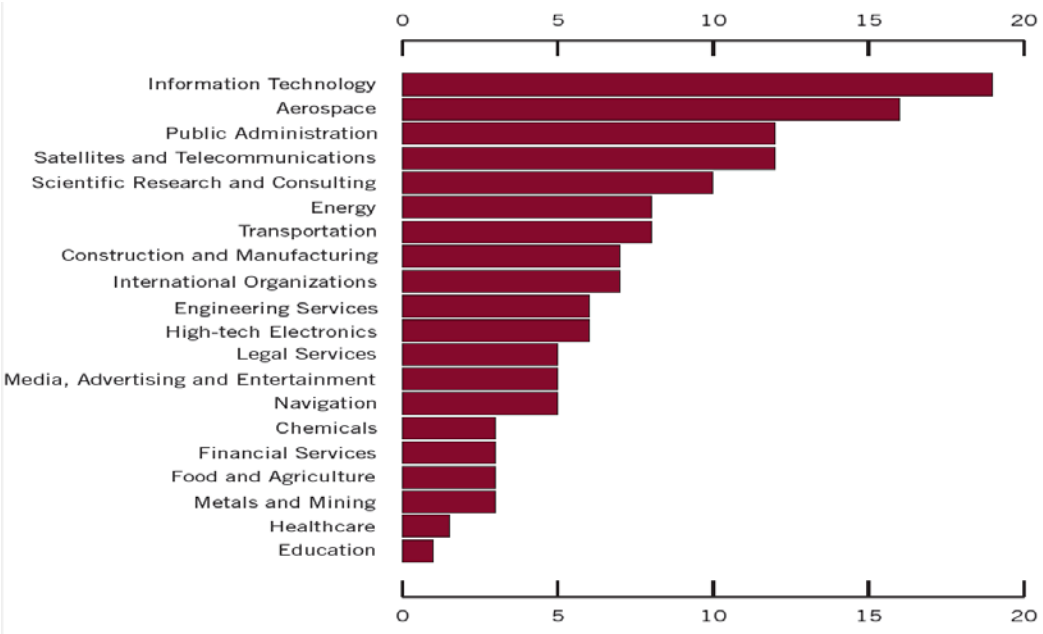
Source: Joseph Casey and Katherine Koleski, *Backgrounder: China's 12th Five -Year Plan*, U.S.-China Economic & Security Review Commission, 19, last modified June 24, 2011, http://www.uscc.gov/sites/default/files/Research/12th-FiveYearPlan_062811.pdf.

The parallels between China's economic cyber espionage and FYP development areas strongly suggest China's cyber strategy and the methods employed under that strategy are influenced by FYP objectives (as Figure 6 demonstrates). The 2015 Chinese cyber espionage of Avago Technologies and Skyworks Solutions cellular technology matches the next-generation IT and next-generation mobile communication goal; the 2014 PLA-sponsored CNE of six U.S. energy companies for nuclear power, solar power, and steel manufacturing information matches the alternate energy source, clean energy technology, and new materials development goals; the 2014 PLA-sponsored attack on U.S. TRANSCOM matches the high-end equipment manufacturing development goal.[363]

[363] "U.S. Indicts 6 Chinese Citizens"; Martinez et al., "Major U.S. Weapons Compromised."

Put another way, each of the seven SEIs listed in Figure 6 have corresponding CNE operations in Table 6 that exploited those specific technologies. These links between Chinese CNE and China's national objectives suggests that cyber espionage is part of a larger Chinese cyber strategy; it also suggests that the FYPs affect China's strategic cyber orientation. PLA Unit 61398's exploitation history of corresponding FYP objectives (in Figure 7) further exemplifies this point that FYPs influence China's CNE targeting. China's MLP also impacts China's cyber strategy, which will be discussed in the following section.

Figure 7. Examples of PLA Unit 61398's CNE Targeted Industries by Type and Number of Attacks



Source: "APT 1: Exposing One of China's Cyber Espionage Units," Mandiant (February 2013), 24, http://intelreport.mandiant.com/.

b. Medium- and Long-Term Plans for the Development of Science and Technology

Since 1956, China's MLPs serve as the country's "grand blueprint for science and technology development."[364] MLPs are released every 15 years to supplement the FYPs.[365] China's MLPs also exemplify domestic policies that impact China's cyber strategy as well as the tactics, techniques, and procedures (TTP) employed under that strategy.[366] The MLP is released by China's Ministry of Science and Technology and provides the guidelines for China's S&T development, as Table 5 shows.[367]

Table 5. China's 2006–2020 MLP

Title	Years Covered	Core Concepts	Target Advancement Areas
The National Program 2006–2020 for the Development of Science and Technology in the Medium and Long Term"	2006 - 2020	*Domestic innovation, R&D breakthroughs, technology-oriented domestic growth and development, forward-leaning posture*	- Biotechnology - Alternative energies - Information technology - High-end equipment manufacturing - Oceanology - Space and Aviation technology

Adapted from: Mao Zhongying, ed., "China's New S&T Development Plan," *China Science and Technology Newsletter*, no. 456 (Beijing, China: Ministry of Science and Technology, November 10, 2006), http://www.most.gov.cn/eng/newsletters/2006/200611/t20061110_37960.htm; Yang Lei, ed., "Innovation 'Motive Power for Development,'" *Xinhua*, January 11, 2006, http://www.gov.cn/english/2006-01/11/content_220696.htm.

364 Lindsay, "Impact of China on Cybersecurity: Fiction and Friction," 22; James McGregor, *China's Drive for 'Indigenous Innovation': A Web of Industrial Policies*(Washington, DC: U.S. Chamber of Commerce, 2010), 4, 8, https://www.uschamber.com/report/china%E2%80%99s-drive-indigenous-innovation-web-industrial-policies; Sylvia Schwaag Serger and Magnus Breidne, "China's Fifteen-Year Plan for Science and Technology: An Assessment," *Asia Policy*, no. 4 (July 2007): 138, doi: 10.1353/asp.2007.0013.

365 Mao Zhongying, ed., "China's New S&T Development Plan," *China Science and Technology Newsletter*, no. 456 (Beijing, China: Ministry of Science and Technology, November 10, 2006), http://www.most.gov.cn/eng/newsletters/2006/200611/t20061110_37960.htm.

366 McGregor, China's Drive for 'Indigenous Innovation,' 4.

367 Mao, "China's New S&T Development Plan"; Yang Lei, ed., "Innovation 'Motive Power for Development,'" *Xinhua*, January 11, 2006, http://www.gov.cn/english/2006-01/11/content_220696.htm.

The SEIs outlined in China's current MLP match the biotechnology, alternative energies, information technology, and high-end equipment manufacturing SEIs in China's 12th FYP; therefore, the aforementioned examples of Chinese CNE of FYP objective targets also match the MLP's developmental objectives (also exemplified by Figure 7). The difference between FYPs and MLP is the MLP's addition of specific ocean, aviation, and space technologies. The 2001–2013 CNE of U.S. defense contractor airframe and combat ship schematics, and the 2011 Chinese cyber espionage of multinational defense contractor firms match the MLP's specific technology development objective.[368] The correlation between Chinese CNE and MLP objectives suggests Chinese cyber espionage is also focused on developing domestic economic objectives, not just PLA modernization-related targets. Additionally, this multiplicity of objectives hints that cyber espionage might not be an exclusive driver for PLA modernization. While the use of cyber espionage in several development areas is not direct evidence of its limited role in PLA modernization, Section B (the next major section) of this chapter presents other evidence to corroborate this observation.

c. A Comparison of China's Developmental Goals and Cyber Espionage

As previous sections discuss, China's FYPs and MLPs identify clean energy, advanced information technology (cloud computing), biotechnology, high-quality R&D and manufacturing (aerospace, space, and transportation sectors), alternate energy sources (nuclear and solar), new materials, and clean energy vehicles (space, sea, and aerospace) SEIs as critical development areas.[369] An examination of the domestic developmental targets in Table 3 suggests 10 or 11 of the 24 entries assisted national economic and development goals: the 2015 Chinese university exploitation of cellular technologies; the 2014 PLA Unit 61398 CNE of six U.S. alternative energy and manufacturing companies; *Nitro*; 2011 American Semiconductor (AMSC) cyber intrusion; *Hidden Lynx; Operation Aurora*; *Shadows in the Cloud*; *NightDragon;* 2006 *Comment Crew* exploitation of Western firms; *Shady Rat; Titan Rain*. Some of these

368 "APT 1," 2–5; "List of U.S. Weapons Designs Compromised"; U.S.-China Economic and Security Review Commission. "Section 2: China's Cyber Activities," 244–48.

369 Casey and Koleski, *China's 12th Five-Year Plan*, 8–9, 18–19.

operations, while they may have primarily targeted another area (like diplomatic or military targets) are also listed in this category for the economic impact they also potentially had.

Even if the attributed entity was not a government or PLA entity, the cyber intrusions are categorized as assisting China's developmental goals because the exploited information matches the CCP's developmental objectives, and the information was extracted from foreign governments back to domestic Chinese servers. For example, in 2011, a Chinese Energy Firm, Sinovel Wind Group, was a private entity that exploited AMSC software. Sinovel's exploitation contributes to China's FYP and MLP objectives of developing "alternative energy technologies" SEIs, even if it was not directly government-sponsored. In addition, upon comparing suspected Chinese CNE with the 12th FYP's SEIs, there are strong parallels: the 2014 PLA-sponsored intrusion on six U.S. energy companies for nuclear power, solar power, and steel manufacturing information matches the alternate energy source development and new materials goals; the 2014 PLA-sponsored attack on U.S. TRANSCOM matches the high-end equipment manufacturing development goal.

While this study uses delineates diplomatic targets by their information and point of destination (in China), Lindsay notes the challenges of relying on this information: "Although Western cyber defenders can observe the exfiltration of petabytes of data to Chinese servers, they cannot…measure China's ability to use the data."[370] This study acknowledges Lindsay's demonstration of the difficulty of directly ascertaining how China employs exploited data and uses the above presented information to primarily demonstrate the range of cyber actors and target areas China pursues. Additionally, these parallels in Chinese CNE and developmental goals underscores that cyber espionage is not an exclusive tool used to modernize the PLA military.

4. Cyber Intrusions that Likely Aided CCP Foreign Policy Objectives

Breaking down the non-military targets in Table 3 further, an analysis of the targets suggests nine or ten of the 24 entries could have been CCP-directed against

[370] Lindsay, "Impact of China Cybersecurity: Fiction and Friction," 24.

diplomatic targets: 2015 OPM data exploitation, 2013 *Calc Team* exploitation of multinational firms, 2012 *Calc Team* exploitation of U.S. media companies, *Taldor*, *Operation Aurora, GhostNet*, *Shadows in the Cloud*, 2007 PLA exploitation of U.S. Secretary of Defense servers, and *Shady Rat*. The 2006–2009 *Shady Rat* operation was an example of a diplomatic target-oriented CNE operation that did not fall under developmental or PLA modernization goals but was crucial to CCP foreign policy objectives. This cyber espionage campaign is significant because it coincided with the 2008 Beijing-sponsored Olympics. The 2006 PLA-sponsored cyber intrusion on the International Olympic Committee and the World Anti-Doping Agency matched China's foreign policy aspirations to excel at hosting and participating in the Olympic Games.

Military-related targets represent approximately one-third of the cyber espionage cases in Table 3; economic developmental-related targets represent the largest portion of the cyber espionage cases with a little more than one-third of the examples; and diplomatic CCP-prioritized targets represent approximately a little less than one-third of the cyber espionage cases. China's cyber espionage has a divided subject focus as the relatively even breakdown between military-development, economic-development, and foreign-policy aiding cyber espionage targets highlights.

The preceding analysis also suggests state-sponsored cyber espionage is not an exclusive driver for PLA modernization. At the very least, the distribution of cases across three developmental target categories suggests that the PRC does not feel the need to allow PLA modernization to monopolize current cyber espionage resources. In order to test this indication that cyber espionage is not the exclusive mechanism behind PLA modernization, the next section examines the PLA's alternate acquisitions methods.

