Dean Cheng

CYBER DRAGON

Inside China's Information Warfare and Cyber Operations

The Changing Face of War

PRAEGER SECURITY INTERNATIONAL

Cyber Dragon

Recent Titles in
The Changing Face of War

Mismanaging Mayhem: How Washington Responds to Crisis
James Jay Carafano and Richard Weitz, editors

Private Sector, Public Wars: Contractors in Combat—Afghanistan, Iraq, and Future Conflicts
James Jay Carafano

Fighting Identity: Sacred War and World Change
Michael Vlahos

The Three Images of Ethnic War
Querine Hanlon

Spying in America in the Post 9/11 World: Domestic Threat and the Need for Change
Ronald A. Marks

The Future Faces of War: Population and National Security
Jennifer Dabbs Sciubba

War and Governance: International Security in a Changing World Order
Richard Weitz

Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World
Paul Rosenzweig

Rebuilding American Military Power in the Pacific: A 21-Century Strategy
Robbin Laird, Edward Timperlake, and Richard Weitz

Cyber Dragon

Inside China's Information Warfare and Cyber Operations

Dean Cheng

The Changing Face of War
James Jay Carafano, Series Editor

PRAEGER™

An Imprint of ABC-CLIO, LLC
Santa Barbara, California • Denver, Colorado

Copyright © 2017 by Dean Cheng

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, except for the inclusion of brief quotations in a review, without prior permission in writing from the publisher.

Library of Congress Cataloging-in-Publication Data

Names: Cheng, Dean (Writer on national security) author.
Title: Cyber dragon : inside China's information warfare and cyber operations / Dean Cheng.
Other titles: Inside China's information warfare and cyber operations
Description: Santa Barbara, California : Praeger, an imprint of ABC-CLIO, LLC, [2017] | Series: Changing face of war | Includes bibliographical references and index.
Identifiers: LCCN 2016031254 (print) | LCCN 2016035081 (ebook) | ISBN 9781440835643 (alk. paper) | ISBN 9781440835650 (eBook)
Subjects: LCSH: Information warfare—China. | Cyberspace operations (Military science)—China.
Classification: LCC UA835 .C427 2017 (print) | LCC UA835 (ebook) | DDC 355.3/43—dc23
LC record available at https://lccn.loc.gov/2016031254

ISBN: 978-1-4408-3564-3
EISBN: 978-1-4408-3565-0

21 20 19 18 17 1 2 3 4 5

This book is also available as an eBook.

Praeger
An Imprint of ABC-CLIO, LLC

ABC-CLIO, LLC
130 Cremona Drive, P.O. Box 1911
Santa Barbara, California 93116-1911
www.abc-clio.com

This book is printed on acid-free paper ∞

Manufactured in the United States of America

To Dr. James Carafano, without whom this book would never have started

and

To Sharon Cheng, without whom this book would never have been completed.

This page intentionally left blank

Contents

Acknowledgments ix

Chapter 1 **Setting the Stage: China's Evolving Views of Information** 1

Chapter 2 **China's Military: This Is Not Your Father's PLA** 18

Chapter 3 **Informationized Conflict: Maintaining Party Control amid the Information Revolution** 37

Chapter 4 **Information Warfare: Waging Information Campaigns in the Next War** 79

Chapter 5 **Information Operations: Putting Theory into Practice** 116

Chapter 6 **Space and Information Warfare: A Key Battleground for Information Dominance** 155

Chapter 7 **Organizing to Secure Information Dominance** 177

Chapter 8 **Chinese Views of Future Warfare and Implications for the United States** 200

Notes 223

Bibliography 255

Index 281

This page intentionally left blank

Acknowledgments

Writing this volume has been a reminder of how much "I get by with a little help from my friends."

To begin with, I must offer my thanks to Dr. James Carafano and Sharon Cheng, to whom this volume is dedicated. It was Dr. Carafano's prodding that got me to start this undertaking. It is safe to say that without his encouragement I would not have begun this journey.

Sharon helped keep me on the straight and narrow. She kept watch so that I met deadlines, endured the inevitable periods of crankiness and cantankerousness, and rarely uttered a cross word, no matter how many reams of paper seemed to overflow out of my office. Without her steadfastness, I would not have completed this journey.

My sincerest thanks to Walter Lohman, whose patience and flexibility gave me the time necessary to research and write in an uninterrupted fashion. If this volume is useful to you, the reader, credit must go in large part to Walter's generosity in granting me the time to make it so. And my deepest appreciation to Nick Zahn, whose counsel was central in the initiation of this volume.

For the most precious gift, that of time, I would like to offer my gratitude to Kathy Gudgel, Priscilla Guthrie, and Richard Larach. Busy professionals, each nonetheless kindly responded to my requests for comments on various drafts.

Thanks, as well, to Steve Catalano, the acquisitions editor at Praeger. His advice and assistance to this neophyte author were instrumental in navigating the proposal and approval process.

Finally, my sincerest appreciation to the intellectual godparents of this volume. Any methodological rigor that inhabits these pages is due in large part to Dr. David Finkelstein, who has always been a great mentor and friend.

My ability to understand Chinese at all, much less sufficiently to exploit the various sources used herein, is purely the result of my mother and the time she spent as an educational Drill Instructor.

And, my thanks to the Heritage Foundation. In a world where the focus too often has shifted to fund-raising and the intellectual close-in battle, it is an oasis where one has the opportunity to engage in longer-term study and analysis, to dig deeper and think wider.

1 Chapter

Setting the Stage: China's Evolving Views of Information

As a society that has revered learning and education for millennia, China has a long history of valuing information. As a disadvantaged, developing country for much of the past century, Chinese leaders, whether imperial, republican, or Communist, have recognized the importance of increasing their access to technical and military information in order to help improve China's standing and capabilities. As a Marxist–Leninist dictatorship for the past several decades, the Chinese Communist Party (CCP) leadership has understood the importance of controlling information, as a central element of retaining power.

This evolving view of the relationship between information and power has crystalized in the past half century, as the world economy has globalized, and as information has become even more integrated with development. Beginning in the 1970s, the proliferation of microelectronics, computers, and telecommunications technology has accelerated the ability to gather, store, manage, and transmit information. Information technology, including computers and telecommunications systems, has permeated all aspects of society and economies and become an integral part of a nation's infrastructure.[1] Chinese analysts have dubbed this process "informationization" (*xinxihua;* 信息化).

From the Chinese perspective,

> Informationization is a comprehensive system of systems, where the broad use of information technology is the guide, where information resources are the core, where information networks are the foundation, where information industry is the support, where information talent is a key factor, where laws, policies, and standards are the safeguard.[2]

In the face of this broad trend of economic, political, and social informationization, Chinese analysts have concluded that threats to national interests and security have also become informationized.

The spread of information technology means that potential adversaries have unprecedented access to each other's national economy, as well as the broader population and the top decision-makers. Just as the bomber and long-range missile allows an opponent to directly strike a nation without having to first break through ground or naval defenses, so too information technology outflanks traditional military forces. The proliferation of information technology into society and economies makes them vulnerable to a range of new pressures and threats.

These threats extend beyond information networks (e.g., vulnerability to denial-of-service attacks) and component computers (e.g., computer viruses, malware). Instead, the very information itself can constitute a threat, if, for example, its content erodes the morale of key decision-makers, popular support for a conflict, or the will of the military to fight. Consequently, China's interpretation of its national interests has expanded, in step with the expanding impact of information writ large on China.

This growing importance of information technology inevitably influences the nature of warfare. Informationized societies and economies lead to informationized wars, which in turn require informationized militaries to fight them successfully. This reflects the interplay between the military and the larger economy and society. Mechanized military forces are a reflection of the Industrial Age, including both industrial economies and an industrialized society. Correspondingly, an informationized society will create an informationized military, while an informationized military can be produced only by an informationized society and economy. In the Chinese view, the People's Liberation Army (PLA) and broader security establishment must be prepared for "informationized warfare" (*xinxihua zhanzheng;* 信息化战争).

In December 2004, Hu Jintao, in his role as chairman of the Central Military Commission, gave a major speech wherein he charged the PLA with a set of "historic missions for the new phase of the new century," commonly referred to as the "new historic missions." The speech essentially provided guidance for what the PLA should be preparing for, given changes in the international strategic context and national development. One of the new historic missions was to "provide strong strategic support for maintaining the nation's interests." While those interests still center on issues of territorial integrity and national sovereignty, they now also extend to outer space and the electromagnetic spectrum, and into the information domain.[3]

INCREASING INFORMATIONIZATION

As early as the 1980s, the People's Republic of China (PRC) began to pay attention to information technology. This was one of the original seven focal

areas for Plan 863, the Chinese National High-Technology Research and Development Plan established in 1986, which sought to promote and accelerate China's capabilities in key technological areas.[4] Initial efforts in this domain included promoting fiber-optic technology in order to facilitate the creation of a Chinese information superhighway, as well as the development of large-scale parallel and distributed computing and symmetrical multiprocessing.[5] China also promoted its own personal computers, the "Legend" brand.

As information technology rapidly advanced throughout the 1990s, China's leaders recognized its growing impact and sought to ensure that China would not be left behind. In 1991, China first joined the Internet, as the Institute of High Energy Physics leased a direct international line to the United States.[6]

In 1993, the PRC established the State Economic Informationization Joint Council. While China had already spent a decade moving away from the stifling hand of centralized economic control, traditional state planning was still heavily emphasized. This new council promoted advances in information technology to gather more and better economic data to assist national development planning. It soon became evident, however, that rapid global advances in information technology had impacts beyond the narrow focus on economic data and national planning. These advances made information technology itself important—and also required thinking beyond computers and fiber optics to information networks and the human capital needed to design and manage them.

Similarly, Deng Xiaoping had already made clear that China could not hope to modernize in isolation and threw open the doors to foreign trade and investment. His successor Jiang Zemin expanded this view, pushing for China to establish a broader presence on the Internet, at that point still an entity largely limited to the United States. In Jiang's view, it was essential that China be plugged into the global information network if it was to sustain its modernization efforts.

THE LEADING SMALL GROUPS

In the People's Republic of China (PRC), power and authority are bifurcated between the Chinese Communist Party (CCP) and the Chinese government. The CCP's Political Bureau (Politburo), the top 24 members of the party's 200-member Central Committee, and especially the Politburo Standing Committee (PSC), seven to nine members of the Politburo, are the leadership cohort of the party. Policy issues are decided by the Politburo or the PSC.

Policy is implemented by the machinery of the Chinese government, through the various ministries and commissions. While all ministers and senior leaders are party members, they are not necessarily of sufficient party rank to be on the Politburo. This can create divides, such as in foreign policy. As of 2016, no Chinese foreign minister has been a member of the Politburo, much less of the PSC, since

the late 1990s. In essence, the foreign minister is not part of the foreign policy–setting system. This system is replicated throughout the PRC political structure, from national to provincial and township levels.

In order to ensure proper coordination between policy setting and policy implementation, there is a system of "leading small groups" (*lingdao xiaozu;* 领导小组), or LSGs, that brings together relevant senior party leaders and ministers and heads of other government bureaucracies at each level of governance. There are three types of national-level LSGs:

- Permanent LSGs that focus on ongoing issues of strategic importance
- Term-oriented LSGs that focus on single programs, such as the Olympics or nuclear development
- Task-oriented small groups that are assembled for shorter-term tasks—often in response to crises, such as earthquakes[7]

While LSGs are typically headed by a principal member of the party leadership at the relevant level, there is no single template governing the organization of the various LSGs. Their staffing varies from group to group, with no standard operating rules, as far as is known.

LSGs serve as venues to bring various stakeholders together, providing background information and generally informing participants (and their home bureaucracies) of the state of policy setting and policy implementation on their topic. LSGs can solicit expert opinions and reconcile views among stakeholder entities.

They also ensure policy implementation. Meetings of the LSGs usually involve updates to key leaders in both the party and the state on how given policies are being implemented. They also present an opportunity for mid-course corrections, incorporating new information and responding to recent developments.

An important part of any LSG is its central or general office, which contains the staff who support LSG meetings. The members of the general office provide background information and research in response to member requests and can arrange for outside testimony, and its director helps set the agenda for meetings.[8]

The Central Group for Internet Security and Informationization, created and headed by Xi Jinping, therefore helps coordinate policy implementation regarding these issues, bringing together the key elements of the party leadership and state ministries. It is expected to typically meet several times a year to provide Xi and other members with updates on how those policies are being implemented. Reporting to Xi and other members of the LSG, as the head of its general office (which is apparently also referred to as the Cyberspace Administration of China), would be Lu Wei. Mr. Lu also serves as head of the State Internet Information Office, the governmental counterpart to the Cyberspace Administration of China.

China's information networks, in terms of both international and domestic connectivity, steadily grew throughout the 1990s. In 1996, the State Council Informationization Work Leading Small Group (LSG) was established. Headed by Vice Premier Zou Jiahua, it promoted broader use of information and information technology across all parts of the Chinese government. Information

technology and informationization was incorporated into the Ninth Five-Year Plan (1996–2000), emphasizing the construction of China's telecommunications infrastructure. This included domestic digital mobile communications equipment and program-controlled switchboards. China's networks would be assembled from Chinese-manufactured hardware.

The Chinese simultaneously introduced a series of information programs, part of the "Golden projects," to push Chinese information exploitation forward. These included the following:

- *Golden Bridge* (*jinqiao;* 金桥). An information infrastructure to facilitate the movement of economic information
- *Golden Card* (*jinka;* 金卡). A nationwide payment system promoting the use of credit and debit cards in what had been a cash-driven economy
- *Golden Tax* (*jinshui;* 金税). Computerization of the nation's tax system, to reduce fraud and tax dodging while simplifying tax payments[9]

It was also during this period that the Chinese "Golden Shield" (*jindun;* 金盾) project was initiated. While China was interested in joining the global telecommunications network, it sought to control what could be accessed. Even as China was taking its first steps into connectivity, research was under way to ensure that those connections were firmly under the control and supervision of the CCP and its censors. The Golden Shield project, popularly known as the "Great Firewall of China," constituted an initial step of defending the PRC from unauthorized information proliferation from without—and within.

Informationization is based on more than technology, however. As information was increasingly emphasized, new bureaucracies arose and industries were reorganized. Chinese informationization efforts were guided by the slogan of "Thorough planning, national leadership; unified standards, joint construction; mutual linkages, shared resources." This reflected efforts to standardize and unify Chinese information technology, increasing compatibility and reducing duplication. In 1998, the Ministry of Information Industries (MII) was organized to supervise China's information industry development. This entity seems to have eclipsed the State Council Informationization Work LSG.

This consolidation was apparently insufficient. In December 1999, the State Informationization Work Leading Small Group was formed. It was headed by Wu Bangguo, a member of Jiang Zemin's Politburo Standing Committee. This LSG promoted further informationization. It was very limited in authority and organization, however, and relied on the MII for its support and staffing.[10]

Yet another reorganization occurred less than two years later, with the establishment of a revived State Informationization Leading Small Group (SILSG) in August 2001, under Premier Zhu Rongji, one of the key architects

and supporters of broader Chinese economic reform (and number two in the CCP hierarchy at the time). This series of reorganizations reflected not only the need to promote informationization but a sense of its growing importance, as more and more senior leaders were included in each iteration of this LSG.[11] As one Chinese observer noted, "Compared with the 1999 State Informationization Work Leading Small Group, the newly organized leading small group's membership was more senior," including the head of the State Council, two members of the Politburo Standing Committee, and two other members of the broader Politburo.[12] This likely reflects the larger effort by Jiang and the senior party leadership to refocus Chinese informationization efforts from building an information *economy* to an information *society*.