B. ALTERNATE ACQUISITION METHODS

As previously discussed, in the wake of the PLA's reduced defense budget and increased focus on China's economic development during the first wave of PLA modernization, the PLA had to cultivate a military that was business-minded, economically savvy, and an independent fund-raiser. As a result, the PLA cultivated a robust acquisitions system that was cost effective, efficient, and kept PLA modernization

moving forward. This acquisitions system, prior to the emergence of the Information Age, included traditional espionage of foreign military and trade secrets, overt purchases of Russian and Southeast Asian military platforms (and then abuse of licensing through reverse engineering and copycat production without licenses), technology agreements with Western nations, and domestic R&D. This section examines the PLA's alternate procurement, acquisitions, and R&D methods (apart from cyber espionage) to delimit the role cyber espionage has played in advancing PLA modernization efforts.

1. Foreign Technological Assistance and Trade Agreements

The PLA has not exclusively relied on cyber data exfiltration to modernize its military. When the modernization process began in 1978, the PLA did not yet have the technological means for cyber acquisitions; what the PLA did have, however, was a longstanding relationship with the Soviet Union.[371] In its infancy, the PLA could not conduct CNE, so it focused its efforts on physical technological procurement—through technology transfers with the Soviet Union first and then later with other countries.[372] Technological export restrictions limit China's access to Western technologies, but China has developed military procurement channels with Russia, the Middle East, and Southeast Asian partners to supplement this setback.[373] Reports on China's foreign technology acquisitions spending from 1991–2011, show a 300 percent increase in annual expenditures: from nine billion renminbi (RMB) in 1991 to 45 billion RMB in 2011.[374] China also encourages foreign firms to establish operations within China and invests in

[371] Chen Jian, *Mao's China and the Cold War: The New Cold War History*, ed. John Lewis Gaddis (Chapel Hill: South Carolina University Press, 2001), 44–45.

[372] Tai Ming Cheung, "The Role of Foreign Technology Transfers in China's Defense Research, Development, and Acquisition Process," The Study of Innovation and Technology in China Policy 2014, University of California Institute on Global Conflict and Cooperation (2014): 1–2, http://escholarship.org/uc/item/4dp213kd.

[373] Andrew Scobell, Michael McMahon, and Cortez A. Cooper III, "China's Aircraft Carrier Program: Drivers, Developments, Implications," Naval War College Review 68, no. 4 (Autumn 2015): 65–66, 68–71, https://www.usnwc.edu/getattachment/c96be200-d3a9-4b6f-9114-179169fa844e/China-s-Aircraft-Carrier-Program--Drivers,-Develop.aspx.

[374] In the late 1990s, these expenditures increased with the high inflation rates China face; however, in the mid- to late-2000s China's inflation rate has remained fairly steady which highlights the increased defense spending China is engaged in in relation to its national inflation rate; Zachary Keck, "China's Defense Budget: A Mixed Bag," *Diplomat*, March 8, 2014, http://thediplomat.com/2014/03/chinas-defense-budget-a-mixed-bag/; Lindsay and Cheung, "Exploitation to Innovation," 73.

foreign companies as part of its foreign acquisitions processes. These foreign investments allow China to engage in foreign technology transfers for military modernization purposes.[375]

China engages in negotiated technology procurement and licensing with countries around the world. China's foreign technology acquisitions are ranked just behind the United States, Japan, the United Kingdom, and Canada in total technology trade agreements per year.[376] Even though, Chinese companies have forged trade agreements with U.S. defense companies in the past, this section primarily presents examples of the PLA's overt acquisitions and technology trade agreements with Russia to because they specifically address exchanges of modernized military platforms.[377] This section's identification of procured military equipment also illustrates that cyber espionage is not the sole driver behind PLA modernization.

After Mao formed the PRC in 1949, the Soviet Union was the largest military equipment provider to China by supplying military designs, technical training, and Soviet experts on modernized military operations.[378] Following the Soviet Union's dismantlement in 1991, China made one of its most critical, military equipment purchases from the disadvantaged country: production licenses and parts for Russia's modernized fighter jet, the Sukhoi-27 (Su-27).[379] From 1994–1997, China also purchased Kilo-class submarines and Sovremenny-class destroyers from Russia in a mutually acceptable arms transfer. These were critical, modern military equipment purchases because they were missile-equipped naval technologies that China had neither acquired, nor developed. From the mid-1990s-2008, Russia provided China more than $30 billion in military

---

375 Lindsay and Cheung, "Exploitation to Innovation," 67–74; Cheung, "Role of Foreign Technology Transfers," 1.

376 Valencia Romei, "Chinese Appetite for Foreign Technology Could be Good News for Everyone," *Financial Times*, accessed November 2, 2015, http://blogs.ft.com/ftdata/2015/11/02/chinese-appetite-for-foreign-technology-companies-could-be-good-news-for-everyone/.

377 Jeremy Page, "China Clones, Sells Russian Fighter Jets," *Wall Street Journal*, December 4, 2010, http://www.wsj.com/articles/SB10001424052748704679204575646472655698844.

378 Page, "China Clones, Sells Jets"; Inkster, "Chinese Intelligence Agencies," 30.

379 Page, "China Clones, Sells Jets."

equipment, platform designs, and arms sales.[380] In 2014, China went under contract with Russia to purchase Russian S-400 long-range, self-guided surface-to-air missiles (SAM).[381] These military purchases from the Soviet Union, and later Russia, allowed China to adapt and assimilate critical technology to modernize PLA forces. These acquisitions also had an equally important role in modernizing the PLA. In addition to its negotiated purchases and technology trade agreements, China and the PLA also exercise traditional espionage operations to bolster preexisting military procurement processes.

2. Traditional Espionage Operations

In addition to technology acquisitions, traditional espionage has also played a supporting role in PLA modernization. Since the 1400s, China has used traditional espionage to obtain foreign military and industrial secrets, as have all powers, which underscores China's developed espionage TTPs. Since that time, China has used espionage to advance its domestic and military developmental goals helping China develop a robust espionage network that exploits military, diplomatic, and economic targets.[382] As discussed in Chapter II (Section A), The U.S. EEA prosecutes cases that involve the theft, transfer or misappropriate of U.S. economic data, industry trade secrets, or proprietary information; several Chinese-attributed citizens are listed as violators of this espionage act.[383]

The 124 cases prosecuted under the EEA involved an individual's exploitation of trade secrets that recognized the high value the secrets would have for a foreign entity.[384] As a summary of U.S. EEA cases highlight, of the total 124 cases, approximately 20 percent of them had some form of Chinese involvement—to include government-sanctioned operations.[385] Even though EEA cases frequently reference the theft of

---

[380] Ibid.

[381] Heginbotham et al., *U.S.-China Military Scorecard*, 99.

[382] Alex Newman, "China's Growing Spy Threat," *Diplomat*, September 19, 2011, http://thediplomat.com/2011/09/chinas-growing-spy-threat/.

[383] Federal Bureau of Investigations, "Economic Espionage: Protecting American's Trade Secrets."

[384] Toren, "Look at 16 Years of EEA."

[385] Ibid.

economic and industrial trade secrets, the prosecuted cases also include theft of U.S. private defense industry designs and technology. If the operations were government-sponsored, China's Ministry of State Security (MSS) was likely the primary organizer of or collaborator with the espionage operations, since it specifically handles foreign intelligence operations.[386] Additionally, reports indicate that China employs over two million people under its intelligence and foreign technology information collection missions.[387]

Since the 1970s, there have been numerous examples of traditional Chinese espionage operations that assisted PLA modernization. Following the Soviet Union's collapse in 1991, China engaged in overt military technology purchases with the Soviets; however, as Lindsay and Cheung note, some of China's most advantageous traditional espionage was targeted against the Soviet Union after it imploded.[388] China capitalized on its close proximity to the Soviet Union to infiltrate their critical infrastructure programs and recruit Soviet military scientists and engineers to assist with PLA modernization objectives.[389] As discussed in Chapter I, beginning in the late 1970s, Chinese-native Dongfan Chung physically transferred thousands of documents on U.S. military-contracted rockets, bomber aircraft, fourth generation fighter aircraft, and helicopter technical data over the course of 27 years, back to China.[390] Chung obtained employment with the U.S. Aerospace Boeing Company to obtain the data, and his espionage efforts directly contributed to PLA modernization objectives in the third and fourth waves of PLA modernization.[391] China also leveraged non-Chinese citizens to conduct espionage on its behalf.

Some of the espionage cases that have assisted PLA modernization over the years have also been conducted by third-party, seemingly non-government connected

386 Lindsay, "Introduction," 11; Inkster, "Chinese Intelligence Agencies," 32, 36.

387 Newman, "China's Growing Spy Threat."

388 Lindsay and Cheung, "Exploitation to Innovation," 66–67.

389 Ibid.

390 Ibid., 57.

391 Lindsay and Cheung, "Exploitation to Innovation," 57.

individuals. For example, in 2002, two Russian-descent U.S. citizens sold sensitive Russian satellite technology to a Chinese entity.[392] Additionally, in July 2011, a Taiwanese General sold military secrets to China.[393] In 2011, U.S. military officials also reported suspected cases of Chinese-sponsored espionage against U.S. military forces stationed in Chile.[394] There are many more examples of traditional Chinese espionage operations, but these cases and information about China's intelligence collection highlight the relative success, efficiency, and prominence traditional espionage plays in China's and the PLA's acquisitions processes. Traditional espionage has, in concert with cyber espionage, had a role in PLA modernization and helped the PLA's developmental goals move forward. In addition to espionage, China also has robust R&D methods that also assist PLA modernization.

3. Indigenous Research and Development Initiatives

In addition to the technology exchanges and international procurement agreements the PLA has also progressed its domestic R&D infrastructure. Despite scholarly articles, publications, and master's theses (like U.S. Navy Lieutenant Commander, Gary L. Pembleton's) that list China's indigenous innovative and R&D capacities as underdeveloped and inefficient (as compared to U.S. and developed nations' innovative capacity), China has developed a robust, effectual research and reverse engineering process that transforms developed Western military technologies into PLA military equipment with "Chinese characters."[395] Chinese scientists are able to adapt foreign-acquired technology, reverse engineer them, improve the designs, add "Chinese characteristics" and reproduce them so that they are functional for the PLA military.[396] Director of the Institute on Global Conflict and Cooperation (IGCC), Tai Ming Cheung,

[392] Inkster, "Chinese Intelligence Agencies," 35–36.

[393] Ibid., 36.

[394] Newman, "China's Growing Spy Threat."

[395] Lindsay and Cheung, "Exploitation to Innovation," 67–74; Cheung, "Role of Foreign Technology," 2; Pembleton, "Assessing Technology Innovation in the PLA," v.

[396] Information Office of the State Council, China's National Defense.

describes China's unique, adaptive research process as the "introduce, digest, absorb, and re-innovate (IDAR)" Model.[397]

a. The IDAR Model

According to Cheung, China's equipment development process, under IDAR, involves overt military acquisitions, traditional espionage, and unclassified and classified information exploitation.[398] IDAR's unclassified research involves Chinese researchers scouring open-sources and media for publicly available information; the classified research is conducted by the PLA military as cyber espionage which was previously discussed.[399] The open source research does not include CNE or CNA methods and further reinforces that China's acquisitions system incorporates a multitude of procurement methods. Reverse engineering is also a prominent feature of the IDAR model.[400] Once China obtains the information—whether from espionage, trade, purchase, or unclassified research—the exploited information is then processed by Chinese engineers and reformatted to serve PLA functions.[401] An added advantage of IDAR is it allows China a degree of separation, and it allows China to decipher trends in other countries' military R&D so it can exploit them in future innovation. Indicating IDAR is a continuing trend in China's R&D strategy, over 50,000 personnel at 400 research centers are dedicated to this mission.[402]

b. Research and Development Programs

China's 863 Program, 973 Program, and rural R&D programs are indigenous Chinese government initiatives that supplement China's cyber espionage, military procurement channels, and traditional espionage acquisitions methods. China's 863 Program, also known as the National High Technology Research and Development

[397] Lindsay and Cheung, "Exploitation to Innovation," 70–74; Cheung, "Role of Foreign Technology," 2–4.

[398] Cheung, "Role of Foreign Technology," 2–3.

[399] Ibid., 3–4.

[400] Lindsay and Cheung, "Exploitation to Innovation," 72–74.

[401] Cheung, "Role of Foreign Technology," 3–4.

[402] Lindsay and Cheung, "Exploitation to Innovation," 72–74.

Program, began in 1986. The 863 Program became a way for China to pinpoint specific technologies for scientific research and to jumpstart China's domestic innovation.[403] The 863 Program reinforces the SEIs outlined in China's FYPs and provides guidelines for the development of high-end technologies.[404] The 973 Program is similar to the 863 Program, but it provides funding to civilian institutes and PLA-sponsored militias for basic research purposes.[405] One of the notable successes of the 863 and 973 programs has been the cultivation of robust, indigenous R&D in China's domestic UAV industry.[406]

Apart from major core national science and technology plans—863 and 973 Programs—China relies on small research programs that are geared toward regional and local R&D efforts: the Torch Program, Spark Program, and New Product Program.[407] These three programs were initiated in the late 1980s to aid China's regional and local R&D efforts.[408] The Torch Program focuses on the development of high-end technology to improve China's economic and industrial infrastructures; the Spark Program provides funds for rural technology development; and the New Product Program provides funding to state institutions and research facilities to develop high-end technology and industrial equipment.[409] The Chinese government devotes up to 20 percent of its annual indigenous

---

[403] Consulate General of the People's Republic of China, "Science and Technology Programs in China," Consulate General, Chicago, IL, accessed September 6, 2015, http://www.chinaconsulatechicago.org/eng/kj/t31882.htm; Micah Springut, Stephen Schlaikjer, and David Chen, *China's Program for Science and Technology Modernization: Implications for American Competitiveness* (Virginia: CENTRA Technology, January 2011), 24, 27, http://origin.www.uscc.gov/sites/default/files/Research/USCC_REPORT_China%27s_Program_forScience_and_Technology_Modernization.pdf.

[404] "Science and Technology Programs in China."

[405] Sheldon and McReynolds, "Civil-Military Integration," 202; Springut, Schlaikjer, and Chen, *China's Program for Science and Technology Modernization*, 24.

[406] Kimberly Hsu, Craig Murray, and Jeremy Cook, *China's Military Unmanned Aerial Vehicle Industry* (Washington, DC: U.S.-China Economic and Security Review Commission, June 13, 2013), 6–8, http://origin.www.uscc.gov/sites/default/files/Research/China%27s%20Military%20UAV%20Industry_14%20June%202013.pdf.

[407] There are additional small research funded projects in China, but these programs are listed as key examples; "Science and Technology Programs in China."

[408] Springut, Schlaikjer, and Chen, "China's Program for Science and Technology Modernization," 35.

[409] "Science and Technology Programs in China"; Springut, Schlaikjer, and Chen, "China's Program for Science and Technology Modernization," 24, 33, 35.

R&D budget to these programs.[410] While many of these R&D programs focus on rural development and basic technology research, they still contribute to China's overall development of modernized technology and generates technological breakthroughs that ultimately benefit the PLA's modernization efforts. China's IDAR model and indigenous research programs demonstrate other acquisitions methods the PLA has at its disposal to modernize its military equipment. The next section compares all the previously discussed acquisition methods with the PLA's modernized military equipment to determine if one method (namely cyber espionage) is used more heavily than others.

C. A CASE STUDY OF MODERNIZED PLA MILITARY PLATFORMS

As the previous sections discuss, the PLA developed alternate acquisitions to modernize the military without virtual assistance. This section, and Table 6 specifically, compares modernized PLA systems (across the PLAAF, the PLAN, and PLA Army) with their respective acquisitions methods to decipher trends among frequently used methods. This section shows that, while the PLA employs cyber espionage to modernize the military, cyber espionage complements the PLA's alternate and preexisting procurement methods.

Table 6 has been formulated by integrating a variety of unclassified government, DOD, scholarly articles and books, media reports, and database sources.[411] The U.S. equivalent models are listed to directly address defense reports that make the assumption that Chinese cyber espionage of U.S. military designs is the reason for the progression of their respective Chinese models. The U.S. equivalent models were also generated based on their similarity in design, technical specifications, and modernized status in relation to the Chinese model. Additionally, the developmental times are listed to highlight the difference in production times between exclusively non-cyber influenced systems and CNE-assisted systems: the exclusively non-cyber produced systems often took additional years to develop. For this table, the "approximate development time" began on the

410 "Science and Technology Programs in China"; Springut, Schlaikjer, and Chen, "China's Program for Science and Technology Modernization," 25.

411 The information in Table 6 is a sampling of modernized PLA military equipment and is solely based on the majority judgements from open source information.

earliest reported date (year) researching and theorizing (as IGCC consultant, Maggie Marcum, terms the "pre-program" phase)[412] on the modernized military platform commenced, not on the date physical production began. For example, Marcum's research shows China's "pre-program" phase for the J-11B took approximately 20 years to complete, extended the total development time of the entire aircraft to 35 years.[413] In another example, publications show as early as the 1950s, Chinese naval and administrative officials began the process of attempting to acquire an aircraft carrier, which puts the total development time at 62 years based on its production date in 2012.[414]

Indigenous R&D efforts, when listed under the "Cyber Compromise?" category, include reverse engineering, copycat production, and assimilated technology from traditional espionage operations. The military platforms listed under "critical military technology" are representative examples based on their relatively recent production year (after 2000) to address claims that the PLA has rapidly modernized its military equipment in the 21st century.[415] Additionally, this study attempted to pull modernized military platforms from each PLA branch (PLAAF, PLAN, and the PLA Army) to demonstrate the diverse modernization efforts the PLA has undertaken.

In several of the "critical military technology" cases China outright purchased the military platform, but the platforms are still included in Table 6 to show the range of non-cyber acquisition methods the PLA employs. For example, China's aircraft carrier the *Liaoning* is a product of both indigenous R&D and China's negotiated purchases with several countries.[416] In some examples China may have purchased the military platform,

---

412 Marcum, "Global Fighter Development Timelines," 2–3.

413 Ibid.

414 Erickson, Denmark, and Collins, "Beijing's 'Starter Carrier'" 17–18; Adrew Erickson and Gabe Collins, "Introducing the 'Liaoning': China's New Aircraft Carrier and What it Means," *Wall Street Journal*, September 25, 2012, http://blogs.wsj.com/chinarealtime/2012/09/25/introducing-the-liaoning-chinas-new-aircraft-carrier-and-what-it-means/.

415 U.S.-China Economic and Security Review Commission, "Section 2: China's Cyber Activities," 244–45, 259; *Annual Report to Congress: 2015*, 22, 35; *Annual Report to Congress: 2014*, 35; Heginbotham et al., *U.S.-China Military Scorecard*, xix-xx, 24–25.

416 Erickson, Denmark, and Collins, "Beijing's 'Starter Carrier'" 18–19.

but the technical information or system components were potentially cyber compromised and are therefore listed as "X/+" or both yes and no for "cyber compromise."

In the "cyber compromise" category, an "X" represents no: that the military platform was not cyber compromised. A "X/+" in the "cyber compromise" category represents a yes and no: parts of the military platform were cyber compromised and other components of the system were not. The military platforms that were completely modernized absent of cyber espionage assistance are highlighted in green; the platforms that combined cyber espionage and alternate procurement methods are highlighted in yellow; and the platforms that likely exclusively relied on CNE for modernization assistance are highlighted in red.

Table 6. A Study of Developmental Timelines and Modernized PLA Platforms

Critical Military Technology	Chinese Model	U.S. Equivalent Model	Approximate Development Time	Year of Production	Cyber Compromise?
Fourth Generation Multirole Fighter Aircraft	J-11B	F-15	35 years	2008	X - NO (Produced from an assimilated Russian Su-27 design and indigenous R&D)
Fourth Generation Multirole Fighter Aircraft	J-10 Firebird	F-16	25 years	2010	X/+ - NO on Design; YES on Technical data (Assimilated from Israeli design & Cyber theft of F-16 technical data)
Fifth Generation Multirole Operational Stealth Fighter	J-20	F-22 Raptor	Still under development	N/A: First Flight Tests in 2011	YES (From exploit in 2008 - 2012)
Fifth Generation Multirole Operational Stealth Fighter	J-31	F-35 Joint Strike Fighter	Still under development	N/A: First Flight Tests in 2012	YES (From exploit in 2008 - 2012)
Carrier Landing-Capable Aircraft	J-15 Flying Shark	F/A-18 Hornet	7-11 years	2012	X - NO (Acquired design from Russian SU-33 jet through Ukraine and indigenous R&D)

Critical Military Technology	Chinese Model	U.S. Equivalent Model	Approximate Development Time	Year of Production	Cyber Compromise?
Aircraft Carrier	*Liaoning*	Forrestal Class	62 years	2012	X - NO (Acquired carrier parts from Australia, Ukraine, France, South Korea, and Soviet Union)
Littoral Combat Ship	Type-056	Freedom-Class Independence Class	10-12 years	2012	YES (From exploit in 2008 - 2012)
Missile-Equipped Destroyers	*Sovremenny Class*	Arleigh-Burke Class, Aegis-equipped Destroyers	7 years	2004	X/+- YES on Aegis system used on ship from U.S. in 2000–2013; NO (Purchased ship design from Russia and used indigenous R&D
Nuclear Attack-Capable Submarines	*Shang Class* (Type-093)	Ohio Class	15-16 years	2006	X – NO (Design and technical schematics potentially acquired from Russian designs)
Anti-ship Cruise Missile Launch-Capable Submarines	*Song Class* (Type-039) *Yuan Class*(Type-041)	Seawolf Class Los Angeles Class Virginia Class	14-16 years	1999 and 2006	X - NO (Purchased submarines from Russia, purchased engines from Germany, and indigenous R&D)
Anti-Ship/anti-sub Warfare, Diesel Torpedo Submarine	*Kilo Class*	Gato Class Balao Class	12 years	2006	X - NO (Purchased Kilo Class from Russia and indigenous R&D)
Medium-Altitude/Medium-Endurance Multirole Tactical UAV	ASN-207 or ASN-209 (Silver Eagle)	RQ-1	10 years	Early 2000s and 2011	X – NO (Produced from indigenous R&D based on original ASN-206 model)
Medium-Altitude/Long-Endurance Multirole Tactical UAV	CH-4 *Yilong* or *Wing Loong* (Pterodactyl)	MQ-1 Predator or MQ-9	6 years	2012	X/+ - YES from potential U.S. UAV exploit in 2000–2013; NO (Primarily indigenous R&D)
High-Altitude/Long Endurance ISR	*Xianlong* (Soar Dragon)	RQ-4 Global Hawk	11 years	2009 or 2011	YES – from exploit in 2000–2013

Critical Military Technology	Chinese Model	U.S. Equivalent Model	Approximate Development Time	Year of Production	Cyber Compromise?
UAV					
Early Radar Warning (AEW), Carrier-Capable Helicopter	KA-31	S-70B Seahawk	UNK	2011	X/+ - YES from potential U.S. helicopter exploit in 2000–2013; NO (Acquired and purchased from Russia and indigenous R&D)
Heavy-Lift Aircraft	Y-20	C-130	13-15 years	2013	X - NO (Produced from an assimilated Russian IL-78M tanker design and used indigenous R&D efforts)
Air Defense Systems: Airborne Early Warning System (AEW)	N/A (System used on KJ-2000)	N/A (System used on E-3 AWACS)	10 years	2009	X/+ - YES on updated Air Defense system requirements from U.S. in 2000–2013; NO on design (Produced from an assimilated Israeli Phalcon design, purchased parts from Russia s-400 system, purchased parts from Russian IL-76, and used indigenous R&D efforts)
AEW-Capable Aircraft	KJ-2000 (*Konjing-2000)*	E-3 Sentry (AWACS)	10 years	2003 or 2006	X - NO (Produced from an assimilated Israeli radar design, Russian A-50 airframe, and used indigenous R&D efforts)
Long-Range Surface-to-Air Missiles (SAM)	HQ-9	Patriot Missile	15 years	2005-2006	X/+ - YES on system functionality requirements; NO on initial design (acquired from Russian and used indigenous R&D