In 2002, at the 16th Party Congress, informationization was formally recognized as essential for growing Chinese "comprehensive national power" (*zonghe guojia liliang;* 综合国家力量). General Secretary Jiang Zemin emphasized the Chinese path to industrialization and economic modernization would depend on the information sector. Jiang noted that information technology was the "logical choice" if Chinese industrialization was to accelerate, especially since informationization would generate other benefits, including raising the overall level of scientific and technical awareness, reducing resource consumption, and developing Chinese human resources. Therefore, "we must give priority to the development of the information industry and apply IT in all areas of economic and social development."[13]

In the 10th Five-Year Plan (2001–2005), national informationization was among the 16 priorities. To achieve this, the government would:

- Promote the information technology sector
- Increase the accessibility and use of computers and computer networks
- Expand the use of digital and network technologies
- Further expand the national information infrastructure, including broadband and telecommunications networks[14]

As Hu Jintao rose to the top leadership positions in 2002 and 2004, the Chinese leadership shifted gears on broader economic policies. Hu and his premier Wen Jiabao were far less enamored of economic reform than their predecessors Jiang Zemin and Zhu Rongji. Nonetheless, they recognized the importance of expanding the role of information technology in the PRC.

In 2005, the Chinese government promulgated the "National Strategy for Informationization Development, 2006–2020." This charted a course for China's efforts to expand and deepen information technology. Major priorities would be increasing the level of informationization in the national economy and society; expanding information and communications infrastructure (e.g., making broadband more widely available); promoting the application of information technology in healthcare, education, and government operations; and improving Chinese global competitiveness in information-related

technology production, including the development of more sophisticated computer programs and applications. Chinese information security systems would meanwhile be strengthened, and informationization of public security ministries would be enhanced.

In 2007, after the 17th Party Congress, the SILSG included five members of the Politburo (out of 24). Not only was this a substantial slice of Chinese political power, reflecting highest-level attention, but military and internal security interests increasingly dominated.[15] This was further reinforced the following year, when the PRC consolidated much of the information technology and aerospace sectors into a new superministry, the Ministry of Industry and Information Technology (MIIT), which also oversees the military industrial complex (through the State Administration for Science, Technology, and Industry for National Defense, or SASTIND).

All of these measures ultimately reflected the interest of the Chinese leadership in expanding its comprehensive national power, which could happen only if information technologies were incorporated and integrated into the broader society. This is the essence of informationization, from the Chinese perspective.

These efforts have borne steady fruit, as China's presence on the Internet and level of computerization has steadily expanded. In 2000, according to the International Telecommunications Union (ITU), China had Internet usage penetration of less than 2 percent, with some 22.5 million users in a population of 1.28 billion. This had more than doubled by 2002, to 59 million users, representing 4.6 percent penetration.[16] By December 2013, the China Internet Network Information Center (CNNIC) reported some 618 million Chinese Internet users, marking a 45.8 percent penetration rate. The CNNIC also reports that 93 percent of Chinese businesses used computers and 83.2 percent used the Internet while much of China accesses the Internet via their mobile phones (the foremost means of Internet connectivity in the PRC).[17] Many Chinese used the Internet for shopping (302 million in 2013), engaged in mobile online gaming (215 million), and instant messaging (532 million). As the CNNIC noted, mobile instant messaging has rapidly expanded because "such applications as information sharing, communication, payment and finance have been added [to mobile communication] based on social contact elements, which has greatly increased user stickiness," that is, willingness of users to stay at a given site.[18] China is clearly on the path toward becoming an information society.

MAINTAINING CONTROL OVER INFORMATION: THE CASE OF CHINESE NEWS

As information has assumed a greater role in economics and society, it has also become a central part of national security considerations. This includes not only generation of military power but a broader revolution in what

constitutes a security threat. For China's leaders, this radical alteration in the central means of generating power and influencing society has required incorporating information management into both peacetime and wartime security planning. This is typified in how the CCP strives to control news, even in the era of informationization.

In some ways, this effort at controlling the various forms of new media is an updating of the Chinese leadership's traditional approach to security. The CCP has always tried to control what information reaches the populace. While the Chinese news environment is more open today than it was during the Mao Zedong era, with a major proliferation of media outlets, the Chinese government continues to exercise very strict control over news media. Indeed, Reporters without Borders ranked China near the bottom of nations for press freedom, ranking it 176 out of 180 countries in its 2015 World Press Freedom Index.[19]

The Chinese news environment has become much more complex, as nonofficial news outlets now exist alongside the state-run news agency Xinhua and state-run national media organizations such as China Central Television (CCTV), *People's Daily,* and provincial-level entities. It is important to recognize that these new entities may not be state run, but they are not a truly private or free press. Many commercially oriented newspapers were spawned by state media organizations to raise additional revenue. *Southern Weekly,* for example, was spun off from Guangdong Province's official newspaper *Nanfang Daily*.[20]

Many of these new media organizations have proven to be very popular. In 2011, a dozen commercially published Chinese newspapers had circulations exceeding one million.[21] These nonofficial outlets enjoy substantial readership because of higher levels of credibility with the broader population. "Official media sources are considered to be experts on the position of the state and aimed at manipulating public opinion. In contrast, nonofficial media sources are seen as reporting from the perspective of the public in a less biased way."[22]

In reality, however, nonofficial media operate under only slightly looser reins than their official counterparts. Indeed, "asked about whether media commercialization has brought about greater independence, journalists and editors commonly answer, 'There is no fully commercialized and private media'" in China.[23]

The CCP's Central Propaganda Department (CPD) exercises close oversight of all Chinese media (including cultural as well as news products). The CPD, in conjunction with state entities such as the State Council Information Office, the General Administration of Press and Publication (GAPP), and the State Administration of Press and Publication, Radio, Film, and Television

(SAPPRFT), as well as their respective subsidiary provincial-level party propaganda departments, ministries, and offices, regularly reviews the content of all Chinese media. This includes not only news broadcasts but television and radio programs, films, and so on.[24] The CPD regularly issues directives on news topics, dictating what topics should, and as important *should not*, be covered. These directives also provide guidance on which specific perspectives should be allowed, should be encouraged, or are forbidden.[25] Depending on the topic, these instructions often apply not only to official state-run media but to nonofficial media as well.

On July 23, 2011, two high-speed trains were involved in a horrific collision outside Wenzhou city in Zhejiang Province. The crash killed some 40 people and injured hundreds more. Initial reporting on the subject was sparse but soon became critical of authorities. Chinese journalists reported that the Railway Ministry had buried some wrecked cars rather than examining them carefully and suspended rescue operations too early. CCTV and newspaper commentators questioned whether the emphasis on rapid national development had overridden safety concerns.[26]

Chinese press censorship began almost immediately. The CPD instructed Chinese journalists not to question official accounts, stating, "Do not question, do not elaborate."[27] Initially, these instructions were not always obeyed. By the following week, however, stricter controls had been imposed. The CPD issued directives warning reporters not to draw any conclusions regarding China's larger effort to promote bullet train development. News media were instructed to write "stories that are extremely moving, for example people donating blood and taxi drivers not accepting fares."[28] Many media sites pulled articles, focused on more upbeat aspects, and often deleted older, more critical stories.[29]

In some cases, censors are much more decisive and overt in their actions. In 2013, the nonofficial newspaper *Southern Weekly* wrote a front-page editorial calling for greater adherence to the Chinese constitution. The Guangdong provincial propaganda ministry (under whose purview *Southern Weekly* operates) replaced it with an essay praising the CCP. Within hours, and over the course of the following week, the national-level CPD issued several directives regarding the rewriting of the newspaper's front page. At first, it forbade any discussion of the situation. It then dictated exactly how it could be described in other news media. Eventually, other newspapers in China were also directed to publish an op-ed that had originally appeared in *Global Times* (a commercial newspaper in the *People's Daily* publishing group), which criticized the originally planned op-ed. Interestingly, the CPD's directive also noted that "external hostile forces are involved in the development of the situation."

DIRECTIVES FROM THE CENTRAL PROPAGANDA DEPARTMENT REGARDING *SOUTHERN WEEKLY*

The Central Propaganda Department's (CPD's) instructions on how to cover the *Southern Weekly* story in January 2013 provide useful insight into how the CPD tries to shape and mold public perceptions. While the CPD initially sought to prevent any discussions, within a week, it had evolved toward influencing the story instead, as seen in these directives provided by China Digital Times. This evolution, and overall rapid response, suggests a flexible organization able to adjust course on short notice.

Central Propaganda Department: Urgent Notice: Upon receipt of this message, controlling departments in all locales must immediately inform all reporters and editors that they may not discuss the *Southern Weekly* New Year's greeting on any public platforms (January 3, 2013).

中宣部：紧急通知，各地主管部门务必于第一时间逐一通知到所有媒体记者、编辑，不得在任何公开平台讨论关于南周新年献辞事件。[30]

Central Propaganda Department: No media, official Weibo accounts, or individual Weibo accounts are to republish or comment on the *Southern Weekly* incident. Do not share the *Global Times* opinion piece or the incendiary Dragon TV program about the New Year's greeting. Henceforth, it is forbidden to republish reports on the aforementioned incident (January 4, 2013).

中宣部：各媒体官方微博及个人微博不转、不评南方周末事件，不转环球时报评论及东方卫视新年献词惹热议节目。今后对同一事件的报道均不得转载。[31]

Central Propaganda Department: Urgent Notice Concerning the *Southern Weekly* New Year's Message Publication Incident: Responsible party committees and media at all levels must be clear on three points related to this matter: (1) party control of the media is an unwavering basic principle; (2) this mishap at *Southern Weekly* has nothing to do with Guangdong propaganda department head Tuo Zhen; (3) external hostile forces are involved in the development of the situation. Every responsible work unit must demand that its department's editors, reporters, and staff discontinue voicing their support for *Southern Weekly* online. Starting tomorrow, media and websites in all locales must prominently republish the *Global Times* editorial "Southern Weekly's 'Message to Readers' Is Food for Thought Indeed" (January 7, 2013).

中宣部：关于南方周末新年献辞出版事件的紧急通知，各级主管党委和媒体，对于此次事件，必须明确以下三点：一，党管媒体是不可动摇的基本原则；二， 南方周末此次出版事故与广东省委宣传部长庹震同志无关；三，此事的发展有境外敌对势力介入。各主管单位必须严格要求其部门的编辑，记者和员工不得继续在网 络上发言支持南方周末。各地媒体、网站明天起以显著版面转发《环球时报》的社评《南方周末"致读者"实在令人深思》。[32]

The intervention of the CPD carries with it the threat of punishment for noncompliance. Violations of CPD-issued guidelines can lead to fines, job dismissal, jail time, or even closure of a given outlet. In 2006, an ongoing effort by the Chinese leadership to rein in the press saw the closing of *Bing Dian* ("Freezing Point"), a weekly newspaper with ties to the official outlet *China*

Youth Daily. Chinese authorities stated that *Bing Dian* had been shut down for publishing an extended study of Chinese middle-school textbooks that claimed the textbooks incorporated major official distortions of history.[33]

Even the publication or discussion of the CPD's guidance is potentially punishable, should any given instruction be deemed a "state secret."[34] In July 2014, the SAPPRFT declared that "Journalists must never violate rules or provide any information about their professional conduct to other domestic or foreign media and websites."

> "Professional conduct" was defined as "any kind of information, source material or news product" acquired or made by "reporters, editors, broadcasters, anchors, as well as other newsroom staff who provide support to them", including "state secrets."[35]

The potential for sanctions aimed at not only individual journalists but their affiliated outlet seeks to inculcate a culture of self-censorship by both. For a nation as large as China, self-policing is much more efficient than externally imposed oversight. Investigations and closer monitoring can then focus on more persistent troublemakers and potential threats.

These restrictions also inhibit professional exchanges and cooperation with foreign media, another potential vulnerability in Chinese media control. The same instructions note that Chinese journalists are strictly prohibited from serving as a contributing writer, columnist, correspondent, or reporter with foreign media organizations. Chinese citizens who work as assistants to foreign media organizations are regularly harassed or arrested.[36] In essence, the government seeks to limit those who best understand the Chinese media structure from tutoring or educating their counterparts.

Chinese Efforts to Control Foreign Media

Chinese authorities try to exercise similar influence over foreign news organizations. China allows only a limited number of J-1 resident foreign journalist visas, thereby restricting the number of people who may operate officially as journalists. Even that low number is granted only after a tortuous process.[37] Journalists from Bloomberg News and the *New York Times* could not get their visas renewed after their organizations published stories detailing corruption in China's leadership ranks.

When a *New York Times* reporter raised this issue during a joint press conference between President Barack Obama and President Xi Jinping, the Chinese leader made clear that the fault lay with Western news organizations.

> "Media outlets need to obey China's laws and regulations," Xi said, before launching into a metaphor suggesting that news outlets'

> credentialing problems were the organizations' own fault. "When a car breaks down in the road, we need to get off the car to see where the problem lies. . . . In Chinese, we have a saying: The party which has created the problem, should be the one to help solve it."[38]

Journalists seeking to enter China for specific stories have little better time of it. Obtaining a J-2 temporary journalist's visa requires securing formal letters of invitation from Chinese-based organizations. This effectively makes hosts responsible for the behavior (including questions and stories) of foreign journalists; not surprisingly, this further discourages openness to foreign reporters. It also limits visiting journalists from reporting on any other issues during their stay. Interviews can be difficult, if not impossible, to obtain, and movement can be monitored, if the journalist strays far from his official focus.

Even when foreign journalists are able to enter the PRC, their access remains limited. The Chinese Foreign Ministry only expanded its press briefings to five times a week in 2011, after holding to a twice-weekly schedule since 1999. Not until 2014 were foreign journalists able to attend the monthly press conference that the Ministry of Defense began holding in 2011. Furthermore, many of the press briefings have been scripted, involving extensive negotiations on what topics would and would not be allowed, how the questions would be phrased, and even in what order questions would be posed.[39] The goal is not to *provide* information but to shape how any information that *is* allowed to disseminate may be presented and therefore perceived.

Chinese efforts to control dissemination and interpretation of information have modernized as the technology has improved. Foreign media organizations that cover China now often experience attacks against their computer networks, especially if they cover stories that embarrass the Chinese leadership or are otherwise sensitive. In 2012, Bo Xilai, party secretary of the provincial-level city of Chongqing, became embroiled in a massive scandal. His wife was charged (and later convicted) of murdering a British national. The Chongqing police chief fled to the U.S. consulate in nearby Chengdu and may have tried to defect. Eventually, Bo himself was expelled from the CCP and later arrested on charges of corruption. All of this was highly controversial and embarrassing to the Chinese leadership, which was in the midst of a power transition from Hu Jintao to Xi Jinping. The U.S.-based website Boxun.com, which provided extensive coverage of the Bo scandal, experienced unremitting attacks on its website, eventually forcing it to shift hosting companies.

Later in 2012, Bloomberg News, the *New York Times,* and the *Wall Street Journal,* which had all reported on Chinese corruption issues, found themselves under concerted, intensive computer hacker attacks.[40] These attacks included theft of various reporters' passwords and penetrations of the

companies' e-mail systems to determine reporters' contacts, as well as apparent monitoring of reporters' stories and investigations.