Critical Military Technology	Chinese Model	U.S. Equivalent Model	Approximate Development Time	Year of Production	Cyber Compromise?
					to reverse engineer Western/Russian models)
Battle Tank	Type-99	U.S. M1A1	11 years	2001	X/+ - YES on turret design; NO on system requirements and functions (Potentially acquired from Russia T-72 model and indigenous R&D from original Type-90/98 design
Laser Weapons Technology	High-energy laser system	Tactical High Energy Laser (THEL)	55 years	2006	X - NO (Produced from indigenous R&D efforts)

Author's Table Created from the Following Sources: "Airborne Early Warning," GlobalSecurity.org, accessed October 12, 2015, http://www.globalsecurity.org/military/systems/aircraft/aew.htm; "CAC J-10 Meng Long," Jane's All the World's Aircraft, IHS: Aerospace, Defence & Security, last modified July 20, 2015, https://janes.ihs.com.libproxy.nps.edu/CustomPages/JanesDisplayPage.aspx?DocType=Reference&ItemId=+++1342293; "CAC J-20," Jane's All the World's Aircraft, IHS: Aerospace, Defence & Security, last modified July 20, 2015, https://janes.ihs.com.libproxy.nps.edu/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=+++1344019; Chan Kai Yee, "China to Build 15 More Yuan-Class Submarines with German Engines," *China Daily Mail*, April 11, 2013, http://chinadailymail.com/2013/04/11/china-to-build-15-more-yuan-class-submarines-with-german-engines/; Gabe Collins, "China has Become a Top Global Warship Builder," *The Study of Innovation and Technology in China Policy Brief 2014* (University of California Institute on Global Conflict and Cooperation, January 2014), 1–5, https://escholarship.org/uc/item/8635t00n#page-1; Andrew Erickson, Abraham M. Denmark, and Gabriel Collins, "Beijing's 'Starter Carrier' and Future Steps: Alternatives and Implications," *Naval War College Review* 65, no. 1 (Winter 2012): 18–20, 32–34, http://www.andrewerickson.com/wp-content/uploads/2011/12/Erickson-Denmark-Collins_Beijings-Starter-Carrier_NWCR_2012-Winter.pdf; Eric Heginbotham et al., *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power 1996–2017* (Santa Monica, CA: RAND, 2015), 2–4, 6, 24–25, 27–29, 31–34, 98–101, 155, 219–20, 238–40, 242, 245–48, http://www.rand.org/pubs/research_reports/RR392.html; Kimberly Hsu, Craig Murray, and Jeremy Cook, *China's Military Unmanned Aerial Vehicle Industry* (Washington, DC: U.S.-China Economic and Security Review Commission, June 13, 2013), 6–10, http://origin.www.uscc.gov/sites/default/files/Research/China%27s%20Military%20UAV%20Industry_14%20June%202013.pdf; "J-15 Flying Shark (Jianjiji-15 Fighter aircraft 15)/F-15," GlobalSecurity.org, accessed November 2, 2015, http://www.globalsecurity.org/military/world/china/j-15.htm; Meg

Jones, "Navy's Vessel of Versatility," *Journal Sentinel*, November 5, 2008, http://www.jsonline.com/news/milwaukee/33947284.html; Robert Johnson, "This is China's Response to the U.S. Navy's Struggling Coastal Warship Program," *Business Insider*, June 25, 2012, http://www.businessinsider.com/chinas-type-056-corvette-and-the-lcs-2012-6; Joakim Kasper Oestergaard Balle, "MQ-1 Predator/MQ-9 Reaper," Aeroweb, last modified May 28, 2015, http://www.bga-aeroweb.com/Defense/MQ-1-Predator-MQ-9-Reaper.html; "Kilo Class," GlobalSecurity.org, accessed November 2, 2015, http://www.globalsecurity.org/military/world/china/kilo.htm; "Kongjing 2000 (KJ-2000)," GlobalSecurity.org, accessed November 2, 2015, http://www.globalsecurity.org/military/world/china/kj-2000.htm; Jon R. Lindsay and Tai Ming Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), 67–74; Maggie Marcum, "A Comparative Study of Global Fighter Development Timelines," *The Study of Innovation and Technology in China Policy Brief 2014* (University of California Institute on Global Conflict and Cooperation, January 2014), 1–5, http://escholarship.org/uc/item/1wm202sh; Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies," *Washington Post*, May 27, 2013, https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html; Jeremy Page, "China Clones, Sells Russian Fighter Jets," *Wall Street Journal*, December 4, 2010, http://www.wsj.com/articles/SB10001424052748704679204575646472655698844; "Predator RQ-1/MQ-1/MQ-9 Reaper UAV, United States of America," Air Force Technology, accessed September 29, 2015, http://www.airforce-technology.com/projects/predator-uav/; Michael Raska, "Submarine Modernization in East Asia," *Diplomat*, July 14, 2015, http://thediplomat.com/2014/07/submarine-modernization-in-east-asia/; John Reed, "New Images of China's J-15 Carrier-Based Fighter," Defense Tech, last modified September 25, 2011, http://defensetech.org/2011/04/25/new-images-of-chinas-j-15-carrier-based-fighter/; Andrew Scobell, Michael McMahon, and Cortez A. Cooper III, "China's Aircraft Carrier Program: Drivers, Developments, Implications," *Naval War College Review* 68, no. 4 (Autumn 2015): 65–66, 68–71, https://www.usnwc.edu/getattachment/c96be200-d3a9-4b6f-9114-179169fa844e/China-s-Aircraft-Carrier-Program--Drivers,-Develop.aspx; Liam Stoker, "Combat Ships do Battle: LCS versus Type 26," Naval Technology, last modified August 29, 2012, http://www.naval-technology.com/features/featurecombat-ships-battle-lcs-type-26/; "Submarines," Navy Recruiting Command, U.S. Department of Defense, accessed October 12, 2015, http://www.navy.com/about/equipment/vessels/submarines.html; *Annual Report to Congress: 2015*, 9–10; Andrew Tarantola, "China's J-15 Flying Sharks are Actually Russian Knockoffs," Gizmodo, last modified January 6, 2014, http://gizmodo.com/chinas-j-15-flying-sharks-are-actually-russian-knockof-1494117956; "Xi'an ASN-209," Jane's Unmanned Aerial Vehicles and Targets, IHS: Aerospace, Defence & Security, last modified September 24, 2015, https://janes.ihs.com.libproxy.nps.edu/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=+++1318867; "Yuan Type 039A / Type 041," GlobalSecurity.org, accessed October 12, 2015, http://www.globalsecurity.org/military/world/china/yuan.htm; Zhao Yan, "China's 'KJ-2000' AWACS Used the Technology that the U.S. and Russia Have Not Yet Used," China Military Report, accessed October 12, 2015, http://wuxinghongqi.blogspot.com/2009/10/chinas-kj-2000-awacs-used-technology.html.

Table 6 identifies 21 examples of modernized PLA military equipment and compares them with open source information that details their respective acquisition methods. Table 6 provides evidence indicating that the PLA uses cyber espionage as a complementary procurement method—in conjunction with technology purchases, traditional espionage, and indigenous R&D—to modernize the military. This study shows that, out of the PLA's modernized platforms, four out of the 21 entries (approximately 19 percent) were likely exclusive products of cyber espionage; 10 of the 21 entries (approximately 48 percent) were likely derivatives from exclusively non-cyber acquisition methods (whether by reverse engineering, negotiated purchases, or traditional espionage); and seven of the 21 entries (approximately 33 percent) are likely products of both cyber espionage and non-cyber procurement methods.

Upon further examination of Table 6, non-cyber methods are used in 17 of the examples (approximately 81 percent), while cyber espionage is employed in only 11 of the examples (approximately 52 percent). Additionally, some form of Russian involvement is noted in 13 of the 21 total entries (approximately 62 percent). The high degree of Russian involvement also indicates that U.S. military technology is not necessarily the source of the PLA's sophisticated military platforms, as many defense reports suggest. If cyber espionage is the primary driver for PLA modernization—instead of a complementary method—the study would show more exclusive cyber espionage-developed military equipment over non-cyber developed systems; however, in actuality, non-cyber acquisitions methods represent the majority of the sampled cases. This observation supports the potential explanation that, contrary to U.S. defense report assumptions, cyber espionage is not the sole driver behind PLA modernization efforts: it is a complementary method that acts in concert to the PLA's alternate acquisition methods.[417]

[417] Franz-Stefan Gady, "Is China the Biggest Thief in Cyberspace?" *Diplomat*, March 16, 2015, http://thediplomat.com/2015/03/is-china-the-biggest-thief-in-cyberspace/.

D. SUMMARY

Based on the review of Chinese cyber espionage versus modernized PLA military equipment in Tables 3 and 6, there is no question that China—whether government-sponsored or not—uses cyber espionage as a tool to advance PLA modernization initiatives, domestic objectives, and foreign policy goals. Upon examining the sampling of CNE incidents, the evidence suggests there is a relatively equal division of cyber espionage efforts toward all target categories: military targets comprise approximately one-third of the cases, domestic developmental targets make up a little more than approximately one-third of the cases, and diplomatic targets are a little under approximately one-third of the cases. The relatively equal division of cyber targets suggests that cyber espionage missions are equally divided across PLA mission sets and therefore are not solely focused on the narrow goal of exploiting foreign networks, thus assisting PLA modernization.

In addition to the PLA's cyber espionage profile, the military also heavily relies on foreign military technology purchases from Russia and other international partners; traditional espionage operations conducted by Chinese citizens, companies, or co-opted individuals; and indigenous reverse engineering, IDAR, or basic R&D programs to modernize the military. These robust, pre-existing alternate acquisitions methods support the conclusion that cyber espionage is not the sole method driving PLA modernization. The examination of modernized PLA military platforms also solidifies that conclusion. Upon identifying the acquisitions methods for 21 modern PLA military platforms (whether cyber espionage or alternate methods), the majority of modernized equipment was developed from non-cyber means. Consequently, cyber espionage's role in PLA modernization is a supplementary mechanism to alternate factors.

VI. CONCLUSION

Due to the rapidly evolving nature of cyber applications and the virtual domain, this thesis primarily relies on up-to-date, unclassified research material to provide an accurate discussion on how state-sponsored cyber espionage fits into PLA modernization. This thesis provides both a widely accessible, unclassified medium for field reference and also addresses emerging defense reports that make the key assumption that cyber espionage is the sole, primary driver for PLA modernization. This thesis did not argue against conclusions that China's cyber espionage profile is increasing across the virtual domain; in fact, much of the research in this study reinforces that conclusion. This thesis did, however, address the U.S. defense reports that assume cyber espionage is the sole driver behind the PLA's rapid advancement. Ultimately this thesis determines that while cyber espionage and cyber intrusions have and continue to assist PLA modernization, cyber espionage works in concert with other procurement methods (foreign technology acquisitions, traditional espionage, and indigenous R&D) as a supplementary, not primary method. In order to build the evidentiary foundation that state-sponsored cyber espionage is a complementary acquisitions tool in PLA modernization, this thesis examines the progression of PLA modernization, China's cyber strategy, and Chinese CNE operations.

A. IMPLICATIONS AND RECOMMENDATIONS

This study finds that China employs and will continue to employ cyber espionage as a sanctioned and necessary cyber application under China's cyber strategy—regardless of the target type—to achieve its strategic goals. This study has also determined that cyber espionage is just one of the several components driving forward PLA modernization. The question that arises from these conclusions is: How do these forces affect China's international stance on cyber warfare; specifically, will it be feasible for China to adhere to "no cyberattack pacts" and "cyber nonaggression pacts" that it

individually forged with the United States and Russia in 2015?[418] Using this study's previously presented evidence base, this section examines the implications and feasibility of the cyber pacts China signed in May and September 2015, respectively. This section also discusses potential U.S. responses to China's CNO. In order to discuss the implications for China, regarding its U.S. and Russian agreements, this section first distinguishes the differences in the two pacts.

China and Russia solidified their cyber agreement in May 2015, as a symbolic move toward increased cooperation.[419] The cyber nonaggression agreement focuses on bilateral sharing of ideas, technology, information, and technical cyber expertise. The agreement also provides a general outline of cyberspace threats to China and Russia (the Internet and Western countries' cyber operations) that the two countries can jointly defend against.[420]

The high number of Russian military technology transfer cases and negotiated defense sales from Russia to China suggest that this agreement may be upheld by both parties. China is induced to uphold the pact because Russia is China's largest foreign technology provider, and Russia assistance will help the PLA modernize more rapidly. Russia is induced to uphold the pact because Russia's modernized military is one of the few most developed forces that can combat the U.S. military. Once the PLA reaches a complete, developed level of modernization, both Russia and China would be able to combat U.S. military capabilities in cases of future conflict, such as Syria or Taiwan. While this pact may not decrease the number of cyber espionage operations each country conducts against foreign entities (or each other), it does symbolize a working partnership on modern issues between Russia and China. This pact is also a crucial factor to study when determining, in IR terms, how China or Russia will rise in power in the

[418] Patrick Tucker, "White House: No Cyber Attack Pact with China, For Now," Defense One, last modified September 22, 2015, http://www.defenseone.com/technology/2015/09/white-house-no-cyber-attack-pact-china-now/121763/; Elaine Korzak, "Russia and China have a Cyber Nonaggression Pact," Defense One, last modified August 20, 2015, http://www.defenseone.com/ideas/2015/08/russia-china-cyber-nonaggression-pact/119302/.; Korzak, "Russia and China have Cyber Nonaggression"; Obama, "Remarks by Obama and Xi."

[419] Korzak, "Russia and China have Cyber Nonaggression"; Obama, "Remarks by Obama and Xi."

[420] Ibid.

international system. Based on China's and Russia's strong history of cooperation and technology sharing, China will likely be able to uphold its agreement with Russia.

In contrast to the Sino-Russian cyber agreement, the U.S.-China cyber agreement contained more direct language. The U.S.-China non-cyberattack agreement addresses the U.S.'s primary concern of limiting China's high-volume, economic-targeted cyber espionage operations.[421] The agreement came after the United States pressured China with economic sanctions if the CCP did not control its domestic Chinese CNE operations.[422] The agreement states that neither country will pursue state-sponsored cyber espionage against economic, industrial, or intellectual property targets.[423] The pact does not, however, put restrictions on state-sponsored cyber espionage against government or military targets, parallel to what is typically accepted with traditional espionage in conventional warfare.[424] Both countries signed the pact on September 25, 2015; however, one day later (September 26, 2015), a U.S. Cyber Monitoring Firm, CrowdStrike, announced that Chinese APTs attempted CNE on U.S. industrial and economic targets. Based on this thesis' study of China's cyber strategy, was China's agreement to the cyber non-attack pact really feasible? The answer to the question is both yes and no.

Media reports frequently cite China's arrest of several hackers in early September 2015 as evidence that China will uphold the pact, in accordance with U.S. wishes.[425] U.S. media uses these arrests as examples that China is serious about remaining true to the pact's non-economic target parameters. These arrests, however, could have also been a part of China's "Operation Clean Internet" that identifies and tracks cyber criminals who

---

421 Obama, "Remarks by Obama and Xi."

422 Ellen Nakashima and Adam Goldman, "In a First, Chinese Hackers are Arrested at the Behest of the U.S. Government," *Washington Post,* October 9, 2015, https://www.washingtonpost.com/world/national-security/in-a-first-chinese-hackers-are-arrested-at-the-behest-of-the-us-government/2015/10/09/0a7b0e46-6778-11e5-8325-a42b5a459b1e_story.html.

423 Ibid.; Kelly Jackson Higgins, "CrowdStrike Spots Chinese APTs Targeting U.S. Firms Post-Pact," Information Tech, last modified October 19, 2015, http://www.darkreading.com/attacks-breaches/crowdstrike-spots-chinese-apts-targeting-us-firms-post-pact/d/d-id/1322712.

424 Ibid.; Tucker, "White House: No Cyber Attack."

425 Nakashima and Goldman, "Chinese Hackers Arrested at Behest of U.S."

have conducted attacks on domestic Chinese targets.[426] This domestic campaign is an effort to improve China's domestic cybersecurity and arrest individuals who commit acts of identity theft and financial data theft.

Also arguing that the cyber pact is unfeasible for China to uphold, many China scholars classify the agreement as purely "symbolic."[427] The cyber agreement is partially unfeasible because China's cyber strategy is oriented around strategic principles that do not distinguish between military and economic targets. Cyber espionage of U.S. economic (and any type of) technology allows China to both supplement its weak R&D infrastructure and maintain an advantage over the United States. Additionally, due to the ambiguous, non-attributable nature of cyberspace, it is relatively easy for China to deny that any CNE on U.S. economic targets came directly from sanctioned Chinese government entities. The non-cyberattack pact is unfeasible because Chinese perspectives on cyberspace and cyber strategy are neither compatible with the agreement nor U.S. views on sanctioned cyber targets. Consequently, the cyber intrusions are not likely to stop.

Additionally, the pact did not provide exact parameters for what the United States and China would constitute as an economic target. For example, critical infrastructure, which includes water or communications companies, was not specifically defined under the pact.[428] Therefore, China, who does not recognize different categorical types of CNE targets, can claim ignorance for any cyber espionage that does occur.[429] If Chinese entities conducted cyber espionage on U.S. companies that supported these functions, China could potentially claim they were not economic targets, while the U.S. would disagree. Ultimately, even though President Xi will be able to uphold the language of the agreement by not pursing government-sanctioned CNE on U.S. economic targets, the pact was unfeasible for China to agree to because its strategic views do not correspond to

---

[426] "China Arrests 15,000 Suspects for Alleged Cybercrimes," *CNN Money*, August 19, 2015, http://money.cnn.com/2015/08/19/news/china-cybercrime-arrests/index.html.

[427] Tucker, "White House: No Cyber Attack."

[428] Ibid.

[429] Shannon Tiezzi, "The Limits of a U.S.-China Cyber Deal," *Diplomat,* September 22, 2015, http://thediplomat.com/2015/09/the-limits-of-a-us-china-cyber-deal/.

the U.S.'s strategic outlook on cyber espionage. As long as China has developmental goals and strong commitment to achieving them by any means, China will continue to pursue cyber espionage on economic targets.

There is other evidence that suggests that the pact is relatively feasible, and China will be able to uphold the agreement. The wide variance in Chinese cyber actors (government, military, militia, university, private groups, and individuals), demonstrated by Table 3 in Chapter V, and the overlapping manner in which they conduct CNE operations, should allow China to adhere to the language of the non-cyberattack agreement. President Xi could adjust China's cyber strategy to allow for military and government entities to focus on exploiting foreign military and government defense technology—since those targets are not prohibited under the agreement. Xi could then leave the economic cyber-targeting to other domestic Chinese entities without being involved, thus upholding the agreement by not pursuing government-sanctioned CNE on U.S. economic targets.

Non-government actors are still incentivized to conduct cyber espionage operations—but specifically on economic targets—for the high value those targets hold for many domestic Chinese and foreign firms. Their exploitation of economic targets progresses China's developmental industries listed in the FYPs and MLP and thus benefits Chinese society as a whole. Non-government hackers do not (and would not) need to be sanctioned by the Chinese government because, as long as they exploited U.S. economic targets, their actions would likely not be condemned: the hackers' actions would be recognized as operations that benefit domestic China. Additionally, Table 3's information further upholds this conclusion, because it shows that China relies on cyber espionage of U.S. economic targets to achieve several of its FYP developmental goals. While Xi may be able to uphold the spirit of the cyber non-attack agreement by not directly sanctioning economic cyber intrusions, he will not be able to stop cyberattacks. If this is the case, then how does the United States respond?

The United States could use several methods of cyber, non-cyber, economic, and diplomatic means to respond to China's cyber espionage actions, related or not related to the non-attack cyber agreement. Since intellectual property and private industry

innovation are of the utmost importance to the United States, the U.S. government could institute a higher level of protection among private industries. The U.S. government already partners with U.S. defense and government-cleared contract companies for basic cybersecurity awareness, but these programs do not provide the level of protection needed to safeguard against high-volume Chinese CNE. The U.S. government could partner with private industries to provide contracted government-level security that protects private corporations from cyber intrusions; specifically hire and contract out security firms (like Mandiant, McAfee, DGI, ThreatConnect, and CrowdStrike) to provide cyber security solutions to private companies, if they do not already. If the private corporations opted out of the government-provided cybersecurity, the United States government could encourage U.S. cybersecurity firms, like Mandiant, to produce more unclassified reports. These unclassified reports would be a free, unclassified tool for U.S. industrial partners to reference. This would allow them to increase awareness on Chinese cyber entities' TTPs and frequent targets. These reports would also allow the U.S. government to build more evidence against Chinese hacker groups to support the government's claims against China.

Additionally, the United States could use the cyber pacts between itself, China, and Russia to pursue international agreements on cyber operations. While it is unlikely that any country will agree to international sanctions on specific cyber actions (because many countries rely on cyber means to monitor adversarial nations), the United States could pursue the establishment of a consensus on cyber terms and the severity level of cyber operations. For example, would "cyberattack" include cyber operations like cyber intrusions, CNE, CNA? If the United States pursued a common definitional understanding across the international community, this could alleviate confusion between itself and China in future cyber agreements; it could also preemptively prevent tensions between newly developed countries that begin to test their cyber espionage skills on a wide scale. Since it is difficult to reach international consensus on a domain (cyber) that is in constant evolution, the United States could bolster its domestic capabilities to match China's CNO. Future research in alternate areas of study that this thesis did not address,

however, could also provide more insight into how the United States could bolster its domestic cybersecurity to protect against Chinese cyber espionage.

B. AVENUES FOR FUTURE RESEARCH

As mentioned in the literature review, the intricate debates over topics of PLA modernization, China's cyber strategy, and Chinese cyber espionage can be studied in further depth. Apart from addressing key discussions in the literature, this thesis also identifies additional areas for future research in China's cyber strategy. This thesis concentrates on exclusively unclassified, open-source information, so a beneficial avenue for future research that would directly respond to this study's research findings would be classified research and data. Due to the secretive, largely unsanctioned nature of cyber espionage, it is likely that more information regarding Chinese cyber espionage is contained in classified reports. Consequently, a research question that could be pursued, using both classified and unclassified information, is: Would classified information change previous conclusions about China's cyber strategy and cyber espionage operations? The inclusion of classified information regarding Chinese cyber espionage and PLA modernization could significantly bolster or revise many unclassified reports that did not address classified data.[430]

Another area of future research would involve more technical cyber skills and computer science knowledge. This thesis concentrates on identifying the conceptual tenets of China's cyber strategy and does not go into detail on the technical aspects of China's employment of specific malware types. An in-depth examination of Chinese CNE operations, compared to the malware programs used, could provide insight into how China's CNO strategy is oriented. This examination would also address the primary debate in the literature regarding whether China's cyber strategy is more offensive or defensive in nature. A potential research question for this area of study is: What does China's use of certain cyber applications or malware programs in state-sponsored cyber

[430] Of course, classified information may also be incomplete. A key feature of the cyber domain is the difficulty of knowing how much is not known, at classified as well as unclassified levels. Examining the conclusions of this thesis in light of classified information would certainly advance knowledge, but possibly only by underscoring the limitations of that knowledge.

warfare suggest about the orientation of its cyber strategy? Within that research question, it would also be beneficial to investigate why China's employs certain malware programs. This area of future research contributes to a large debate in Chinese cyber literature and also provides additional potential explanations for why China's cyber strategy operates the way it does.

This thesis also focuses on explaining current Chinese cyber operations and strategies and does not detail how that information could be tapped by the United States' or other Chinese-targeted countries' to bolster their CND against Chinese cyber espionage. Specifically, how could the United States leverage what it knows about how China's cyber strategy is implemented to appropriately respond or create a legal framework that allows China to uphold these principles and also allows the United States to protect its intellectual property? In reference to China's CNO strategy, a future research question to explore is: How could the United States use what it knows about China's strategic cyber principles to create a comprehensive defense against it?