UNDERSTANDING HOW THE PLA THINKS OF FUTURE WARS

If information is central to maintaining the CCP's grip on power, the PLA has concluded that it is also vital for fighting and winning future wars. The Chinese military has devoted substantial energy over the past 25 years to understanding the nature of Information Age wars and preparing itself for them. This has required overhauling the entire PLA, including core concepts such as its strategic guiding thoughts and basic operational principles, and has led to the creation in 2015 and 2016 of several new services as well as complete restructuring of the PLA's administrative headquarters and war-fighting commands.

Nor is this process complete. It is clear, from the PLA's own writings and statements, that it is still both carefully analyzing other people's wars and broader international trends and engaging in close assessments of its own capabilities.

In order to modernize itself and accommodate these changes, the PLA has had to keep its own officers and troops informed about its thinking on informationized warfare. To do this for a military over two million strong, it has produced a variety of reference materials, textbooks, teaching materials, as well as professional readings. This volume examines a wide array of such writings, in order to provide an understanding of how the PLA discusses information and warfare.

These Chinese writings generally fall into five broad categories:

- *PLA reference materials*. These comprise volumes such as official military encyclopedias and military dictionaries. These are materials used by the PLA itself to provide consistent definitions and explanations of key concepts and reflect the corporate knowledge of the PLA.
- *PLA textbooks*. These are recently published books that are required readings for PLA officers at institutions of professional military education. These provide a common foundation of knowledge for PLA officers.
- *PLA teaching materials*. In addition to PLA textbooks and reference materials, the PLA publishes an extensive array of supplemental teaching materials. These complement the textbooks and reference materials, as part of a professional military educational curriculum. They flesh out concepts laid out in the textbooks, often providing more extensive analysis, exploration of key concepts, and enumeration of guiding concepts

and basic principles of operations. There are typically study-aid-type questions at the conclusion of each chapter, further identifying key concepts and terms.

- *Professional military journals*. Any organization as large as the PLA will have professional journals to facilitate debates about future concepts, airing of various points of view, and informing the overall body of new developments. The PLA is no different; indeed, it publishes a range of newspapers and journals not only for the entire PLA (e.g., *People's Liberation Army Daily, China Military Science*) but for narrower audiences (e.g., *Journal of the Academy of Equipment*).
- *Professional reading materials*. The PLA also publishes various volumes on more specific topics. These are not teaching materials or textbooks but are study guides and volumes of "frequently asked questions." These provide important insight into Chinese views of fundamental operational issues.

From this array of materials, this volume will try to provide the reader with some insight into how the PLA talks and writes about the interplay of information and future security. It will begin with an introduction to the PLA. The next three chapters will explain the key, interrelated concepts of "informationized warfare," "information warfare," and "information operations," as the PLA uses those terms.

Because the Chinese see future space operations as a key determinant of who is likely to dominate the information environment, Chapter 6 will review recent Chinese military writings on space-related activities.

As the PLA has never been organized entirely along Western military lines, Chapter 7 will provide an overview of some key Chinese military organizations charged with implementing information warfare. It will also provide some initial thoughts on the 2016 reorganization of the PLA and how it might affect Chinese informationized warfare efforts.

It is important to caution that this volume is *not* an assessment of how well the PLA can wage "local wars under informationized conditions." The PLA has not fought a war since it concluded hostilities with Vietnam in the early 1980s, so it is impossible to know with any precision how it will perform in any future war, its first in a generation or more.

Rather, Chinese writings provide insight into PLA aspirations—where it hopes to wind up, rather than necessarily where it is. These aspirations and interim objectives in turn provide a framework for assessing current and future Chinese activities and efforts. It is sobering to consider, however, that the PLA of today hews closely to the aspirational doctrine laid out by the PLA in the 1990s.

EXECUTIVE SUMMARY

The Chinese leadership believes we now live in the Information Age. Over the past quarter century, the leadership of the People's Republic of China (PRC) has been increasingly focused on moving China into the Information Age. From the perspective of the Chinese Communist Party (CCP) leaders, this is a matter of national as well as regime survival. The new currency of "comprehensive national power"—the measurement of a state and society's power, which includes military, economic, political, diplomatic, science and technology, and cultural components—is measured in terms of information.

Information has become decisively important in the conduct of current and likely future wars. In the view of the Chinese People's Liberation Army (PLA), the rise of the Information Age means that future wars will be contests in the ability to exploit information. Such informationized warfare will be the hallmark of the Information Age, as mechanized warfare was for the Industrial Age. Wars will be decided by the side better able to generate, gather, transmit, analyze, and exploit information. This will require the PLA to sustain its efforts to focus more on quality than quantity and to improve its ability to conduct joint operations.

The PLA is reorienting itself, at a fundamental level, to better conduct informationized warfare, information warfare, and information operations. The PLA has never been organized entirely along Western lines; there has always been a lesser emphasis on services and greater focus on different functions (especially with a political department). This divergence will grow in the future, as the PLA modifies itself to fight informationized wars. The resulting overhaul already touches on every aspect of the PLA, including not only its equipment but its doctrine (how the equipment will best be used), its training, and even its organizational layout, in terms of both peacetime administration and wartime command.

Informationized warfare blurs the lines between peacetime and wartime, between what is considered military and what is considered civilian. Part of this overhaul is necessary because, in the Information Age, peace and war, military and civilian are increasingly indistinguishable. One cannot wait until the outbreak of war to gather intelligence, influence psychological outlooks, develop antisatellite systems, or design computer software weapons. The interlinkages of information infrastructure mean that all of these elements are melded together. The preparation and conduct of informationized warfare will therefore include activities in peacetime, aimed at civilian and commercial entities, as well as wartime operations against adversary military systems.

Informationized warfare is more than just cyber warfare; cyber warfare is just one piece of the larger whole. In the Chinese view, informationized warfare extends beyond cyber activities and is instead about establishing "information

dominance." This involves being able to gather, transmit, analyze, assess, and exploit information more quickly and more accurately than one's adversary. It includes the conduct of political warfare, which shapes and influences friendly, adversary, and third-party views and assessments. Winning future wars will depend upon winning information dominance, while denying it to the adversary.

Establishing information dominance involves waging information warfare. This encompasses a range of military operations, including warfare in the electromagnetic domain, warfare across networks, and warfare of the mind and perception, that is, electronic warfare, network warfare, and psychological warfare. There will be special emphasis placed on targeting the adversary's command and control and intelligence organizations and infrastructure, at the strategic, operational, and tactical levels of conflict, as these are the most important networks, systems, and commanders. Information warfare also entails establishing space dominance, because of the extent to which various nations depend on space-based systems for collecting and transmitting their information. In all of these cases, what matters is the information, rather than the hardware or software per se. Information has itself become not only a resource but a weapon.

Information warfare is comprised of an extensive array of information operations. These include reconnaissance operations, offensive and defensive operations, and deterrence operations, in the electromagnetic, network, and psychological realms. It also includes the employment of physically destructive means against key information infrastructure targets, ranging from satellite constellations to landlines and command posts. Just as information warfare is about more than computer network warfare, information operations involve more than just interfering with information systems.

Information warfare is fundamentally shaping the PLA, including its organization. Several of the major reforms announced in 2015 and 2016 are aimed at sharpening the PLA's ability to secure information dominance. This includes the creation of a new service, the PLA Strategic Support Force, which will bring under a single bureaucratic umbrella all the key combat elements that the PLA believes are central to waging information warfare—space forces, network warfare (cyber) forces, and electronic warfare forces.

For American decision-makers and analysts, understanding the context of Chinese information activities is as important as determining the specific actions being undertaken. Influencing Chinese information operations requires understanding the context within which they occur. Deterring them from waging informationized wars requires holding at risk what the Chinese leadership values. Only by understanding the Chinese leadership's perspective can the United States effectively counter the PRC. Even then, given the high priority accorded to improving China's comprehensive national power, and

the PLA's relentless preparations to fight and win future informationized wars, success is not assured.

A NOTE ON TRANSLATIONS

There is an Italian phrase *Traduttore, traditore,* which roughly means "translator, traitor." It captures the idea that translation is, at best, imperfect. There are many different ways to translate any given phrase, and capturing the nuance as well as the literal translation is always a challenge.

In the first place, there are always different ways to translate any given phrase. *Ronghe* (融合) may be translated as "melded" (as I have in this volume) or as "fused" or "integrated." All of these meanings are clearly synonymous.

This is further complicated, however, because in some instances, the same phrase has very different meanings, depending on the context. Thus, the Chinese term *zuozhan* (作战) will sometimes mean "operations" and in other instances mean "combat."

Similarly, the Chinese term *weishe* (威慑), while translated as "deterrence," also embodies the idea of "coercion."

In still other cases, different phrases all translate to the same phrase in English but cover different aspects that the English phrase embodies. Thus *zhengti* (整体) and *yiti* (一体) are often translated as "integrated," but there are differences in nuance and intensity.

Finally, translations are always somewhat idiosyncratic, based on the choices and mental associations of the translator.

In general, I have tried to include the Chinese characters where there may be some confusion or disagreement, so that the reader can be aware of the specific Chinese term.

2 Chapter

China's Military: This Is Not Your Father's PLA

The Chinese People's Liberation Army (PLA) is the world's largest military. It has two million people under arms. It fields over 20 divisions and 70 brigades in its ground forces; over 70 major surface combatants and 65 submarines in the PLA Navy (PLAN); and over 2,000 combat aircraft in the PLA Air Force (PLAAF).[1] The PLA's Second Artillery branch (which became the PLA Rocket Forces on December 31, 2015) controls a stock of nuclear weapons capable of reaching the United States and Russia, as well as several thousand medium- and intermediate-range ballistic missiles.

Despite the popular image of a military that emphasizes quantity over quality, the PLA has been steadily sharpening its focus on qualitative improvements to complement its quantitative advantages. PLAAF pilots fly Su-27/30/33 fighter aircraft (and their Chinese-produced variants), comparable to late-model US F-15s and Eurofighter Typhoons. PLAN sailors go to sea aboard destroyers and frigates that incorporate stealth designs and advanced air defenses, while some PLAN pilots are now operating from the *Liaoning*, the first aircraft carrier to fly a Chinese flag.

As important, China has been steadily expanding its ability to operate in the realm of information space, including the electromagnetic spectrum, cyberspace, and outer space. Here, the Chinese military has no disadvantage, since it is no more inexperienced in high-intensity information warfare than other nations. Although the PRC has not fought a war since its 1979 conflict with Vietnam, no *other* nation has fought a war since then involving counterspace operations or intense integrated electronic and computer network warfare.

At the same time, China has been steadily developing a doctrine for its new conventional forces, in conjunction with its expanding portfolio of space

and information weaponry. While the PLA ground forces remain prominent, the Chinese military has steadily shifted its doctrine toward emphasizing joint operations. This is an important element that distinguishes the Chinese from many other adversaries that have confronted the United States over the past three decades—China's military has devoted substantial intellectual capital to thinking about future warfare and how best to wage it. The PLA is not simply interested in acquiring new equipment. Instead, it is striving to figure out how to best exploit all the equipment that it has on hand, whether old or new, by developing a suitable set of doctrine and attendant tactics, techniques, and procedures to implement that doctrine.

A BRIEF HISTORY OF THE PLA

Today's increasingly sophisticated and modern PLA is emblematic of the larger evolution of the People's Republic of China (PRC). At the time of its founding in 1949, the PRC was one of the poorest nations on earth. Its population was largely illiterate; its industrial base was weak. China did not produce its own aircraft, tanks, or even automobiles. Worse, it had just endured not only a four-year civil war, but an eight-year war with Japan (known in China as "the War of Resistance"). This had seen large swaths of the nation devastated—including key urban centers containing China's limited industrial base.

The one thing China had in abundance was people. Mao Zedong, China's leader at the time of its founding, had exploited that resource in his battles with the Kuomintang and Chiang Kai-shek (Jiang Jieshi). When China intervened in the Korean War against the American-led UN forces in 1950, Mao and other senior Chinese leaders employed the same numerical advantage. Surprising General MacArthur's UN forces as they approached the Yalu, Chinese infantry divisions drove them south of the 38th Parallel to the positions that now constitute the inter-Korean border.

This reliance on masses of indifferently trained and equipped troops remained the basis for PLA thinking throughout the Mao era. Mao fashioned the concept and doctrine of "People's War" around an emphasis on quantity over quality. He pitted China's numbers against qualitatively superior enemies, whether the forces of Imperial Japan, the Soviet Union, or the United States. The Chinese military under Mao further capitalized upon this advantage by relying on "protracted war," waging a prolonged guerrilla war against any adversary who might invade China. Mao also firmly held that superior numbers of people, even with inferior equipment, could win—provided that they were suitably ideologically motivated. This led to the slighting of military professionalization. Superior political training and indoctrination would sustain this large force in any conflict, as it had in the decade of the Chinese Civil War and the war with Japan.

It was this sort of an army, largely infantry with minimal support equipment, heavily politicized but decreasingly trained in the specialties of war, that not only fought in Korea but also engaged the Indians in the Sino-Indian War of 1962, and the Soviet military in the Sino-Soviet border clashes of 1969.

Consequently, through the 1970s, the PLA was largely comprised of light infantry formations, with very limited motorization and mechanization, supplemented by a handful of armored divisions. At sea, the Chinese navy was largely a coastal defense force. It could not venture far beyond its shores with its few destroyers and frigates, while relying on hundreds of torpedo and missile-armed fast-attack craft (modern versions of PT boats) to harry any seaborne adversary. In the air, the PLAAF was numerically significant but largely equipped with 1950s' and 1960s' vintage aircraft.

The Rise of Deng Xiaoping and the Decline of "People's War"

This was the army that fought the Sino-Vietnam War of 1979. During the month-long invasion, PLA casualties were comparable to those the United States suffered in eight years. In one example, an entire Chinese army, comprising three divisions, took nearly a week to breach a line held by a single regiment of Vietnamese.[2] The PLA's performance was abysmal, with poor artillery–infantry coordination, primitive communications, and sporadic logistical support.

This war, launched after Deng Xiaoping had secured power after Mao Zedong's passing, led to a major evolution in how the Chinese thought about both warfighting and the broader strategic environment. The PLA's experience in Vietnam, coupled with observations of the American military in the Vietnam War, the 1967 and 1973 Arab–Israeli wars, and the Falklands War soon after, persuaded the Chinese military that its approach to war was no longer appropriate.

The rise of Deng Xiaoping also allowed for a fundamental reassessment of the strategic context. As noted earlier, Mao's view of military preparations was extremely ideologically driven, with little confidence in military professionalization (which also opened the door to "Bonapartism," i.e., a military challenge to party authority). Mao also believed that major, global, nuclear war was imminent (in part because of the likelihood of a massive confrontation between the socialist and capitalist camps). China, in his view, would probably have to fight a protracted war against not only the United States but the Soviet Union. Therefore, absolute priority was accorded to not only creating a military that could fight a protracted guerrilla war but establishing military industries that could sustain it. As a result, many factories were scattered inefficiently (but it was thought survivably) throughout the Chinese hinterlands, to sustain the extended guerilla war that Mao expected in the wake of the thermonuclear holocaust between the superpowers.