The last areas for future research correspond to specific countries and regional focuses: the South China Sea and North Korea. One research avenue would involve the examination of Chinese cyber espionage or cyber intrusions employed against countries operating in the South China Sea oceanic territory China claims. A possible research question is: How does China's use of certain cyber applications, like state-sponsored cyber warfare, fit into its actions in the South China Sea?

Another topic of research could involve China's cyber assistance to North Korea. A question that arises from this topic is: How does China's technical and cyber assistance affect North Korea's regime; specifically, does it help the North Korean regime maintain its unstable rule? This avenue of research provides insight into several areas: the nature of China's and North Korea's relationship; the nature of North Korea's cyber capabilities and cyber strategy; and a potential explanation for how the belligerent, underdeveloped North Korean regime remains in power.

There are several future areas for research due to the rapid evolution of virtual applications and the increase of nations' use of cyber warfare. Due to this rapidly

changing virtual environment, basic cyber definitions are contested and dynamic. This thesis provides insight into one facet of cyber warfare: cyber espionage. Future studies, reflecting on newer developments and perhaps using evolved conceptual definitions, could potentially reach alternate conclusions. Nevertheless, this thesis' study of the important role that cyber espionage plays in China's military modernization indicates that the virtual realm and cyber warfare are growing key areas for research, as national networks become more interconnected, nations conduct more of their operations online, and hackers continue to exploit these areas through cyber applications.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Air Force Technology. "Predator RQ-1/MQ-1/MQ-9 Reaper UAV, United States of America." Accessed September 29, 2015. http://www.airforce-technology.com/projects/predator-uav/.

Allen, Kenneth. "Introduction to the PLA's Administrative and Operational Structure." In *The People's Liberation Army as Organization: Reference Volume v1.0,* edited by James C. Mulvenon and Andrew N. D. Yang, 1–44. Santa Monica, CA: RAND, 2002. http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2008/CF182part1.pdf.

Allen, Kenneth W., Glenn Krumel, and Jonathan D. Pollack. *China's Air Force Enters the 2st[t] Century.* Santa Monica, CA: RAND, 1995. http://www.rand.org/pubs/monograph_reports/MR580.html.

Alperovitch, Dmitri. "Revealed: Operation Shady RAT." McAfee. Accessed June 3, 2015. http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

Andres, Richard B. "The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 89–104. Washington, DC: Georgetown University Press, 2012. https://muse.jhu.edu.libproxy.nps.edu/books/9781589019195/9781589019195-12.pdf.

APCO China. "China: Summary of the Tenth Five-Year Plan (2001-2005) – Information Industry." Translated by Ministry of Industry and Information Technology (China). Accessed August 21, 2015. http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan022769.pdf.

Ball, Desmond. "China's Cyber Warfare Capabilities," *Australia's Leading Journal for Future Security Issues* 7, no. 2 (Winter 2011): 81–103. http://www.securitychallenges.org.au/ArticlePDFs/vol7no2Ball.pdf.

Beauchamp-Mustafaga, Nathan and Peter Wood. "In a Fortnight." *China Brief* 15, no. 12 (June 2015): 1–2. http://www.jamestown.org/uploads/media/China_Brief_Vol_15_Issue_12_1.pdf.

Blasko, Dennis J. "The 2015 Chinese Defense White Paper on Strategy in Perspective: Maritime Missions Require a Change in the PLA Mindset." *China Brief* 15, no 12 (June 2015): 3–6. http://www.jamestown.org/uploads/media/China_Brief_Vol_15_Issue_12_1.pdf.

———. *The Chinese Army Today: Tradition and Transformation for the 21st Century.* New York: Routledge, 2006.

———. *The Chinese Army Today: Tradition and Transformation in the 21st Century.* 2nd ed. New York: Routledge, 2012.

Cartwright, James E. *Attachment 1: Cyberspace Operations Lexicon*. DOD Memorandum on Joint Terminology for Cyberspace Operations. Washington, DC: Vice Chairman of the Joint Chiefs of Staff, 2010. http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

Casey, Joseph and Katherine Koleski. *Backgrounder: China's 12th Five-Year Plan.* U.S.-China Economic & Security Review Commission. Last modified June 24, 2011. http://www.uscc.gov/researchpapers/2011/12th-FiveYearPlan_062811.pdf.

Cavaiola, Lawrence J., David D. Gompert, and Martin Libicki. "Cyber House Rules: On War, Retaliation and Escalation." *Survival: Global Politics and Strategy* 57, no. 1 (February-March 2015): 81–104. http://www.iiss.org/en/Topics/chinas-cyber-policy/57-1-07-cavaiola-gompert-and-libicki-3ab8.

Center for Strategic International Studies. "Significant Cyber Incidents Since 2006." Last modified July 13, 2015. http://csis.org/files/publication/150714_Significant_Cyber_Events_List.pdf.

Cha, Victor. "North Korea: What Not to Do." *PacNet*, no. 1 (January 2012): 1–2. http://csis.org/files/publication/Pac1.pdf.

Chang, Maria Hsia. *Return of the Dragon: China's Wounded Nationalism*. Boulder, CO: Westview Press, 2001.

Chen, Jian. *Mao's China and the Cold War: The New Cold War History.* Edited by John Lewis Gaddis. Chapel Hill: South Carolina University Press, 2001.

Cheng, Joey and Kevin McCaney. "Cyber Charges against China Could Raise the Stakes for U.S. Command." Defense Systems. Last modified May 19, 2014, https://defensesystems.com/articles/2014/05/19/us-china-cyber-charges.aspx.

Cheung, Tai Ming. "China's Emergence as a Defense Technological Power: Introduction." *Journal of Strategic Studies* 34, no. 3 (June 2011): 295-97. doi: 10.1080/01402390.2011.583155

———. "Rejuvenating the Chinese Defense Economy: Present Developments and Future Trends," *The Study of Innovation and Technology in China Policy Brief* . No. 19. University of California Institute on Global Conflict and Cooperation, September 2011. https://escholarship.org/uc/item/60z7p0kp.

———. “The Role of Foreign Technology Transfers in China’s Defense Research, Development, and Acquisition Process.” *The Study of Innovation and Technology in China Policy 2014*. University of California Institute on Global Conflict and Cooperation (2014). http://escholarship.org/uc/item/4dp213kd.

China Direct. “China’s Twelfth Five Year Plan (2011-2015) – the Full English Version.” Last modified September 11, 2011. http://cbi.typepad.com/china_direct/2011/05/chinas-twelfth-five-new-plan-the-full-english-version.html.

China Information Center. “The Tenth Five-Year Plan.” Accessed August 22, 2015. http://www.china.org.cn/english/features/38198.htm.

Christensen, Thomas J. “Windows and War: Trend Analysis and Beijing’s Use of Force.” In *New Directions in the Study of China’s Foreign Policy*, edited by Alastair Iain Johnston and Robert S. Ross, 5085. Stanford, CA: Stanford University Press, 2006.

Collins, Gabe. “China has Become a Top Global Warship Builder.” *The Study of Innovation and Technology in China Policy Brief 2014*. University of California Institute on Global Conflict and Cooperation, January 2014. https://escholarship.org/uc/item/8635t00n#page-1.

Consulate General of the People’s Republic of China, “Science and Technology Programs in China.” Consulate General, Chicago, IL. Accessed September 6, 2015. http://www.chinaconsulatechicago.org/eng/kj/t31882.htm.

Cooper, Jeffrey R. “A New Framework for Cyber Deterrence.” In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 105–20. Washington, DC: Georgetown University Press, 2012. https://muse.jhu.edu.libproxy.nps.edu/books/9781589019195/9781589019195-13.pdf.

Cordesman, Anthony H., Ashley Hess, and Nicholas S. Yarosh. *Chinese Military Modernization and Force Development: A Western Perspective*. Washington, DC: Center for Strategic & International Studies, August 2013. http://csis.org/files/publication/130725_chinesemilmodern.pdf.

Cornish, Paul. “Governing Cyberspace through Constructive Ambiguity.” *Survival: Global Politics and Strategy* 57, no. 3 (June-July 2015): 153–76. http://www.iiss.org/en/Topics/chinas-cyber-policy/57-3-09-cornish-a772.

Denning, Dorothy E. *Information Warfare and Security.* New York: ACM Press Books, 1999.

Dreyer, June Teufel. “Washington Contemplates the Chinese Military.” *Foreign Policy Research Institute*. Last modified September 2015. http://www.fpri.org/docs/dreyer_-_chinas_military.pdf.

Dunn, John E. “Chinese ‘Hidden Lynx’ Hackers behind Major Cyberattacks on U.S., Claims Symantic.” Tech World. Last modified September 17, 2013, http://www.techworld.com/news/security/chinese-hidden-lynx-hackers-behind-major-cyberattacks-on-us-claims-symantec-3469248/.

Engstrom, Jeffrey G., Michael S. Chase, Tai Ming Cheung, Kristen A. Guinness, Scott Warren Harold, Susan Puska, and Samuel Berkowitz. *China’s Incomplete Military Transformation: Assessing the Weaknesses of the People’s Liberation Army (PLA).* Santa Monica, CA: RAND, 2015. http://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR893/RAND_RR893.pdf.

Erickson, Andrew, Abraham M. Denmark, and Gabriel Collins. “Beijing’s ‘Starter Carrier’ and Future Steps: Alternatives and Implications.” *Naval War College Review* 65, no. 1 (Winter 2012): 15–54. http://www.andrewerickson.com/wp-content/uploads/2011/12/Erickson-Denmark-Collins_Beijings-Starter-Carrier_NWCR_2012-Winter.pdf.

Fan, C. Cindy. “China’s Eleventh Five-Year Plan (2006-2010): From ‘Getting Rich First’ to ‘Common Prosperity.” *Eurasian Geography and Economics* 47, no. 6 (2006): 708–23. http://www.sscnet.ucla.edu/geog/downloads/597/300.pdf.

Federal Bureau of Investigations. “Economic Espionage: Protecting American’s Trade Secrets.” Accessed October 7, 2015. https://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage.

Finklestein, David M. “China’s National Military Strategy: An Overview of the ‘Military Strategic Guidelines.’” *Asia Policy*, no. 4 (July 2007): 67–72. http://muse.jhu.edu/journals/asia_policy/v004/4.finkelstein.pdf.

———. “The General Staff Department of the Chinese People’s Liberation Army: Organization, Roles, & Missions.” In *The People’s Liberation Army as Organization: Reference Volume v1.0*, edited by James C. Mulvenon and Andrew N. D. Yang, 122–224. Santa Monica, CA: RAND, 2002. http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2008/CF182part1.pdf.

Fleming, Daniel C. “Intellectual Property Rights in China.” Wong-Fleming Attorneys at Law. Accessed December 13, 2015. http://wongfleming.com/intellectual-property-rights-in-china/.

Fravel, M. Taylor. *Strong Borders, Secure Nation: Cooperation and Conflict in China’s Territorial Disputes*. Princeton, NJ: Princeton University Press, 2008.

Friedman, Allen A. “Cyber Theft of Competitive Data: Asking the Right Questions.” Center for Technology Innovation. Brookings Institute, September 2013.

http://www.brookings.edu/~/media/research/files/papers/2013/09/25-cyber-theft-competitive-data-friedman/brookingscybertech_revised.pdf.

Gilboy, George J. “The Myth behind China’s Miracle.” *Foreign Affairs* 83, no. 4 (2004): 33–48. http://www.jstor.org/stable/2003404534-35.

Global Fire Power. “Countries Ranked by Military Strength (2015).” Last modified April 1, 2015. http://www.globalfirepower.com/countries-listing.asp.

GlobalSecurity.org. “Airborne Early Warning.” Accessed October 12, 2015. http://www.globalsecurity.org/military/systems/aircraft/aew.htm.

------. “J-15 Flying Shark (Jianjiji-15 Fighter aircraft 15)/F-15.” Accessed November 2, 2015. http://www.globalsecurity.org/military/world/china/j-15.htm.

------. “Kilo Class,” Accessed November 2, 2015. http://www.globalsecurity.org/military/world/china/kilo.htm.

------. “Kongjing 2000 (KJ-2000).” Accessed November 2, 2015. http://www.globalsecurity.org/military/world/china/kj-2000.htm.

------. “Yuan Type 039A / Type 041.” Accessed October 12, 2015. http://www.globalsecurity.org/military/world/china/yuan.htm.

Hachigian, Nina. “China’s Cyber-Strategy.” *Foreign Affairs* 80, no. 2 (March–April 2001): 118–33. http://www.jstor.org/stable/20050069.

Harmala, Jason. “Cyber Experts Weigh in on Threat of Chinese Cyber Espionage.” Discussion with Franklin D. Kramer, Dmitri Alperovitch, James C. Mulvenon, and Gregory J. Rattray. Washington, DC: Brent Scowcroft Center on International Security, Atlantic Council. http://www.atlanticcouncil.org/events/past-events/cyber-experts-weigh-in-on-threat-of-chinese-cyber-espionage.

Heginbotham, Eric, Michael Nixon, Forrest E. Morgan, Jacob L. Heim, Jeff Hagen, Sheng Li, Jeffrey Engstrom, Martin C. Libicki, Paul DeLuca, David A. Shlapak, David R. Frelinger, Burgess Laird, Kyle Brady, and Lyle J. Morris. *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power 1996–2017.* Santa Monica, CA: RAND, 2015. http://www.rand.org/pubs/research_reports/RR392.html.

Higgins, Kelly Jackson. “CrowdStrike Spots Chinese APTs Targeting U.S. Firms Post-Pact.” Information Tech. Last modified October 19, 2015. http://www.darkreading.com/attacks-breaches/crowdstrike-spots-chinese-apts-targeting-us-firms-post-pact/d/d-id/1322712.

Hjortdal, Magnus. “China’s Use of Cyber Warfare: Espionage Meets Strategic Deterrence.” *Journal of Strategic Security* 4, no. 2 (2011): 1–24. doi: 10.5038/1944-0472.4.2.1.

Hsu, Kimberly, Craig Murray, and Jeremy Cook. *China’s Military Unmanned Aerial Vehicle Industry*. Washington, DC: U.S.-China Economic and Security Review Commission Staff, June 13, 2013. http://origin.www.uscc.gov/sites/default/files/Research/China%27s%20Military%20UAV%20Industry_14%20June%202013.pdf.

Hu, Guangzheng et al. *Yingxiangdao ershiyi shiji de zhengming (Contention Affecting the 21st Century)*, (Beijing: Liberation Army Press, 1989), 113. Quoted in Nan Li, “The PLA’s Evolving Campaign Doctrine and Strategies,” in *The People’s Liberation Army in the Information Age* (Santa Monica, CA: RAND, 1999), 146, http://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF145/CF145.chap8.pdf.

Hurst, Cindy. “China’s Digital Destroyers: Striving for Information Dominance,” Foreign Military Studies Office, Ft. Leavenworth. U.S. Army. Accessed May 28, 2015. http://fmso.leavenworth.army.mil/documents/China’s-digital-destroyers.pdf.

Information Office of the State Council of the People’s Republic of China. *China’s National Defense*. Beijing: State Council, December 2004. http://en.people.cn/whitepaper/defense2004/defense2004.html.

Inkster, Nigel. “China in Cyberspace.” in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 191–205. Washington, DC: Georgetown University Press, 2012. http://muse.jhu.edu/books/9781589019195/9781589019195-19.pdf.

———. “The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace.” In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 29–50. New York: Oxford University Press, 2015.

International Crisis Group. “China and Taiwan: Uneasy Détente.” *Asia Briefing*, no. 42 (September 2005). http://www.crisisgroup.org/~/media/Files/asia/north-east-asia/taiwan-strait/b042_china_and_taiwan_uneasy_detente.pdf.

Jane’s. “CAC J-20.” All the World’s Aircraft. IHS: Aerospace, Defence & Security. Last modified July 20, 2015. https://janes.ihs.com.libproxy.nps.edu/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=+++1344019.

———. “CAC J-10 Meng Long.” All the World’s Aircraft. IHS: Aerospace, Defence & Security. Last modified July 20, 2015. https://janes.ihs.com.libproxy.nps.edu/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=+++1342293.

———. “Xi’an ASN-209.” Unmanned Aerial Vehicles and Targets. IHS: Aerospace, Defence & Security. Last modified September 24, 2015. https://janes.ihs.com.libproxy.nps.edu/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=+++1318867.

Jian, Zhang. “China’s Defense White Papers: A Critical Appraisal.” *Journal of Contemporary China* 21, no. 77 (May 2012): 881–98. doi: 10.1080/10670564.2012.684969.

Jin, Jianbin and Chengyu Xiong. “Digital Divide in National Informationization Quotient: The Perspective of Mainland China.” Paper presented at the International Conference on the Digital Divide: Technology & Politics in the Information Age, Beijing, PRC, 2002. http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan046441.pdf.

Jong-Chen, Jing De. “U.S.-China Cybersecurity Relations: Understanding China’s Current Environment.” *Georgetown Journal of International Affairs*, September 15, 2014. http://journal.georgetown.edu/u-s-china-cybersecurity-relations-understanding-chinas-current-environment/.

Kaplan, Robert D. “The Geography of Chinese Power: How Far Can Beijing Reach on Land and at Sea?” *Foreign Affairs* 89, no. 3 (2010): 22–41. http://www.jstor.org/stable/25680913.

Kasper Oestergaard Balle, Joakim, III. “MQ-1 Predator/MQ-9 Reaper.” Aeroweb. Last modified May 28, 2015. http://www.bga-aeroweb.com/Defense/MQ-1-Predator-MQ-9-Reaper.html.

Kelly, Jason. “A Chinese Revolution in Military Affairs?” *Yale Journal of International Affairs* 1, no. 2 (Winter-Spring 2006): 58–71. http://www.yale.edu/yjia/articles/Vol_1_Iss_2_Spring2006/kelly217.pdf.

Korzak, Elaine. “Russia and China have a Cyber Nonaggression Pact.” Defense One. Last modified August 20, 2015. http://www.defenseone.com/ideas/2015/08/russia-china-cyber-nonaggression-pact/119302/.

Krekel, Bryan. *Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation for the U.S.-China Economic and Security Review Commission.* McLean, VA: Northrup Grumman, 2009. http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf.

Krekel, Patton Adams, and George Bakos. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage.* Virginia: Northrup Grumman, March 2012. http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-066.pdf.

Leopold, George. “China’s Military Calls for ‘Online Great Wall.’” Defense Systems. Public Sector Media Group. Last modified May 21, 2015. http://defensesystems.com/articles/2015/05/21/china-pla-online-great-wall.aspx.

Lewis, James A. *Assessing the Risks of Cyber Terrorism, Cyber War, and Other Cyber Threats.* Washington, DC: Center for Strategic and International Studies, December 2002. http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

Li, Nan. “The Central Military Commission and Military Policy in China.” in *The People’s Liberation Army as Organization: Reference Volume v1.0,* edited by James C. Mulvenon and Andrew N. D. Yang, 45–94. Santa Monica, CA: RAND, 2002. http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2008/CF182part1.pdf.

———. “The PLA’s Evolving Campaign Doctrine and Strategies.” In *The People’s Liberation Army in the Information Age*. Santa Monica, CA: RAND, 1999: 146–74. http://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF145/CF145.chap8.pdf.

Libicki, Martin C. “Cyberspace is not a Warfighting Domain.” *Journal of Law and Policy for the Information* Society 8, no. 2 (2012): 321–36. http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Libicki.pdf.

Libicki, Martin C., Lillian Ablon, and Andrea A. Golay. *Markets for Cybercrime Tools and Stolen Data: Hacker’s Bazaar.* Santa Monica, CA: RAND, 2014. http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

Lindsay, Jon R. “The Impact of China on Cybersecurity: Fiction and Friction.” *International Security* 39, no. 3 (February 2015): 7–47. doi:10.1162/ISEC_a_00189.

———. “Introduction: China and Cybersecurity Controversy and Context.” In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain,* edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 1–28. New York: Oxford University Press, 2015.

———. “Stuxnet and the Limits of Cyberwarfare,” *Security Studies* 22, no. 3 (2013): 365–404. doi: 10.1080/09636412.2013.816122.

Lindsay, Jon R. and Derek S. Reveron. “Conclusion: The Rise of China and the Future of Cybersecurity.” In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 333–54. New York: Oxford University Press, 2015.

Lindsay, Jon R. and Tai Ming Cheung. “From Exploitation to Innovation: Acquisition, Absorption, and Application.” In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 51–86. New York: Oxford University Press, 2015.

Mandiant. “APT 1: Exposing One of China’s Cyber Espionage Units.” February 2013. http://intelreport.mandiant.com/.

———. “Beyond the Breach: 2014 Threat Report.” M-Trends. 2014. https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf.

Mao, Zhongying, ed. “China’s New S&T Development Plan.” *China Science and Technology Newsletter*, no. 456. Beijing, China: Ministry of Science and Technology, November 10, 2006. http://www.most.gov.cn/eng/newsletters/2006/200611/t20061110_37960.htm.

Marcum, Maggie. “A Comparative Study of Global Fighter Development Timelines.” *The Study of Innovation and Technology in China Policy Brief 2014*. University of California Institute on Global Conflict and Cooperation, January 2014, http://escholarship.org/uc/item/1wm202sh.

———. “Assessing High-Risk, High-Benefit Research Organizations: The ‘DARPA Effect.’” *The Study of Innovation and Technology in China Policy Brief 2014*. University of California Institute on Global Conflict and Cooperation, January 2014. http://escholarship.org/uc/item/7n49c638.

Marcum, Maggie and Aliaksandr Milshyn. “Changing Trends in Global Research, Development, and Acquisition Process.” *The Study of Innovation and Technology in China Policy Brief 2014.* University of California Institute on Global Conflict and Cooperation, January 2014. http://escholarship.org/uc/item/7s48w1ck.

McDade, Wylie. “Attribution, Delayed Attribution and Covert Cyber-attack. Under What Conditions Should the United States Publicly Acknowledge Responsibility for Cyber Operations.” Master’s thesis, Naval Postgraduate School, Monterey, CA, March 2014. http://hdl.handle.net/10945/41417.

McGregor, James. *China’s Drive for ‘Indigenous Innovation’: A Web of Industrial Policies*. Washington, DC: U.S. Chamber of Commerce, 2010. https://www.uschamber.com/report/china%E2%80%99s-drive-indigenous-innovation-web-industrial-policies.

McKune, Sarah. “‘Foreign Hostile Forces’: The Human Rights Dimension of China’s Cyber Campaigns.” In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 260–96. New York: Oxford University Press, 2015.

McReynolds, Joe. “Network Warfare in China’s 2015 Defense White Paper.” *China Brief* 15, no. 12 (June 2015): 10–13. http://www.jamestown.org/uploads/media/China_Brief_Vol_15_Issue_12_1.pdf.

Mearsheimer, John J. “China’s Unpeaceful Rise.” *Current History* 105, no. 690 (April 2006): 160–62. http://archives.cerium.ca/IMG/pdf/Chinas_Unpeaceful_Rise.pdf.

Mulvenon, James C. “PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability.” In *Beyond the Strait: PLA Missions Other Than Taiwan*, edited by Roy Kamphausen, David Lai, and Andrew Scobell, 253–85. Carlisle, PA: U.S. Army War College, 2009.

Nathan, Andrew J. and Andrew Scobell. *China’s Search for Security*. New York: Columbia University Press, 2012.

National People’s Congress and Chinese People’s Political Consultative Conference (NPC&CPPCC). “The 8th Five-Year Plan (1991-1995).” Last modified February 23, 2011. http://www.chinadaily.com.cn/china/2011npc/2011-02/23/content_12068062.htm.

Navy Recruiting Command. “Submarines.” U.S. Department of Defense. Accessed October 12, 2015. http://www.navy.com/about/equipment/vessels/submarines.html.