Deng, by contrast, stated that "peace and development are the two outstanding issues in the world today."[3] While there remained the possibility of war on China's periphery (which the Chinese characterize as "local wars"), the prospect of a massive global war in the foreseeable future was now considered low. This strategic reassessment fundamentally altered not only the PLA's planning requirements but also available resources. Where Mao had kept the nation on a virtual war footing, Deng shifted the economy toward light industry, consumer goods, and joining the global economy. For Deng, the priority was to rebuild China's economy, which had been effectively bankrupted by Mao's policies.

The new strategic situation led to a reassessment of the likely nature of future wars. Rather than preparing for imminent, major, nuclear wars, the PLA would focus on "local wars under modern conditions." These would be more limited conflicts on China's periphery; the model would be the Sino-Vietnam War of 1979 or the earlier Sino-Indian War of 1962. Such wars would be fought with limited means (e.g., no nuclear weapons) and for limited ends (e.g., territorial adjustments, political signaling). Regime survival would not be directly threatened.

Deng also believed that the PLA could no longer rely solely or even primarily on masses of militia, luring the enemy deep into China and waging protracted guerrilla wars. There was little prospect of foreign forces invading and occupying China, making themselves vulnerable to Mao's vision of a protracted guerilla war.

Instead, the more limited nature of "local wars under modern conditions" required meeting and defeating adversaries on the frontier. This shift would increase reliance upon mechanized formations and require more modern equipment. It would also entail a more professional approach to warfare. Rather than militiamen equipped with little more than "rifles and millet," the PLA would have needed troops with more specialized skills and capabilities (e.g., greater ability to coordinate operations involving not only infantry but tanks, artillery, airpower, logistical support, etc.).

In 1985, the PLA began to field its first "group armies," reflecting an effort to develop more combined arms operations. It also accorded greater priority to improving logistical support and to incorporating more technical equipment such as radios and other command-and-control equipment. At the same time, the PLA was directed to reopen institutions of professional military education (PME), which had been shut down during the Great Proletarian Cultural Revolution (1966–1976). Among its various functions was to provide the common foundational knowledge about different branches and equipment, as well as the specialized training associated with staff work, operational planning, and command and control. The PLA would remain a party army, firmly under Chinese Communist Party (CCP) control, but it would be more professional in training and education.

It would have to do so, however, with drastically fewer resources. Perhaps most dramatically, Deng radically cut the size of the PLA. In 1985, nearly a million troops were demobilized. Two subsequent reductions, in 1997 and 2003, saw the PLA ultimately pared from nearly 4.5 million in 1980 to some 2.2 million by 2006.[4]

This was part of Deng's larger reversal of Mao's priorities between war preparations and military preparations. In Deng Xiaoping's Four Modernizations, the military was last, after agriculture, industry, and science and technology. The PLA's official budgetary allocation was slashed by at least 25 percent, with the resultant savings redirected to the broader national economy.[5]

To make this shift more palatable, the PLA was encouraged to enter the world of commerce. This took two forms. First, the CCP allowed those industries that were already operating under the PLA's control to convert to production of commercial items for the consumer and export markets. As important, military formations were encouraged to supplement their incomes by opening businesses and were allowed to use their organic assets (e.g., trucks, troops) as part of those businesses.[6] By the late 1980s, the PLA was running a host of hotels, restaurants, farms, and nightclubs to supplement its official budget.

This set of moves proved to be a double-edged sword. On the one hand, as more of the Chinese military focused on running profitable businesses, military preparedness dropped. Similarly, military-run factories focused on commercial sales rather than military production.

While these moves eroded combat readiness, they also introduced PLA officers to a different way of running things. As officers sought to tailor their businesses to local demands, they operated under imperatives that were neither especially Communist nor necessarily rigid. As important, running businesses in the early 1980s exposed officers to various information and sensor technologies that were just beginning to affect both civilian and military capabilities.

Jiang Zemin and the Two Transformations

In 1989, the CCP faced a major challenge to its authority. Protests in Tiananmen Square, which began after the death of CCP General Secretary Hu Yaobang, persisted and grew. As protests escalated, Hu's successor Zhao Ziyang was seen as having lost control. Deng replaced Zhao with Jiang Zemin, then the party secretary for Shanghai, who became both leader of the CCP and official leader of the PRC.

With Jiang's rise, Deng Xiaoping assumed a somewhat lower profile in the Chinese leadership, although he was always able to exert influence until his death in 1997. (Indeed, in 1992 Deng went on his famous "southern tour" to reignite support for continued economic reform.) Nonetheless, especially in terms of overall strategic policy, Jiang initially continued

to adhere to his patron's overall strategic assessment—the world remained in a condition of "peace and development." Therefore, China's military modernization efforts should not displace the broader goal of national economic development.

During this period, however, the PRC was confronted by a series of major, systemic shocks in the strategic environment. The first was the consequence of the Tiananmen Square massacre. While China and the West, including the United States, were strategic partners against the Soviet Union for much of the 1980s, the Tiananmen massacre of June 4, 1989, brought that level of close interaction to a close. The West imposed a series of sanctions that remain in place as of 2016, limiting Chinese access to advanced military technology and imposing restrictions on certain dual-use technologies.

The shift in Chinese interaction with the West precipitated by the Tiananmen massacre overlapped with the collapse of the Soviet Union. At a stroke, the single greatest threat to the PRC and the West, the strategic motivation for Sino-Western cooperation, evaporated. The rise of Mikhail Gorbachev and the dissolution of the USSR made China far more secure, especially as Gorbachev also signed a number of agreements with Deng Xiaoping codifying the Sino-Soviet borders. The successor states to the USSR were in no real position to challenge Beijing, who promptly moved to ensure that post-Soviet Russia and the various central Asian republics would all abide by the extant borders.[7]

That same collapse, and subsequent economic implosion, also devastated the Russian military. Russia's naval and air forces atrophied, and the army shrank significantly; only the Russian nuclear forces remained fairly intact. The Soviet military industrial complex fragmented, as newly independent republics controlled different pieces of what had been an integrated whole. The Russian ability to threaten China rapidly receded.

Unfortunately, the collapse of the USSR also removed the strategic impetus behind Western cooperation with China. With the end of the Warsaw Pact, there was no longer a need to tie down as many Soviet troops as possible. The West could choose to impose sanctions on China after Tiananmen in part because the end of the Soviet Union made China less important as a strategic military partner.

Ironically, although the dissolution of the USSR was strategically advantageous, it also constituted a profound threat to the legitimacy of the CCP. Indeed, the student protestors at Tiananmen had been motivated by the visit of Gorbachev, who had already initiated the policies of "perestroika" and "glasnost." The end of the Soviet Communist Party constituted a cautionary tale for the CCP.

Not only had the external security environment changed during this period, but so had China's internal situation. Even by 1992, while China remained an underdeveloped country, it was *less* underdeveloped than it had

been. Deng Xiaoping's reforms were already bearing fruit, as China's economy steadily expanded and its infrastructure improved. Ironically, this meant that China now had more to lose—where it could once afford to cede the urban centers and fall back on the hinterlands to wage protracted guerrilla wars, the PRC's economic growth meant that such a strategy would relinquish significant economic, financial, industrial, and human resources.

For the PLA, the changes in the overall strategic environment were matched by a significant change in how wars were fought, as evidenced by the Gulf War. Despite being the lowest priority in Chinese modernization, the PLA of 1990 was better than it had been a decade earlier. Weapons dating back to World War II and the Korean War (including T-34 tanks and MiG-15 fighters) had been retired, some of them replaced by equipment incorporating more advanced systems (e.g., some of China's J-8II fighters had Western radars, as part of the U.S.–China "Peace Pearl" program).

Any confidence in how the PLA would fare in modern wars, however, was dissipated by the course and speed of the first Gulf War. As one Chinese officer observed, "While lasting only 42 days, it [Operation Desert Storm] had a great effect on the PLA."[8] The extended air campaign and the subsequent 100-hour ground campaign indicated that China's military improvements since 1979 had been almost totally eclipsed.

As important, the conflict "compelled many Chinese strategists to realize the way of war-fighting was experiencing a fundamental transformation."[9] One instructor at China's National Defense University observed that the "characteristics of a joint operation of all branches of the military displayed in that war gave us a glimpse of things to come in the early 21st century."[10] Another PLA analyst wrote that "the form of joint operations appearing in it [the Gulf War], of coordination among all service arms, will undoubtedly be a key trend of future war developments."[11] This was echoed by the then-deputy director of the PLA's Academy of Military Science (AMS), the top Chinese military think tank:

> The Gulf War marked a big step forward in both military theory and practice. For instance, strategy and the battles were closely interwoven, with the latter playing a major role, sometimes overlapping with strategy and tactics.[12]

For the PLA, there was broad recognition that this new approach to war would require a thorough revamping of its approach to warfighting. A variety of contemporary reports indicated that "Chinese military leaders now publicly estimate the military-technical gap with the West at twenty to thirty years."[13] Nor could this technological gap be offset by the Mao-era solutions of relying on ideological motivation or sheer mass of forces.

The first Gulf War suggested that future wars would still be "local wars," with no use of nuclear weapons and relatively limited duration. Indeed, these conflicts could be so violent that they might last for only a single campaign and be concluded in a matter of weeks or months. However, there would be no time either for the mass mobilization of industry or for protracted guerrilla warfare to have an impact. The political results of the war would, however, be decisive, involving the destruction of entire armies and collapse of regimes.

The advances in technology had also changed how these wars would be fought. The Chinese concluded that future wars would be characterized by the "three nons": noncontact, nonlinear, and nonsymmetric.

Noncontact (*fei jierong*; 非接融). The advent of long-range, precision-strike capabilities allows forces to engage adversaries well beyond visual range. Extended-range artillery and rockets, stand-off air-to-ground munitions, and long-range bombers carrying cruise missiles bring massive destructive power to bear. Coupled with the precision granted by space-based navigation systems such as the U.S. global positioning system (GPS) satellites, such noncontact warfare was as effective as or more effective than traditional engagements at close range. The defenders may not be aware that they are under attack until too late. Noncontact warfare ultimately focuses on the massing of effects, rather than troops or assets, through the coordination of joint forces, including land, sea, air, outer space, and information power.[14] Information is the key enabling element. Without prompt access to accurate information, the precision operations necessary for noncontact warfare are not possible.

Nonlinear (*fei xianshi*; 非线式). Modern warfare increasingly involves operations where the two sides are often interpenetrated; there is no longer a clear forward edge of the battle area. This is in part because the density of forces on the battlefield has dropped precipitously; large concentrations of forces are simply large targets for the precision munitions of noncontact warfare. Moreover, the long reach of weapons also means that there is no longer a distinct front line or rear area. Finally, the importance of information means that the main battlefield in future wars will be in information space, with physical space only one component. Integrated, joint operations across the land, sea, air, outer space, and information space domains, especially the latter two, negate many of the traditional concepts of battle lines.[15]

Nonsymmetric (*fei duicheng*; 非对称). While many Western analysts consider the PLA to be masters of asymmetric warfare, the Chinese see the West, and especially the United States, as having repeatedly demonstrated asymmetric operations. The use of airpower to counter land power has been a hallmark of Western operations since at least World War II, such as strategic bombing campaigns and the substitution of close air support for ground-based artillery. The Balkan conflict, with its reliance on airpower, embodies the Chinese view of Western asymmetric warfare.[16] The ability to engage an adversary's entire

strategic depth, denying it any sanctuary (even deep in its homeland), and to do so from long distance with extended-range, precision munitions is the epitome of nonsymmetric warfare.

Confronted with this radically altered strategic landscape, the PLA would require not only substantial investments in modernizing its military equipment but also a fundamental overhaul of its doctrine, that is, how it thought about *using* its new equipment. In this context, Jiang Zemin charged the PLA with undertaking the "two transformations":

- The PLA should shift from a military preparing to fight "local wars under modern conditions" to one preparing to fight "local wars under modern, high-technology conditions".
- The PLA should shift from being a military based on quantity to one based on quality.[17]

In order to be able to handle the new types of conflicts that the Gulf War presaged, Jiang demanded that the PLA shift itself bureaucratically and programmatically (toward a greater emphasis on quality), but also in its approach to warfighting. In particular, it would have to be able to meet the demands of "local wars under modern, high-technology conditions." Such wars are marked by several characteristics that are fundamentally different from those of "local wars under modern conditions":

- The quality, as well as the quantity, of weapons matters. The side with more technologically sophisticated weapons would be able to determine the parameters of the conflict and effectively control its scale and extent.
- The battlefields are three-dimensional and extend farther and deeper into the strategic rear areas of the conflicting sides.
- The conflict is marked by high operational tempos conducted around the clock, under all-weather conditions.
- The fundamental approach would emphasize joint operations.
- Finally, the role of command, control, communications, and intelligence (C3I) is paramount. C3I functions are essential to successful implementation of such wars; therefore, the ability to interfere with an opponent's C3I functions also is more important.[18]

From the PLA's perspective, the centerpiece of such future wars was the ability to conduct joint operations.

PURSUING AND PROMOTING JOINT OPERATIONS

While the PLA had explored jointness in the 1980s as military theory, the rapid American victory in the Gulf War forced it to adapt and adopt joint

operations into its operational repertoire. Joint operations therefore became a major focus of the Eighth (1991–1995) and Ninth (1996–2000) Five-Year Plans. As Chinese Five-Year Plans are a key organizing and funding mechanism for the PLA and the PRC in general, the incorporation of jointness reflected the seriousness of this effort. With its inclusion into Five-Year Plans, joint operations clearly had become a matter of national interest, rather than a purely internal PLA affair.

During the Eighth Five-Year Plan, the PLA engaged in significant debate over how to think about joint operations. In particular, there was extensive discussion about whether there was a qualitative difference between joint operations (i.e., operations involving multiple services) and combined arms operations (i.e., operations involving multiple branches within the same service).

PLA analyses ultimately concluded that joint operations were not simply a form of combined arms operations but a separate type of activity requiring its own distinct doctrine. Developing such a doctrine, however, posed a significant challenge to the PLA. As a military grounded in Marxist–Leninist principles, the PLA viewed war as a science, with underlying operational principles (*zhanyi yuanze*; 战役原则) and guiding concepts (*zhidao sixiang*; 指导思想) that can be scientifically derived. Determining these principles and concepts is essential for understanding the "correct" approach (i.e., the scientific one) to wartime problems.

Deriving these overarching concepts requires historical foundations for validation and testing purposes. The PLA, like most militaries, generally tries to define its operational concepts in terms of its own historical experiences.

JOINT OPERATIONS AND COMBINED ARMS OPERATIONS

Most militaries are comprised of "services," forces that largely operate in a specific domain (e.g., land, sea, air). Typically, services have individual budgets and bureaucracies. Most militaries' services include the navy, the air force, and the ground forces (usually also referred to as the army). In the United States, the services also include the U.S. Marine Corps and U.S. Coast Guard. The Soviet Union also had additional services, in the form of the Air Defense Forces and the Strategic Rocket Forces. In the Chinese military, until 2016, the services were the ground forces (implicitly), the navy, and the air force.

Services, in turn, are usually comprised of "branches." Branches are subdivisions of services, often involving specific technical knowledge. Within the U.S. ground forces (U.S. Army), for example, are branches such as infantry, armor, artillery, and Army aviation. Within the Chinese air force, there are branches for aviation, surface-to-air missile (SAM), antiaircraft artillery, radar, and airborne/paratroops. Until 2016, the Second Artillery, responsible for Chinese nuclear forces, was a branch, rather than a service.

"Joint operations" are those that involve two or more services. "Combined arms operations" are those that involve two or more branches.

None of China's military experiences during the Chinese Civil War, World War II, the Korean War, or the various conflicts with India, the USSR and Vietnam had been joint, however.[19] The PLAN and PLAAF had almost never had to operate in conjunction with the PLA ground forces. Given the absence of Chinese experience in joint operations, the PLA was therefore compelled to look abroad for models and examples and to develop its own joint theory based on vicarious observation and study.

Previously, the PLA had generally drawn from Soviet experience, which probably had the greatest aggregate influence on the PLA's thinking. In the course of this doctrinal shift from combined arms to joint operations, however, the PLA found little to use in the Soviet experience. As one Chinese volume notes, the Soviet military viewed interservice cooperation as simply an expanded version of combined arms operations. Indeed, according to the Chinese, the Soviets did not even use the term "joint" operations; they characterized such interaction as "inter-service combined arms operations."[20] Chinese analysts concluded that the Russian military was excessively wedded to the concepts of "combined arms" *within* a service and had not explored the scientific laws behind joint operations *between* services. Consequently, in the Chinese view, the Russians had mistakenly categorized joint operations as a subset of combined arms operations.[21] The Chinese would have to find someone else to serve as a role model.

If Soviet approaches were mistaken, Western ones had demonstrably succeeded. This conclusion was partly based on the British experience in the Falklands War. From the PLA's perspective, this was an exemplary model of what joint operations could achieve. An outnumbered British force, operating from a very extended logistics chain, nonetheless was able to defeat an emplaced, numerically superior foe through forced entry operations. Moreover, the two sides had relatively similar levels of equipment, so victory could not solely be attributed to British superiority in matériel.

Instead, as several Chinese assessments noted, the key difference was the British ability to undertake coordinated joint combat activities. The Argentine forces were not organized to be mutually supporting, either tactically or in terms of their capabilities. One PLA analysis noted that the Argentine forces "showed superb combat technology and a valiant and tenacious combat style." However, the Argentine air force "never received the coordinated support of the other service arms. . . . The three Argentine service arms were not coordinated, rather each acting on its own."[22] The Argentine ground and air forces failed to shield each other's weaknesses or reinforce each other's strengths. By contrast, the British military was much more closely coordinated.[23] This allowed the British forces to triumph, despite attacking a larger opponent. To Chinese analysts, joint operations seemed to confirm "the ability of the inferior to defeat the superior," a long-standing tenet of Maoist military doctrine.

Even more important in shaping the Chinese assessment of joint warfare were the American military's reform efforts, which were proceeding contemporaneous to the British Falklands experience. The success of the American-led coalition in the Gulf War was even more resounding than the British Falklands experience. The Chinese appear to have extensively studied the entire course of American doctrinal development throughout the 1980s, which had laid the groundwork for the success in the Kuwaiti and Iraqi desert. Indeed, Chinese authors credit the United States with pioneering the rigorous study of joint campaigns and suggest that "AirLand Battle" was one of the most important intellectual components in the evolution of the subject.[24]

The end of the Eighth Five-Year Plan (1991–1995) saw the PLA's military academic community moving steadily toward an emphasis on joint, rather than combined arms, operations. The PLA appeared to accept that any large-scale combat operations in future wars would have at least air and land forces operating in a coordinated fashion.[25] In the Ninth Five-Year Plan, the PLA proceeded to convert academic theory into formal doctrine, through a multi-pronged approach.

One essential element was the emphasis placed upon studying joint operations within Chinese PME. This extended careful scrutiny beyond the Gulf War, to subsequent conflicts such as the Western intervention into the Balkans in the late 1990s. As one Chinese analysis concluded:

> The 1999 Kosovo War, with the US-led NATO forces engaging the Yugoslavs in fully integrated land, sea, air, space, and electronic environments full, was precisely what "full-spectrum warfare" theory suggested, implementing an example of a joint campaign under high-technology conditions.[26]

Meanwhile, field exercises began to incorporate joint concepts and operations under high-technology conditions.

> In particular, in March 1996, our land forces, naval forces, air forces, and Second Artillery in the Taiwan Straits successfully implemented a large-scale joint campaign exercise under high-tech conditions, exploring many new joint campaign experiences appropriate to our military's unique aspects, and had great impetus in developing our military's development of joint campaigns under high-tech conditions.[27]

Not only was the PLA intending to teach jointness to its forces, but it was now beginning the process of refining the theory in order to implement it.

It was also during this period that Jiang Zemin dissolved the military–business complex. In a speech in July 1998, he ordered the PLA to divorce itself

from most major businesses by 2000. While this was the public face of the effort to move the PLA out of running commercial businesses, there is evidence that divestiture had been under way for months, if not years, in part to fight rising corruption.[28] But there was one industrial sector that was exempt from the divestiture order—telecommunications. As James Mulvenon observed in 2001, the military was allowed to remain involved in telecommunications because the "information technology acquisition was seen as an essential contributor to the C4I [command, control, communications, computers, and intelligence] revolution currently underway within the PLA."[29]

All these efforts culminated in 1999, when the PLA officially issued its guidance on joint operations, as part of the "New Generation Operations Regulations" (*xinyidai zuozhan tiaoling*; 新一代作战条令). These seem to comprise two parts. The first was the "Ordinance of Joint Campaigns of the Chinese People's Liberation Army" (*zhongguo renmin jiefangjun lianhe zhanyi gangyao*; 中国人民解放军联合战役纲要). This "ordinance" (*gangyao*; 纲要) provided overall guidance about the importance and method of undertaking joint operations. In addition, there were the "Joint Campaign Regulations" (*lianhe zuozhan tiaoling*; 联合作战条令). These regulations likely provided not only more specific guidance on the conduct of joint campaigns but also for training, logistics and maintenance support, and various other aspects of "high-tech" combat, such as air defense.

The end of the Ninth Five-Year Plan in the year 2000 therefore saw the PLA explicitly preparing a common foundation for operational thinking by the entire PLA. It had cleared the way for forces to focus more on preparing to fight, rather than be distracted by operating businesses. As important, it had developed a doctrine for joint operations and had promulgated that doctrine, through the two sets of documents.

PLA Concepts of Coordinated Joint Operations

A central part of this foundation was the Chinese vision for joint operations. Indeed, all the individual service regulations, as well as those governing logistics and support functions, were subordinated to those governing joint campaigns.[30] Joint operations were seen as informing and shaping service-led, combined arms operations. This elevation of joint operations reflected the Chinese military's view that joint operations would be more important, more decisive, than combined arms operations.

For the PLA, the main focus for joint operations at this point was to create synergies among participating forces, based on their capabilities in different domains (mainly land, sea, and air at this point). Properly implemented, the commander could orchestrate a symphony of effects, exploiting the advantages

that participating forces brought to the campaign. Chinese writings at this stage often referred to "coordinated" joint operations (*xietong lianhe zuozhan*; 协同联合作战), referencing the importance of this orchestration.

At this stage, however, joint operations were still seen as occurring at high levels of aggregation. Jointness was envisioned primarily at the campaign level of war. That is, at this point there was no concept of joint "battles", only joint "campaigns". Indeed, in the PLA taxonomy, joint campaigns were actually comprised of linked, service-centered, combined arms campaigns. Jointness resulted from the creation of a suitable command architecture and campaign plan, rather than arising from joint tactical activities.

PLA writers believed that the building blocks for joint operations would be fairly substantial entities, *juntuan* (军团) or "military groups," drawn from each service, operating at the campaign level of war. For the PLA's ground forces, for example, the basic *juntuan*-level force at the time was the group army (*jituanjun*; 集团军), roughly comparable to a U.S. Army corps. The group army was comprised of component divisions and brigades, which were thought of as tactical, rather than campaign-level units.

For the PLAN, *juntuan*-level units were the three fleets (*jiandui*; 舰队): the North Sea Fleet, the East Sea Fleet, and the South Sea Fleet. Each contained surface, submarine, and support flotillas, as well as fast missile attack

LEVELS OF WARFARE

When analyzing warfare and conflict, there are broadly three levels of conception and planning.

Wars occur at the "strategic" level of warfare and involve the entire nation. For the PLA, the past several decades have seen a shift in emphasis from total war, which would involve nuclear weapons and be global in nature, to local war, which would be more limited in both scope (e.g., no use of nuclear weapons) and physical extent (e.g., limited to one nation such as Iraq or one region such as the Balkans). Local wars can still be decisive in their impact—the 1990s' Balkan wars saw the Serbian government's collapse and Slobodan Milosevic's arrest, while the Iraq War led to the toppling of Saddam Hussein.

Campaigns occur at the "operational" level of war. Campaigns involve ground forces at corps and army level (multiple divisions), air forces (multiple wings), and fleets (dozens or more naval combatants). Campaigns bridge the gap between battles and wars. Wars involve multiple campaigns.

Battles occur at the "tactical" level of war. Battles involve ground forces from squads (tens) to brigades (thousands of troops), squadrons of aircraft (dozens of aircraft), and squadrons or flotillas of ships. Campaigns are typically comprised of multiple battles.

craft and naval aviation assets. In the event of war, the participating fleet or fleets would reorganize its forces into "navy task forces" (*haijun biandui*; 海军编队) as their *juntuan*-level units, tailored to the scale and objectives of the campaign. While it would be centered on either destroyers or frigates, a task force would probably also contain elements of all the other available platforms (i.e., fast-attack craft, submarines).

The PLAAF's *juntuan*-level units were the seven military region air forces (MRAFs) (*junqu kongjun*; 军区空军), one per military region. Each MRAF was comprised of several air divisions, including fighter divisions, bomber divisions, and other specialized divisions. The MRAF would be the lowest campaign-level unit; the component air divisions, as with the ground forces' divisions, were considered tactical elements.

Finally, for the Second Artillery Corps, the basic *juntuan*-level unit was the conventional missile force base (*changgui daodan budui jidi*; 常规导弹部队基地) and its associated missile launch units. There are currently six such bases; each is considered the equivalent to a group army in scale.[31] Conventional missile force bases are comprised of brigades, which are considered the equivalent of division-level units of the ground forces, that is, tactical forces.[32]

In this initial reconception of future warfare, the PLA defined campaigns as joint if it involved at least *juntuan*-level forces from two or more services.[33] Combinations of smaller forces would not rise constitute jointness. Thus, although the PLA was moving away from quantity toward quality and was interested in conducting joint operations, those joint operations would still involve large numbers of troops, whose activities would be focused on service-oriented activities, insulated from each other at the tactical level. The desired synergies would occur at the campaign, not tactical, level of war.

Indeed, despite the emphasis on preparing to conduct joint operations, the PLA at this point seems to have viewed them more as a special type of campaign, rather than the norm, in future "local wars under high-technology conditions" (their characterization of the nature of future wars). Joint operations were more powerful than service-centered operations and would be pursued wherever possible. But service-centered campaigns were still considered to be the building blocks for those joint operations.

Nonetheless, jointness was recognized as more than simply the physical colocation of various large forces from two or more services. As PLA writings at this point emphasized, to have a joint campaign required a *single, unified command structure*. Generally termed a "joint campaign command structure" (*lianhe zhanyi zhihui jigou;* 联合战役指挥机构), it is drawn from the staffs of the participating services and, depending on the size or level of the campaign, may be augmented by personnel from the Central Military Commission (CMC), general departments of the PLA, and senior political leaders. This joint campaign command structure is superior to the individual service

command structures of the participating *juntuan*. In effect, it sits atop the service command structures, coordinating their activities.

This joint campaign command structure develops a *single, unified plan* for the joint campaign. The plan coordinates participating forces' activities, guiding the overall joint campaign. The plan schedules participating forces' operations, deconflicts logistical and support requirements, provides detailed planning of subsidiary (combined arms) campaigns, and provides individual service campaign staffs with an understanding of their respective roles, missions, and objectives. The plan will provide participating forces with coordination methods, based on the phase of the campaign, task involved (e.g., fire support, assault, exploitation), or location, to maximize synergies.

The single, unified command structure formulated the single, unified plan in order to ensure that participating forces coordinate their activities across time and battlespace. The goal was to confront an adversary with forces operating in different battlespaces with different attributes and different operational patterns. This would divert and divide the enemy's attention and response, while coordinating one's own forces, especially in terms of timing.

The ability to strike an adversary simultaneously or sequentially was, at this point, considered a hallmark of joint operations.

> In future joint campaigns, we must emphasize the need to have all the services engage in combat activities at the same time. Based on combat requirements, we must fully develop the various services' combat capabilities in order to be able to strike at simultaneous or near-simultaneous times, across the depth of the theater.[34]

Modern high technology allowed coordinated strikes across the breadth and depth of a theater, at a variety of targets, at the same time. Long-range missiles, long-range strike aircraft, extended-range artillery, all could be coordinated to achieve time-on-target (i.e., near-simultaneous) barrages.

Growing Awareness of the Importance of Information

The ability to effect such precise timing, however, would be dependent not only upon accurate, long-range weapons, and the ability to establish air and naval dominance but upon secure communications to issue orders and decisions. Even at this early stage, the PLA was recognizing that the successful conduct of information combat was an essential part of joint operations. Consequently, there was an increasing "focus of contention for information superiority with each passing day."[35] To this end, the unified headquarters for joint operations included an information warfare cell.

The Chinese concept of information dominance, moreover, was rapidly evolving in this same time frame. In the 1980s, the focus had been more on electronic warfare and "electronic (or electromagnetic) dominance" (*zhi dianzi quan*; 制电子权). Electronic warfare remained a priority for joint operations. As one PLA analysis observed:

> It is necessary to make electronic offensive the centerpiece [of information warfare], with other information strengths complementing, striking at key points of the enemy's battlefield information systems [including] their command and control centers, information nodes, radar stations, computer network nodes, etc. [36]

By the time the New Regulations were promulgated, however, interest in information dominance had expanded to include "computer network dominance" (*zhi wangluo quan*; 制网络权). The two were increasingly discussed together, under the term "information dominance" (*zhi xinxi quan*; 制信息权).[37]

This was the ability to accurately collect, transmit, and apply information, while denying an adversary the ability to do the same. Electronic warfare and computer network warfare were also discussed in conjunction with military deception, psychological warfare, and physical attacks against adversary information systems (e.g., their electronic sensors; command, control, and communications networks), as elements of information combat.[38]

Such combat would be especially important in joint operations.

> The joint campaign *juntuan* plan, in future conflicts, to actually realize multi-service jointness and high degrees of integrated, unified combat, must plan to engage in all-out combat against the enemy's information control capabilities, while at the same time making all-out efforts to preserve their own information control capabilities.[39]

The PLA's first steps toward joint operations therefore included efforts not only to integrate different services but also to incorporate information combat.

Focusing High-Technology Concerns on Information Technology

The promulgation of the New Regulations in 1999 did not mark the end of the PLA's interest in jointness, nor efforts to further develop joint operations capability. As the PLA began to develop its doctrine and train to it, Chinese military leaders recognized that this was only the beginning. The participating forces were still at extremely high levels of aggregation. If the PLA wanted to create the synergies it described, it would have to move beyond different services coordinating at the *juntuan* level.