Negroponte, John D., Samuel J. Palmisano, Adam Segal, Elana Berkowitz, Bob Boorstin, Jeff A. Brueggeman, Peter Cleveland, Esther Dyson, Martha Finnemore, Patrick Gorman, Michael V. Hayden, Eugene J. Huang, Anthony P. Lee, Catherine B. Lotrionte, Susan Markahm Lyne, Naotaka Matsukata, Jeff Moss, Craig James Mundie, Joseph S. Nye Jr., Neal A. Pollard, Elliot J. Schrage, Anne-Marie Slaughter, James B. Steinberg, Lawrence P. Tu, Ernest James Wilson III, Phoebe Yang, and Jonathan L. Zittrain. “Defending an Open, Global, Secure, and Resilient Internet.” *Independent Task Force Report No. 70*. New York: Council on Foreign Relations, 2013. accessedhttp://www.cfr.org/cybersecurity/defending-open-global-secure-resilient-Internet/p30836.

Novetta Threat Research Group. *Bird’s Eye View Report*, no. 1 (March 2015). http://www.novetta.com/wp-content/uploads/2014/11/BirdsEyeView_001_March_2015.pdf

Oakley, John T. “Cyber Warfare: China’s Strategy to Dominate in Cyber Space.” Master’s thesis, Fort Leavenworth, Kansas, 2011. http://www.dtic.mil/dtic/tr/fulltext/u2/a547718.pdf.

Obama, Barak. “Cybersecurity.” Foreign Policy Office. U.S. Whitehouse. Accessed May 19, 2015. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity#section-engage-internationally.

———. “Remarks by President Obama and President Xi of the People’s Republic of China in Joint Press Conference.” Office of the Press Secretary. U.S. Whitehouse. Last modified September 25, 2015. https://www.whitehouse.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

Office of the Secretary of Defense. *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2014*. Washington, DC: Department of Defense, 2014. http://www.defense.gov/pubs/2014_DOD_China_Report.pdf.

Office of the Secretary of Defense. *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2015*. Washington, DC: Department of Defense, 2015. http://www.defense.gov/pubs/2015_China_Military_Power_Report.pdf.

Oxford Dictionaries. “Espionage.” Accessed October 7, 2015. http://www.oxforddictionaries.com/definition/english/espionage.

Pembleton, Gary L. “Assessing Technology Innovation in the PLA.” Master’s thesis, Naval Postgraduate School, Monterey, CA, March 2015. http://hdl.handle.net/10945/45238.

Peng, Guangqian and Yao Youzhi, ed. *The Science of Military Strategy*. Beijing: Military Science Publishing House, 2005.

Pollpeter, Kevin. “Chinese Writings on Cyberwarfare and Coercion.” In *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 138–62. New York: Oxford University Press, 2015.

Public Intelligence. “U.S. Cyber Command Presentation: Assessing Actions Along the Spectrum of Cyberspace Operations.” Last modified August 26, 2013. https://publicintelligence.net/uscc-cyber-spectrum/.

Rawnsley, Gary D. “Old Wine in New Bottles: China-Taiwan Computer-based ‘Information Warfare’ and Propaganda.” *International Affairs* 81, no. 5 (October 2005): 1061–78. http://www.jstor.org/stable/3569075.

Reed, John. “New Images of China’s J-15 Carrier-Based Fighter.” Defense Tech. Last modified September 25, 2011. http://defensetech.org/2011/04/25/new-images-of-chinas-j-15-carrier-based-fighter/.

Reveron, Derek S. “An Introduction to National Security and Cyberspace.” In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron, 3–19. Washington, DC: Georgetown University Press, 2012.

Robinson, Neil. “Cybersecurity Strategies Raise Hopes of International Cooperation.” RAND Review. RAND. Last modified July 11, 2013. http://www.rand.org/pubs/periodicals/randreview/issues/2013/summer/cybersecurity-strategies-raise-hopes-of-international-cooperation.html.

Sanders, Phillip C. and Andrew Scobell. “Introduction: PLA Influence on China’s National Security Policymaking.” In *PLA Influence on China’s National Security Policymaking*, edited by Phillip C. Sanders and Andrew Scobell, 1–32. Stanford, CA: Stanford University Press, 2015.

Segal, Adam. *Advantage: How American Innovation Can Overcome the Asian Challenge*. New York: W. W. Norton & Company, 2011.

———. “Cyberspace: The New Strategic Realm in U.S.-China Relations.” *Strategic Analysis* 38, no.4 (2014): 577–81. http://dx.doi.org/10.1080/09700161.2014.918447.

Scobell, Andrew, Michael McMahon, and Cortez A. Cooper III. “China’s Aircraft Carrier Program: Drivers, Developments, Implications.” *Naval War College Review* 68, no. 4 (Autumn 2015): 65–79. https://www.usnwc.edu/getattachment/c96be200-d3a9-4b6f-9114-179169fa844e/China-s-Aircraft-Carrier-Program--Drivers,-Develop.aspx.

Serger, Sylvia Schwaag and Magnus Breidne. “China’s Fifteen-Year Plan for Science and Technology: An Assessment.” *Asia Policy*, no. 4 (July 2007): 135–64. doi: 10.1353/asp.2007.0013.

Shabad, Theodore. “Communist China’s Five Year Plan.” *Far Eastern Survey* 24, no. 12 (December 1955): 189–91. doi: 10.2307/3023788.

Sheldon, Robert and Joe McReynolds. “Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias.” In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 188–224. New York: Oxford University Press, 2015.

Shipman, J. Scott. “Wylie’s Military Strategy.” U.S. Naval Institute. Last modified July 2011. http://blog.usni.org/2011/07/23/wylies-military-strategy.

Shirk, Susan. *China Fragile Superpower: How China’s Internal Politics Could Derail its Peaceful Rise*. Oxford: Oxford University Press, 2007.

Singer, P.W. and Allen Friedman. “Cult of the Cyber Offensive: Why belief in the First-Strike Advantage is as Misguided Today as it was in 1914.” Foreign Policy. Last modified January 15, 2014, http://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/.

Springut, Micah, Stephen Schlaikjer, and David Chen. *China's Program for Science and Technology Modernization: Implications for American Competitiveness*. Virginia: CENTRA Technology, January 2011. http://origin.www.uscc.gov/sites /default/files/Research/USCC_REPORT_China%27s_Program_forScience_and_ Technology_Modernization.pdf.

Stoker, Liam. "Combat Ships do Battle: LCS versus Type 26." Naval Technology. Last modified August 29, 2012. http://www.naval-technology.com/features/featurecombat-ships-battle-lcs-type-26/.

Stokes, Mark A. "The Chinese People's Liberation Army Computer Network Operations Infrastructure." In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 163–87. New York: Oxford University Press, 2015.

Stokes, Mark A. and L.C. Russell Hsiao. *Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests.* Project 2049 Institute, October 29, 2012. http://www.project2049.net/documents/countering_chinese_ cyber_operations_stokes_hsiao.pdf.

Tarantola, Andrew. "China's J-15 Flying Sharks are Actually Russian Knockoffs." Gizmodo. Last modified January 6, 2014. http://gizmodo.com/chinas-j-15-flying-sharks-are-actually-russian-knockof-1494117956.

Tellis, Ashley J. "The United States and Asia's Rising Giants." In *Strategic Asia 2011–2012: Asia Responds to its Rising Powers China and India*, edited by. Ashley J. Tellis, Travis Tanner, and Jessica Keough, 35–64. Seattle: The National Bureau of Asian Research, 2011.

Theohary, Catherine A. and Anne I. Harrington. *Cyber Operations in DOD Policy and Plans: Issues for Congress* (CRS Report No. R43848). Washington, DC: Congressional Research Service, 2015. fas.org/sgp/crs/natsec/R43848.pdf.

Thomas, Timothy L. "China's Concept of Military Strategy." *Parameters* 44, no. 4 (Winter 2014–2015): 39–48. http://strategicstudiesinstitute.army.mil/pubs/ parameters/Issues/Winter_2014-15/7_ThomasTimothy_ChinasConceptofMilitaryStrategy.pdf.

———. "China's Cyber Incursions: A Theoretical Look at What They See and Why They Do It Based on a Different Strategic Method of Thought." *OE Watch* (March 2013). http://fmso.leavenworth.army.mil/documents/China's-Cyber-Incursions.pdf.

———. "The Chinese Military's Strategic Mind-set." *Military Review* 87, no. 6 (November-December 2007): 47–55. http://fmso.leavenworth.army.mil/documents/chinese-mind-set.pdf.

Thomas, Timothy L., Cindy Hurst, Youngjun Kim, Lianna Faruolo, Scott Moskowitz, and Blaise Zandoli. “A PLA Cyber ‘Rules of the Road’ Proposal.” *OE Watch* 3, no. 7 (July 2013): 48. http://fmso.leavenworth.army.mil/OEWatch/201307/201307.pdf.

ThreatConnect. “Piercing the Cow’s Tongue: China Targeting South China Seas Nations.” Last modified May 19, 2014. http://www.threatconnect.com/piercing-the-cows-tongue-china-targeting-south-china-seas-nations/.

ThreatConnect and Defense Group Inc. (DGI). *Project Camerashy: Closing the Aperture on China’s Unit 78020*. Arlington, VA, 2015. https://www.threatconnect.com/camerashy/.

Toren, Peter. “A Look at 16 Years of EEA Prosecutions.” Law 360. Portfolio Media. Last modified September 19, 2012. http://www.law360.com/articles/378560/a-look-at-16-years-of-eea-prosecutions.

———. *Intellectual Property and Computer Crimes.* 4th ed. New York: Law Journal Press, 2005.

Tucker, Patrick. “White House: No Cyber Attack Pact with China, For Now.” Defense One. Last modified September 22, 2015. http://www.defenseone.com/technology/2015/09/white-house-no-cyber-attack-pact-china-now/121763/.

U.S.-China Economic and Security Review Commission. “Section 2: China’s Cyber Activities.” *2013 Annual Report to Congress.* Washington, DC: USCC, 243–65. http://origin.www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%202%3B%20Section%202%20China%27s%20Cyber%20Activities.pdf.

Valencia, Mark J. “Foreign military Activities in Asian EEZs: Conflict Ahead?” *NBR Special Report*, no. 27, The National Bureau of Asian Research (May 2011): 1–5. http://www.nbr.org/publications/specialreport/pdf/Preview/SR27_EEZs_preview.pdf.

Walsh, Kathleen A. “China’s Defense Technology Acquisition System, Processes, and Future as an Integrator and Supplier.” *The Study of Innovation and Technology in China Policy Brief 2014*. University of California Institute on Global Conflict and Cooperation, January 2014. http://escholarship.org/uc/item/82r7r1nj.

Xu, Beina and Eleanor Albert. “The Chinese Communist Party,” CFR Backgrounders. Council on Foreign Relations. Last updated August 27, 2015. http://www.cfr.org/china/chinese-communist-party/p29443.

Ye, Zheng. “From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond.” In *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 123–37. New York: Oxford University Press, 2015.

Yu, Peter K. “From Pirates to Partners: Protecting Intellectual Property in China in the Twenty-First Century.” *American University Law Review* 50, no. 131 (2001): 131–243, https://www.wcl.american.edu/journal/lawrev/50/yu.pdf.

Zhao, Yan. “China’s ‘KJ-2000’ AWACS Used the Technology that the U.S. and Russia Have Not Yet Used.” China Military Report. Accessed October 12, 2015. http://wuxinghongqi.blogspot.com/2009/10/chinas-kj-2000-awacs-used-technology.html.

Zhou, Dewang, Fu Xiaodong, and Li Rui. “On Cyberspace Confrontation.” Academy of Military Sciences. Edited by Li Hongkai, August 2013. Translated by Open Source Center. Washington, DC, July 2014.

Zhu, Feng. “China’s Rise Will Be Peaceful: How Unipolarity Matters.” In *China’s Ascent: Power, Security, and the Future of International Politics*, edited by Robert S. Ross and Zhu Feng, 34–54. Ithaca: Cornell University Press, 2008.

Zhu, Rongji. “Report on the Outline of the Tenth Five-Year Plan for National Economic and Social Development (2001).” Speech. Fourth Session of the Ninth National People’s Congress, China, March 5, 2001. http://www.gov.cn/english/official/2005-07/29/content_18334.htm.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California