Synchronizing effects could not be achieved simply through preplanning, where land, sea, and air forces appeared, like swimmers in an Esther Williams water ballet, according to a rigid schedule. Instead, true jointness would require more flexible operations, responding to enemy actions and exploiting developments on the battlefield. Much more extensive communications among the disparate forces were required. Because of the extended range of modern weapons and long-range strike assets, and the logistical support for all these forces (in order to sustain operations), the volume of operational space was enormous. The span of command, control, and communications activities would now have to reach across thousands of cubic miles. Moreover, voice communications alone would no longer suffice—modern warfare requires creating a common situational picture. This means sharing data among various platforms and units, not just among the commanders, and certainly not only among *juntuan*-level commanders.

As the PLA increasingly incorporated jointness into its training and exercises, it is likely that this need for a common situational picture became more prominent. PLA analysts meanwhile spent significant time examining NATO operations in the Balkans, as well as the U.S. war in Afghanistan, and the coalition war against Iraq in 2003. The PLA apparently concluded over the course of the 1990s and early 2000s that, while raising the overall technological sophistication of the PLA was important, the most essential systems would be information related—sensors, communications, computers.

This shift is prominently reflected in evolving PLA descriptions of the nature of future wars. The 1990s formulation of preparing for "local wars under modern, high-technology conditions" was replaced with concern over "local wars under informationized conditions." This change was incorporated in the 2004 Chinese white paper on national defense, but was being discussed in 1999 PLA professional military literature, and was "officially incorporated into the lexicon of the 'Military Strategic Guidelines for the New Period'" in 2002.[40]

New Historic Missions and the Importance of the Cyber Domain

Hu Jintao, who had been selected by Deng Xiaoping to succeed Jiang Zemin, further emphasized in December 2004 the importance of information dominance as a fundamental PLA responsibility. In a speech to the CMC, Hu, as its chairman, outlined the "historic missions of the PLA in the new phase of the new century" (*xinshiji xinjieduan wojun lishi shiming*; 新世纪新阶段我军历史使命). These "new historic missions" essentially are the main tasks charged to the PLA. These comprise:

- Guaranteeing the continuing rule of the CCP
- Safeguarding national economic development, through defense of sovereignty, territorial integrity, and domestic security

- Safeguarding China's expanding national interests, specifically within the realms of outer space, electromagnetic spectrum, and the maritime domain
- Helping ensure world peace[41]

Some of these "new historic missions" are of long standing. The PLA is a party army, the armed wing of the PLA. Therefore, sustaining the party's continued rule has always been a foremost task. Similarly, the PLA has long known that a fundamental responsibility was ensuring Chinese sovereignty and territorial integrity, that is, being prepared to retake Taiwan and enforcing Chinese rule over Xinjiang and Tibet in the face of separatist sentiments.

The task of safeguarding Chinese expanding interests, however, constituted a major revision of the PLA's responsibilities. As Hu noted, the PLA was now charged with preserving Chinese national interests beyond its traditional borders. In light of national development requirements and broader global trends, Hu observed that China's national interests and security were no longer limited to the traditional land, sea, and air. "Maritime security, space security, electromagnetic spectrum security," he noted, "are already vital regions for national security," where a number of major powers are seeking to secure advantage. In essence, Hu was expanding China's defined interests beyond its traditional borders, to the electromagnetic domain, the reaches of outer space, and the world's sea lanes.[42] In doing so, he was clearly elevating the information realm, of which the electromagnetic spectrum is an essential part and outer space is an integral part of its physical infrastructure.

For the PLA, Hu's instructions were a call to arms, to prepare for informationized warfare.

3 Chapter

Informationized Conflict: Maintaining Party Control amid the Information Revolution

For the PLA, preparing for informationized warfare complicated a modernization effort that had focused on mechanizing the world's largest army. Indeed, for much of the first decade of the 21st century, PLA writings observed that the PLA was still "half-mechanized, half informationized." For at least part of this period, the PLA appears to have simply sought to acquire more information technology, ranging from computers to better communications systems, while still converting its forces from light infantry to motorized and mechanized forces.

In relatively short order, however, the PLA recognized that informationization meant more than just adding a layer of information technology atop more mobile forces. Rather, it would require a thorough reexamination of the nature of conflict.

INFORMATIONIZATION OF CONFLICT

The PLA concluded that, just as informationization has affected global economy and society, it has also influenced the nature of war. War, from the PRC's perspective, is a function of not just military forces and politics, but also larger social, economic, and technological trends. According to PLA writings, the "shape of war" (*zhanzheng xingtai*; 战争形态) is a reflection of the dominant economic order of the day, which in turn affects the main types of weapons, military organizational structure, concepts of operations, and forms of combat.[1] These factors, in combination, help define the overall nature of warfare.

Historically, warfare has evolved as societies have progressed from agrarian to industrialized, and economies have shifted from agrarian, through feudal, to capitalist.[2] The weapons wielded have correspondingly transitioned from "cold weapons," that is, swords, spears, and other edged weapons, to "hot

weapons," that is, gun powder–based to mechanized forces. Concomitant with the changes in societal organization and technology have been shifts in military tactics and organizations. Thus, agrarian militaries relied on chariots and columns of foot soldiers. Feudal armies were comprised of knights and other mounted troops, as well as archers, pikemen, and other increasingly specialized forces, who could coordinate between mounted and marching forces. Industrial militaries included artillery and eventually tanks and aircraft, which in turn demanded more specialized training and more extensive logistics. For the same reason, the rise of the Information Age, marked by the widespread integration of information and information technology into all aspects of modern society and economics, also affects the nature of conflict, leading to "informationized warfare" (*xinxihua zhanzheng*; 信息化战争).

For the PLA, recognition of the growing centrality of information in modern warfare grew over the last years of the 20th and first years of the 21st century. Although the PLA was overhauling its approach to warfare throughout the 1990s, this involved incorporating more high technology and sophisticated equipment throughout the PLA and training its soldiers and officers to use that equipment. There was not, however, a focus on information and associated technology per se. Similarly, in authoritative PLA sources such as the 1997 edition of the *Chinese Military Encyclopedia,* and its 2002 supplement, there was no entry for the concept of "informationization" (*xinxi hua*; 信息化).

There was, however, already thinking in some quarters about the specific impact of advances in information technology on future warfare. The 1997 edition of the Chinese volume on military terminology includes an entry for "information warfare" (*xinxi zhan*; 信息战), describing it as

> the conflict activities conducted by the two sides in the information realm. It mainly involves securing information resources, seizing the initiative in the production, transmission, and management of information, disrupting the enemy's ability to transmit information, in order to create the conditions for constraining or fighting and winning conflicts.[3]

An analytical piece by a Chinese military professor in 2001 chastises Chinese military thinkers for failing to recognize that, besides the physical elements of soldiers and weapons, combat power would be increasingly generated through both greater access to information and information exploitation to link together forces.[4]

The military volume of a 2003 Chinese encyclopedia of phrases defined "informationized warfare" as arising when one or both sides in a conflict relies on informationized weapons and combat methods to undertake combat activities. Such warfare will typically include forces drawn from multiple services,

jointly conducted precision firepower attacks, computer network warfare, space warfare, special operations activities, and so on, in the various domains.[5] This suggests that the concepts associated with informationized warfare were already beginning to be discussed beyond purely military audiences.

Meanwhile, below the surface but shaping Chinese military modernization priorities was the need to concentrate on improving information technology and exploit its capabilities. This was reflected in the 2002 Chinese defense white paper, which stated that the shape of warfare was moving toward "informationization." In response, the PLA was charged with fulfilling the twin responsibilities of mechanization and informationization as it modernized.[6]

The subsequent 2004 Chinese defense white paper made even more references to the importance of informationized warfare. It noted, for example, that "the forms of war are undergoing changes from mechanization to informationization. Informationization has become *the key factor in enhancing the warfighting capability of the armed forces*."[7] PLA modernization, the white paper went on to note, would focus on improving "the operational capabilities of self-defense under the conditions of informationization."[8]

By 2005, the PLA had published a study guide for informationized warfare and associated operations, reflecting extensive internal discussion of information, information technology, and related issues. The PLA's 2011 volume on terminology describes "informationized warfare" as warfare where there are networked information systems and widespread use of informationized weapons and equipment, all employed together in joint operations in the land, sea, air, outer space, and electromagnetic domains, as well as the cognitive arena. In informationized warfare, the main form of conflict is between systems of systems.[9] As part of this systems-of-systems construct, informationized warfare is envisioned as informationized militaries, operating through networked combat systems, command-and-control systems and logistics and support systems.

In informationized warfare, information serves as both a force multiplier for people, matériel, and capability and a form of combat power itself. Older weapons that are modernized with modern sensors and communications equipment (e.g., the B-52 and the A-10 or adding laser guidance modules to "dumb bombs") can retain or even enhance their effectiveness. Improved command-and-control systems can better coordinate various forces. Better information can allow more effective allocation of limited resources, allowing one's own forces to be more flexible and agile. Information weapons, such as computer viruses, in turn, can paralyze an opponent's system of systems, causing them to disintegrate and decohere.

The focus of informationized warfare is establishing "information dominance" (*zhi xinxi quan*; 制信息权), the ability to establish control of information and information flow at a particular time and within a particular space.[10]

It entails the ability to collect more information, manage it faster, and employ it more precisely than the adversary.[11] By doing so, in the Chinese view, one can maximize the effects of all this newly available information. The side that enjoys information dominance can then seize and retain the initiative and force the adversary into a reactive mode, losing the ability to influence the outcome of an engagement. This exploits a key difference between mechanized warfare of the Industrial Age and informationized warfare of the Information Age. "Mechanized warfare focuses on physically and materially destroying an opponent, whereas informationized warfare focuses on inducing the collapse of the opponent's psychology and will."[12]

Establishing information dominance involves efforts that span the strategic to the tactical level. The knowledge required to establish information dominance includes an understanding of not only the adversary's information systems but also their key decision makers and decision-making processes. This entails significant intelligence gathering throughout peacetime. Because of the rapid, decisive nature of "local wars under informationized conditions," it is not possible to wait until the formal commencement of hostilities to begin preparations. At a minimum, identifying opposition capabilities and weaknesses must be undertaken in peacetime.

Nor can establishing information dominance be solely a military function. As the world has informationized, so has the global economy; consequently, key vulnerabilities may not be in military systems but in the financial system or critical infrastructures such as power or transportation. Because modern information networks are interconnected and given their extensive permeation, "information dominance" involves gaining access not only to enemy military networks but to essential nonmilitary ones as well. Civilian and commercial decision makers and the broader population are also vital targets. Similarly, it is essential to target not only an adversary's data but also the systems involved in data collection and management, and the users and analysts of that data as well.

For these reasons, successful defense against adversary efforts to establish information dominance makes enormous demands upon one's own information systems, both military and nonmilitary. Successful defensive efforts require countering adversary targeting of all three aspects of one's own information architecture, that is, data, systems, and users. Since information itself can be used as a weapon (beyond the incorporation of viruses and malware) by influencing its consumers, successful defense requires that information itself be monitored and information flow be tightly controlled.

Given the more expansive view of information's role, the human element is especially important. Chinese analysts note that the advent of more advanced weapons technologies did not necessarily lead to a change in war's basic nature. Instead, the core of informationized warfare is the expanded

range of abilities to influence and control an opponent's judgment and will to fight.[13] The ability to influence people, including their politics, thinking, morale and spirit, and psychology, can be as decisive and effective as the ability to interfere with databases or computer networks. Influencing an adversary through proper application of suitable information is embodied in the Chinese approach to political warfare.

POLITICAL WARFARE AS INFORMATIONIZED WARFARE

The Chinese conception of political warfare epitomizes its views of informationized warfare. "Political warfare" (*zhengzhi zhan*; 政治战) uses information to undertake sustained attacks against the enemy's thinking and psychology, to eventually subvert their will.[14] Successfully waging political warfare can help secure information dominance at its most basic level, influencing adversary thinking and perceptions. Conversely, information dominance is essential for successful political warfare; failure to establish information dominance opens the way to attacks on one's political stability.[15] From the Chinese leadership's perspective, there is a constant threat of "Westernization" and "splittism," endangering the nation's political security and the party's hold on power. This is at the root of Western calls for greater democratization and liberalization.

Although political warfare is mainly waged with strategic communications tools, including television, radio, the Internet, and news organizations, it is nonetheless considered *a form of warfare*. It envisions the use of information to attack opponents, eroding will, imposing psychological pressure, and influencing cognitive processes and the framework of perceptions. Because of the informationized condition of the global economy, political warfare efforts are no longer limited to frontline military forces but are applied against adversary populations and leadership. Political warfare is the weaponization of soft power.

Similarly, because modern information technology blurs the lines between peacetime and wartime, between military and civilian, and among strategy, operations, and tactics, political warfare is not limited to when hostilities have formally commenced and is not focused solely on military targets.[16] Instead, informationized warfare includes activities that are undertaken in peacetime, many of which are aimed at the adversary's political leadership and broad population. Informationized warfare, even more than Industrial-era mechanized warfare, encompasses the entire society of both sides.

PLA Concepts of Political Warfare Operations

Given the importance of political warfare, it should not be surprising that it is entrusted to the highest bureaucratic levels of the PLA. According to the

2003 "Political Work Regulations of the Chinese People's Liberation Army," and the subsequent 2010 revision, the General Political Department (GPD), one of the four General Departments that runs the PLA, is responsible for the conduct of political warfare. In particular, it is responsible for waging the so-called three warfares (*san zhan*; 三战)—public opinion warfare, psychological warfare, and legal warfare, the central methods of political warfare.[17]

The "three warfares" will be conducted in combination, as they are an integrated whole. Both individually and in concert, these political warfare efforts strive to shake the enemy's will, question their motives, induce divides and splits within the enemy's ranks, and constrain their activities. While ideally they might cause an opponent to concede the struggle entirely, more likely they will erode an adversary's will and thus reduce the ability to sustain any resistance to more kinetic operations.

Because of the difficulties in coordinating political warfare efforts with each other, as well as with both broader strategic measures (e.g., economic, diplomatic efforts) and military operations, the Chinese are emphatic about the need for coordination. This includes establishing a coherent plan for its conduct, incorporating not only the elements of political warfare (including the three warfares) but also other military, media, political, and diplomatic activities.

PLA efforts at political warfare are simplified and facilitated by vesting it within the GPD. Many GPD officers have undergone training in political warfare and indeed are specialists. Therefore, they will be planning and implementing operations for which they have been specifically trained. Moreover, the PLA contains an entire GPD chain of command that parallels the operational chain. This allows political warfare practitioners to oversee, coordinate, and integrate political warfare activities from tactical level to strategic, while maintaining methodological consistency and focus on specific goals.

The GPD's role will also facilitate coordination between political officers and staff and their operational counterparts of the General Staff Department (GSD). Because of the dual-control system (where authority is shared between GSD and GPD, especially through the political committee that runs the unit), there are extensive peacetime, day-to-day links between the two staffs as they manage the unit together.

While there is undoubtedly bureaucratic stove-piping between the two entities, there are also likely established means within individual units to coordinate activities, honed through peacetime interactions. This mutual familiarity is likely to pay off in wartime, in terms of integrating political warfare measures with other military operations.

The broad outlines of the political warfare effort, including "guiding principles" (*fangzhen yuanze*; 方针原则) and overall directives will come from the CCP Central Committee (in practice, the Politburo) and Central Military

Commission (CMC). Higher-level commanders will take these principles, directives, and overall objectives and fashion plans of action for their level of command (joint campaign command headquarters [JCCH], group armies/military region air forces/fleets, etc.), while issuing guidance and directives for subordinate forces. Lower-level commanders, in turn, will draw up plans to fulfill their assigned operational missions and issue orders to their subordinates.

At each level of unit, specific political warfare efforts are developed by the unit's party committee, its political officer, and his staff. Organizationally, this means that the operational commander and main department heads, as well as the political officers of a unit, will participate in developing the political warfare effort, since all of them are part of the party committee. Again, at least theoretically this means that political warfare efforts are organically tied to more kinetic operations and activities. Military commanders are admonished, when laying out their operational plans, to integrate those plans with three warfare operations, making them all mutually supporting and complementary. This includes deconflicting resource demands and reconciling means and objectives.

The specific measures and plans for political warfare at the strategic and higher operational levels will likely be planned within the "political work office" (*zhengzhi jiguan*; 政治机关) contained in the joint JCCH. This office will usually be organized into a human affairs center, a propaganda and mobilization center, a military legal affairs center, a political warfare center, and the joint campaign party committee general office.[18] It will typically include the unit's top political officer and his staff, comprising three to five cadre, one of the unit's deputy operational commanders, and a senior member of the headquarters staff, as well as subordinate units' chief political officers.[19] The political work office is at the same level of importance as the JCCH's information operations center, firepower coordination center, joint logistics and safeguarding center, local support center, and so on. In some campaigns, depending on the forces committed, there may also be separate service political work offices, responsible for the individual services participating in a given campaign.

Not only will the main JCCH have a political work office, but there will also usually be a smaller counterpart office assigned to the forward command post of the JCCH. Headed by a deputy head of the political department, it will provide immediate, frontline political work support. These are more tactical-level activities, such as propaganda broadcasts and leaflet drops aimed at adversary frontline forces. Meanwhile, a reserve, rear-area command post will also have a political work office, headed by another deputy head of the unit's political department. This will often interact with the local civilian authorities, building upon the peacetime interactions that occur between a military unit's party committee and corresponding local civilian party committees. (For example, military districts, prior to the recent reform, were usually coterminous

with provincial boundaries.) The political warfare planners would be able to draw upon local, civilian personnel, equipment, and facilities (e.g., broadcasting stations, cyber specialists, Internet, and communications equipment).

Waging Political Warfare through the "Three Warfares"

Taken together, the three warfares seek to employ various types of information, for example, diplomatic, political, economic, as well as military, in a manner consistent with military strategic guidelines and objectives, to win the political initiative and achieve a psychological advantage. The aim is to strengthen one's own resolve while disheartening the adversary, since the lack of will makes even the most sophisticated weaponry irrelevant. An essential element of achieving this psychological advantage is to present oneself as the aggrieved party and holding the moral and legal high ground. Not only does this serve to stiffen one's own will, but it can be an important part of influencing bystanders and third parties.[20] Political warfare complements, but does not necessarily displace, traditional use of force.

Each of the three "warfares" employs information in a different manner to achieve these goals, but reinforces the other two. Psychological warfare exploits information by drawing upon political, economic, and cultural, as well as military elements of power. Information of each type can serve as a powerful weapon, influencing values, concepts, emotions, and context.[21] Legal warfare can build psychological support and sympathy among bystanders and erode an opponent's will by constraining the opponent's preferred courses of action for fear of legal repercussions. Public opinion warfare can directly build support, persuading domestic and foreign audiences of the justice of one's own cause and the success of one's own efforts, while undermining an adversary's attempts to do the same. In particular, the growth and expanded reach of media of various sorts makes public opinion warfare especially important, as it can have global effects. Broad domestic and international support, in turn, will generate psychological benefits for oneself and adversely affect the enemy.

Psychological Warfare

The central element of the three warfares is psychological warfare (*xinli zhan*; 心理战). This involves the application of psychological principles and methods to attack an opponent's psychology and erode the enemy's will to resist, while also engaging in psychological defensive measures to protect one's own will and encourage greater effort.[22] Psychological warfare pressures an opponent by employing information to affect its thinking, to create damaging or deleterious habits and ways of thinking, to reduce its will to resist, and perhaps even to induce defeatism and surrender.[23] At the same time, it seeks to limit the effect of enemy psychological warfare operations on one's own

troops, population, and leadership; building morale; encouraging greater resistance and effort; and strengthening will.

Psychological warfare employs a variety of measures including terror, intimidation, deception, enticement, as well as propaganda. The latter includes media warfare. Although psychological warfare draws on a variety of nonmilitary resources, it has always been a PLA responsibility, vested in the GPD's military political work structure.[24]

In many ways, all of the three warfares are ultimately aimed at influencing the adversary's psychology, whether by undermining popular support or imposing legal challenges and constraints. Psychological operations will be integral in future conflicts, affecting and influencing the very perceptions that inform decision making, from context to biases. Successful psychological operations in informationized warfare will generate repercussions at strategic, operational, and tactical levels of operations, influencing both military and civilian leaders and the masses, affecting the course and outcome of the conflict.

In the past, psychological warfare was more domestically or tactically focused and was primarily supplementing more kinetic operations.[25] It was very difficult to access an opponent's population; consequently, one sought to maintain domestic support or undermine enemy military forces through leaflets, battlefield loudspeakers, and so on. In World War II, radio broadcasts sought to undermine troop morale (e.g., "Axis Sally" and "Tokyo Rose"), but to limited effect. With advances in information technology, however, strategic psychological warfare is much more significant because of its broader reach.

By combining greater penetration and more comprehensive forms of psychological attack, modern psychological warfare practitioners have an unprecedented capacity for undermining an adversary's will and psychological balance. Psychological warfare can powerfully supplement traditional military means and effects. The rise of international news media, for example, provides a global messaging forum that magnifies strategic psychological warfare efforts. Similarly, international entertainment conglomerates influence audiences around the world, with attendant psychological impacts (e.g., subtly shaping perceptions and preferences).

Psychological warfare is not solely passive, however. Economic sanctions and blockades have long been employed to psychologically isolate an adversary as well as weaken its economy. Similarly, diplomatic measures such as withholding recognition of a regime underscore its isolation and vulnerability. The growth of global financial interconnectivity allows financial attacks, such as against an adversary's currency, generating psychological as well as economic repercussions. The Chinese believe modern technologies and techniques strengthen such measures, inducing "psychological shock and awe" (*xinli zhenshe*; 心理震慑).[26]

An additional method afforded by modern technology is the "information sanction" or "information blockade." By limiting the kinds of information an adversary can access, while preventing it from getting its own message out, a sense of strategic isolation is induced. This can erode domestic support and sap the will to resist. Chinese authors credit the United States with employing such methods against the Serbians in the Balkan conflict. NATO press conferences dominated global impressions of the situation, overwhelming Belgrade's ability to present its side. Meanwhile, NATO psychological warfare units broadcast messages into Serbia, employing a variety of platforms to transmit alternative television and other programming; they also exploited popular music and other means to obtain audience interest and generate public appeal.[27]

Similarly, Chinese analysts note how the United States imposed an information blockade on the Taliban, prior to intervening. This denied the Taliban information about American military preparations, while ensuring that the global understanding of the Afghan situation was seen through an American lens.[28]

By imposing an information blockade, the target's perceptions and viewpoints are more easily manipulated, since only limited information is available to it, and that may well be influenced or tainted. At the same time, the target is isolated, which may undermine its resistance, especially in the face of overwhelming force. The target's inability to spread its own message further heightens the sense of isolation, while limiting prospects for external support, which would afford both psychological and material relief. The spread of the Internet provides an important new venue for information blockades, raising the importance of imposing one but also providing an essential new means of doing so.[29]

Chinese examples of information blockades all commence *before* the formal onset of hostilities. This is typical, in the Chinese view, of most psychological operations. According to Chinese analyses, psychological warfare operations blur the line between wartime and peacetime, as well as between frontline and rear areas, military and civilian. Indeed, to be effective, such operations *cannot* be limited to wartime or just military targets. Instead, peacetime psychological operations are necessary to better understand an opponent and to lay the groundwork for more focused wartime efforts.

Peacetime applications of psychological warfare techniques influence and alter an opponent's unconscious, implicit views, making it more susceptible to coercion. An important approach is to employ various forms of strategic communications, including diplomatic efforts and economic influence, to foster a positive national image of oneself and increase foreign sympathy and support for one's own policies and goals. In addition, one should employ all types of communications, including various forms of media, to emphasize

one's own strengths, and the willingness to use it, to improve the ability to deter and coerce opponents.[30]

PLA writings also call for peacetime undermining adversary positions. This includes portraying others as fostering ill intentions and forcing them to react to various charges so their energy is dispersed and not concentrated on supporting their own goals. All the while, one must also be countering likely opposition efforts to foster their own image of strength and unity and defend oneself from their efforts at sowing demoralizing concepts.[31]

Wartime applications of psychological warfare shift the emphasis more specifically toward military targets and goals. The primary objective of wartime efforts is generating confusion, doubt, anxiety, fear, terror, regret, and exhaustion in an opponent, especially among senior military and civilian leaders. Ideally, this will induce neglect and maximize the chances of mistaken decisions or actions that can then be exploited. Wartime psychological warfare operations also aim to generate uncertainty and indecisiveness at all levels, degrading adversary decision-making processes. Interfering with an opponent's information systems, coupled with efforts to influence its decision makers, can create a strong psychological impact.

Another facet of wartime psychological operations is to sow discord and hopelessness in the enemy. Not only will this generate war weariness among enemy forces and populations, discouraging resistance, but can facilitate peace negotiations and induce more concessions. "When one defeats the enemy, it is not solely by killing the enemy, or winning a piece of ground, but is mainly in terms of cowing the enemy's internal heart."[32] This involves emphasizing information favorable to oneself and transmitting parallel messages via various forms of media, as well as through third parties, friendly elements in one's society, and so on.

Offensive psychological warfare operations must be complemented by defensive measures, since an opponent will be trying to undermine one's own forces, population, and leaders. It is essential to solidify popular support for the conflict, to highlight one's successes and the enemy's failures, and to instill confidence and support for the party and the state. This requires tight control over information flows in one's own society and insulating one's decision makers and decision-making processes from enemy information warfare efforts.

Both peacetime and wartime psychological warfare efforts require dedicated psychological warfare units and their staffing with suitably trained personnel. The units and personnel, moreover, must be familiar with modern information systems, as well as psychology, culture, and language, to maximize their effectiveness. Their training should incorporate "creation and application of information for psychological attacks; thoroughly understanding the enemy's military, social, and psychological weaknesses within likely conflict

areas, to facilitate focused creation of information for various types of [psychological] attacks; psychological warfare techniques and weapons, including broadcasting, battlefield loudspeakers, aircraft transmissions."[33]

Legal Warfare

Chinese analyses of legal warfare emphasize it is a central means of political warfare, supporting both psychological and public opinion warfare by "controlling the enemy through the law, or using the law to constrain the enemy (*yifa zhidi huo yong fa zhi di*; 以法制敌 或 用法制敌)."[34] Indeed, based on recent conflicts, the Chinese have concluded that "military warfare and legal warfare have already thoroughly combined," with legal warfare permeating conventional military operations, while military conflict intrinsically contains legal warfare.[35]

As with other forms of political warfare, legal warfare begins before formal commencement of military hostilities. By applying various types of legal information, including international and domestic laws, the laws of armed conflict, legal pronouncements, legal education, and law enforcement, Chinese leaders try to influence both foreign and domestic audiences. The objective is to garner support, deter action, and even influence military behavior, such as the choice of targets or weapons.[36]

Legal warfare involves depicting "one's own side is obeying the law, criticizing the other side for violating the law (*weifa*; 违法), and making arguments for one's own side in cases where there are also violations of the law."[37] The ultimate aim is securing the initiative in time of conflict by gaining the legal high ground, portraying oneself as more firmly grounded in legal standing, and implicitly being more virtuous and just. As one Chinese analyst observed,

> implementing "legal warfare" is to gain the right in warfare. Regardless of whether a war is just or not (*zhengyi yu fo*; 正义与否), the two sides in a war will both make every effort to develop "legal warfare," and seek out means of constructing legal bases for undertaking the war, and confirm that they themselves are the reasonable and legal side.[38]

The employment of legal information can play an important role prior to, during, and after the outbreak of formal hostilities. Legal warfare is integral to political preparation of the battlefield, employing legal information and arguments to influence various audiences in support of deterrent or coercive goals. It is especially important to broadly propagate Chinese legal positions and perspectives, so that they are "recognized by the international community."[39]

In peacetime, legal warfare influences domestic and foreign populations and leaders, weakening opposing coalitions while building support for one's own side. In wartime, it manipulates the rule of law in order to "destroy the will to fight by undermining the public support that is indispensable" for successful warfighting.[40]

Thus, Chinese passage of the 2005 Anti-Secession Law provides the political justification for any future move against Taiwan (or Tibet or Xinjiang) but also politically signals Chinese resolve to the native populations of these areas and any states or actors that might support them. Similarly, China's idiosyncratic interpretations of the UN Convention on the Law of the Sea signal not only China's position but its commitment to that position, which will potentially influence other claimants and players.

Indeed, the Chinese use of law enforcement vessels in many of its maritime territorial disputes is a form of both legal warfare and psychological warfare. It reduces escalatory pressures, since it employs civilian, not military, vessels. At the same time, the use of law enforcement vessels and agencies implicitly signals that a given piece of territory or water is Chinese—hence, it is subject to Chinese law enforcement as a matter of internal or domestic security rather than the military.

Beyond strategic uses of legal warfare, there are also operational and tactical benefits from the militarization of legal information and approaches. One potential use of legal warfare could be to delay American responses to Chinese actions. This could span a variety of options, such as filing motions relating to the War Powers Act or challenging the right to mobilize various American resources. In addition, there may be legal action in environmental, labor, and other arenas, beyond those directly linked to foreign policy and national security.

Chinese legal warfare efforts can also try to limit American access to foreign bases and facilities, essential for U.S. operations in the western Pacific. Such efforts would target any American ally and friends that might provide forward basing facilities, including Singapore, the ROK, the Philippines, and Thailand. These measures would likely be coordinated with pressurizing military activities (military overflights, nearby naval exercises), as well as economic actions, such as promises of expanded investment or threats of factory closures, and also diplomatic legal steps, such as support in other territorial or economic disputes (e.g., World Trade Organization cases). If successful against either the American or allied audience, such legal warfare measures could affect American deployments, reducing their ability to operate successfully against Chinese forces.

In wartime, American analysts have expressed concern that legal warfare efforts may induce excessive restraint in military operations. Military commanders may choose to err on the side of caution for fear of violating international law, especially the laws of armed conflict, and becoming liable to charges

of war crimes. Indeed, the American 2008 National Defense Strategy expresses concern about "growing legal and regulatory restrictions that impede, and threaten to undermine, our military readiness."[41]

Chinese analysts have reached similar conclusions. Legal warfare, in their view, can directly affect popular support for a conflict, both at home and abroad. One goal of legal warfare is

> to psychologically dissipate the other sides' fighting will in both the military and the civilian realms, while exciting one's own military and civilian passions and obtaining international sympathy and support.[42]

These analysts note, for example, the outcry after the bombing of the Al-Firdos bunker in the 1991 Gulf War and that "the substantial loss of human life and the serious violation of the laws of war" led to adverse political and moral consequences, which directly affected military planning and operations.[43]

Chinese analysts also see legal warfare as playing a significant role in the aftermath of conflict. Coupled with diplomatic and military measures, it can help consolidate wartime gains.

To achieve these ends, Chinese writings on legal warfare emphasize that it is a form of *warfare*. Therefore, it must be undertaken under a unified command organization, with a unified plan, coordinating among various political warfare measures, but also with more traditional, kinetic military measures.[44] These measures must also be undertaken in coordination with other strategic and operational goals.

Those coordinated legal warfare operations are *offensive* in character. They force an adversary to react and to devote time and resources responding. Chinese writings suggest that legal warfare measures would include

- Legal coercion/deterrence efforts, warning an opponent that it is under close scrutiny for possible violations of the laws of armed conflict, in order to impose self-constraint;
- Legal strikes, charging the enemy with operational activities in violation of international and domestic laws; and
- Legal counterattacks, highlighting enemy efforts at slanting or misrepresenting international law in its favor, unfavorably contrasting its conduct with one's own (in legal terms), and countering any enemy legal activities.[45]

By contrast, typical Western concepts of legal warfare are more *defensive*, driven by fears of legal sanction (and attendant loss of public support), that have often constrained exploitation of Western advantages.[46] Perhaps most controversially, early in the Afghanistan War, because the legal officer (JAG) on the American staff had concerns about civilians in Mullah Omar's convoy, an

orbiting *Predator* drone was denied permission to attack. Omar therefore escaped.[47] More notably, in the context of informationized warfare, the U.S. Department of Defense reportedly did not employ certain cyber options against Slobodan Milosevic during the Kosovo conflict, because the legality of such actions was unclear.[48]

Public Opinion Warfare

Chinese analysts envision public opinion warfare (*yulun zhan*; 舆论战), also translated as "media warfare" or "consensus warfare," shaping targeted audiences through information derived and propagated by mass information channels, including the Internet, television, radio, newspapers, movies, and other forms of media. While news media play an important role in the Chinese conception of public opinion warfare, it is only a subset of the larger set of means available for influencing public opinion.[49] All these channels will transmit a consistent message to the intended audience, in accordance with an overall plan, to instill certain views and conclusions that are beneficial to oneself and detrimental to the adversary.

Public opinion warfare is an essential support for psychological warfare efforts, as it prepares audiences for the psychological warfare messages. Chinese analysts see public opinion warfare as an especially powerful element of informationized warfare. Because of the wide permeation of information technology, public opinion warfare can now reach every part of society.

The goal of public opinion warfare is to shape public and decision-maker perceptions and opinion, shifting perceptions of the overall balance of strength between oneself and one's opponent.[50] Successful public opinion warfare will influence three audiences: the domestic population, the adversary's population and decision makers (both military and civilian), and neutral and third-party states and organizations. It will preserve friendly morale, generate domestic and foreign support, weaken the enemy's will to fight, and alter the enemy's situational assessment. Public opinion warfare is both a national and local responsibility. Not only will the PLA engage in it, but so will the People's Armed Police, national and local media, spokespeople, netizens, and other groups.[51]

Public opinion warfare is an autonomous activity; it occurs independent of an actual, formal conflict. Put differently, it is always under way. According to Chinese analyses, the side that plants its message first enjoys a significant advantage influencing public opinion. Indeed, Chinese analyses repeatedly emphasize that "the first to sound grabs people, the first to enter establishes dominance (*xian sheng duoren, xianru weizhu*; 先声夺人，先入为主)." Essentially, the Chinese seek to define the terms of the debate and parameters of coverage. By presenting one's message first, the PLA expects to shape everyone

else's views. This will allow Beijing to underscore the justice and necessity of its operations, better display national strength, exhibit the superiority of its forces, and shake an opponent's will to resist.[52] By contrast, adversaries must overcome ideas that are already planted and taking root by Chinese public opinion warfare efforts. In a very real way, Chinese decision makers see public opinion warfare as being waged even in peacetime, as part of larger efforts shaping people's perceptions of the PRC. There is a constant effort to influence audiences to accept China's narrative and perceptual framework.

To maximize the effectiveness of public opinion warfare, all channels of information dissemination must be exploited, so that a given message is reiterated, reinforced by different sources and different versions. Public opinion warfare efforts embody the ideal of "combining peacetime and wartime operations; civil-military integration of resources; military and local resources unified (*pingzhan jiehe, junmin jiehe, jundi yiti*; 平战结合, 军民结合, 军地一体)."

The Chinese have established a Ministry of National Defense Information Office (MNDIO), responsible for engaging the press. This office is the main mechanism for disseminating China's position on military and security-related issues. It promotes the image of the PLA as a competent and capable force and tries to counter negative impressions, including that the PLA is a secretive organization. Established in 2008, spokespeople from the MNDIO have held monthly press conferences since 2011.[53]

Civilian resources play a prominent role in public opinion warfare, because there are substantially more civilian and commercial media assets, including broadcasting facilities, Internet users, and news organizations and reporters. Nonmilitary assets also often have better techniques and information than their military counterparts.[54] Where possible, public opinion warfare efforts will exploit the reputation and long-term presence (e.g., branding, established relationships) of those nonmilitary assets.

To be successful, public opinion warfare messaging must be flexible, incorporating shifts in strategic, political, and military contexts. Rather than a one-size-fits-all approach, different messages are tailored for different audiences. When engaging in public opinion warfare against what the PRC regards as secessionist elements, for example, "one must make distinctions between the more stubborn elements and the general populace."[55]

Careful preparation of the public opinion battleground in peacetime is essential. This requires understanding potential opponents' psychology and national moods, extensive research into tactics and methods, and developing public opinion warfare specialists. This is not limited to the news media; in the Iran–Iraq War, for example, Chinese analysts note that Iran linked news-based propaganda with religious outlets. Employing religious fervor helped bolster public morale in support of the state.[56] Such efforts, however, require a thorough understanding of target audiences. PLA writings consistently invoke the saying, "Before the

troops and horses move, public opinion is already in motion (*bingma weidong, yulun xianxing;* 兵马未动，舆论先行)," emphasizing that public opinion warfare preparations must begin far in advance of formal hostilities.[57]

Indeed, it is not clear that public opinion warfare differentiates between peacetime and wartime. In the first Gulf War, the United States is said to have fully used its advantage in information dissemination to constantly bombard the Iraqi military and civilian population with various messages undermining Iraqi will (and especially to induce uncertainty in Saddam Hussein). This began long before the first cruise missiles struck or first air raids began. Chinese analysts note that before invading Afghanistan, Washington employed public opinion warfare mechanisms to create an antiterrorism coalition; gain international support; and allay concerns among Arab and Muslim nations.[58]

Defensive public opinion warfare efforts limit the impact of enemy public opinion warfare. These efforts entail strong education and news management efforts to minimize domestic popular exposure to enemy messages and to nullify the impact of those messages. Defensive public opinion warfare builds public skepticism toward external and internal criticisms of the government. Those criticisms that do leak through are countered by prompt, credible responses.

CHINA'S STRATEGIC INFORMATION DEFENSE

For the Chinese leadership, establishing information dominance requires preventing an adversary from exercising undue influence on the population. In the Information Age, this means that Chinese authorities must control the flow of information to the Chinese people, including via traditional media, but especially across the Internet and through social media channels.

Not only must the CCP counter foreign intrusions and interference, but it must also prevent *domestic* opponents from creating and spreading unrest. Social media platforms especially increase the potential of organized protests against CCP rule. The specter of internal and external opposition combining, or worse cooperating, makes information control a paramount priority and unfettered information flow a *strategic* threat.

The confluence of information technology expansion and the collapse of the Soviet Union affect CCP threat perceptions. After all, China's first connection to the Internet in 1994 occurred in the shadow of the USSR's collapse, which itself came on the heels of the Tiananmen Square massacre. The growing ability to share information, and act upon it, clearly poses burgeoning challenges to a Chinese leadership that has witnessed the collapse of global Communist ideology and significant domestic unrest. Chinese efforts to control the Internet and social media, with their extensive permeation and reach, should be seen as the equivalent of strategic homeland defense. The CCP's

determination to limit the vulnerability of the population (and therefore itself) to information weapons parallels civil defense measures to protect the population from nuclear weapons.

Especially important is control of social media platforms, which not only allow prompt dissemination of information to large audiences (akin to traditional media) but also can rapidly organize public opinion and even action. Indeed, preserving social control and preventing the population from engaging in unapproved action appears to be as important as censoring information outright. Rebecca MacKinnon observed in 2009 that Chinese governmental regulatory bodies base rewards and punishments "on the extent to which Internet companies successfully prevent groundswells of public conversation around politically inflammatory topics that might inspire a critical mass of people to challenge Communist Party authority."[59]

A subsequent study reached a similar conclusion, observing that "the purpose of the censorship program is to reduce the probability of collective action by clipping social ties whenever any collective movements are in evidence or expected."[60] Researchers found that Sina Weibo postings and other expressions were far more likely to be taken down and would be taken down faster, when they promoted collective action, for example, protests or gatherings. This was true *even if the messages supported the government's position*. "Whether or not the posts are in favor of the government, its leaders, and its policies has no measurable effect on the probability of censorship."[61]

The Chinese government closely monitors not only information but how that information is interpreted and acted upon. While it is not possible to totally control what is expressed, Beijing clearly tries to suppress unauthorized, popular reactions to that expression.

The central authorities' efforts are facilitated by the near total dominance of domestic providers, as well as governmental control of China's telecommunications infrastructure. By creating an indigenous set of social media platforms, rather than relying on foreign programs, Beijing can control not only what is transmitted via social media but also how that information travels over China's information and telecommunications networks. For example, Beijing has been able to shut down text messaging systems while maintaining cellular phone network operations. This has been essential, given the heavy reliance on mobile phones rather than landlines for general internal connectivity. Both private citizens and the government can continue to communicate, even when the government simultaneously clamps down on the ability to organize opposition, but the ability to create crowds is minimized.

In sensitive areas such as Tibet and Xinjiang, Chinese authorities have amply demonstrated both will and capability to prevent unauthorized and uncontrolled dissemination of information. In Tibet, both Internet and telephone connectivity has reportedly been spotty and uncertain since 2008 protests.

When protests about racial violence against Uighur workers in Guangdong became violent in 2009, Internet access was suspended across the entire Xinjiang Autonomous Region within hours. Limits on phone calls and text messaging followed.[62] Since then, there have been repeated shutdowns and disruptions of Xinjiang Internet and telephone service. However, in both areas, government agencies (e.g., police) and critical infrastructure such as finance and transportation have retained connectivity, reflecting the Chinese ability to wield a scalpel as well as a cleaver when controlling information.[63]

Through central control of physical infrastructure and promotion of indigenous software and platforms, China has created a fairly insulated, relatively controlled internal information environment, even as it is connected to the global information network. This is backed by an overlapping array of technical and human censors. These ensure not only that disseminated information is politically acceptable but any reactions can be channeled into acceptable forms.

The average Chinese citizen's view of the world, and even of China, is bounded by a pervasive, but not necessarily obvious, set of blinders. So long as they stay within those limits, they are free to enjoy the benefits of both an extensive internal information network and access to broader global resources. But should Beijing deem it necessary, the authorities can close some or even all of those shutters, in ways that few other authoritarian states can, because all of the levers are in Chinese hands.

Countering Political Warfare: Controlling Information

Especially important for the conduct of political warfare is mobilizing public opinion. This serves two functions. First, it builds and sustains support for the war effort and the top leadership. This, in turn, may signal an adversary of Chinese will and commitment, which may deter it from intervening or resisting Chinese actions. At the same time, mobilizing public opinion can help inoculate the population against the effect of local or strategic reverses. It is a means of manipulating the public's perceptions to avoid defeatism and uphold morale. This is especially important, given the likelihood of attacks on key Chinese economic, communications, and energy facilities.

Public opinion mobilization is a part of the larger information mobilization effort. It requires focused, targeted employment of information to obtain the intended effects.[64] This entails not only directly influencing Chinese public opinion but also shielding it from adversary efforts to influence and shape it.

Therefore, even as the Chinese authorities are waging political warfare against likely adversaries, they are also defending the Chinese population from such efforts. One essential concern is the ability of outsiders to exacerbate internal unrest and jeopardize CCP control. This is not a theoretical

concern, but instead reflects genuine worry among the senior Chinese leadership. The 2014 Chinese defense white paper, for example, notes that external forces seek to foment a "color revolution" in China, which would topple the CCP from power.[65]

CCP concerns are not only that outsiders might influence the broad Chinese population, but that senior political and military leaders might be suborned, undermining leadership morale and the will to fight. Events during the 1989 Tiananmen incident undoubtedly haunt Chinese decision makers about the possible impact of political warfare and other efforts to sow discord among senior leaders. As the senior Chinese leadership planned to use military force to suppress the protestors in Tiananmen Square, Major General Xu Qinxian, commander of the 38th Group Army, the centerpiece of ground forces in the Beijing Military Region, reportedly rejected the idea. He apparently felt that the protests "were a political problem and should be settled through negotiations, not force," a stance that reportedly led to his arrest.[66] Nor was Xu alone in holding such views. Other officers reportedly signed a petition to withdraw the troops. Eventually, other units had to be activated to move against the protestors. For China's leaders, the ability to control the military with absolute certainty was an open question.

Less than two years later, American and coalition forces overwhelmed Iraqi forces in Kuwait and Iraq. During Operation Desert Storm in 1991, Chinese commanders witnessed the impact of psychological warfare and public opinion warfare enhanced by modern technology. American and coalition forces coupled sustained aerial bombardment with leaflet drops and, in the Chinese view, carefully gauged the psychological impact of their attacks. The ferocity of initial strikes, moreover, had their own psychological impact, enhancing dedicated psychological warfare efforts.[67]

At the same time, Chinese analysts saw American and coalition forces waging public opinion warfare and psychological warfare campaigns to both undermine Iraqi support for Saddam Hussein and deny Iraq international support and sympathy. Chinese analysts have identified a variety of public opinion warfare techniques, ranging from spreading rumors via the media to describing Iraqi destruction of Kuwaiti oil fields as "environmental terrorism." All these measures denied Iraq any foreign sympathy, while eroding the regime's internal support.[68] The United States also employed monetary inducements and threats of war crime trials to undermine Iraqi military leaders' willingness to fight or otherwise obey Saddam's orders. Chinese writings assess that these political warfare efforts helped propel the American victory in the Gulf War by undermining Iraqi will.[69]

For China's leadership, the threat is clear: an advanced adversary, using various means of manipulating and inserting information, could create

divisions within the party's military, between military and civilian leaders, and between leadership and masses. The adversary could then exploit these divisions to erode national will, instill defeatism, and fray national support, thereby defeating the PRC.

This has made CCP efforts to control information and its flow both into and within China, in both wartime and peacetime, even more urgent. It has also made the CCP prioritize efforts to influence how that information might be perceived and interpreted. These include controlling the news, establishing an extensive web of Internet controls and censorship, as well as specific monitoring and control of social media.

Government Limitation of the Internet

While China's opening to the West forced it to accommodate greater media access, this was controllable. As described earlier, the Central Propaganda Department has long been an established mechanism for press censorship, so it could readily accommodate changes in the traditional media environment, including greater foreign presence. Indeed, even with the introduction of foreign journalists, there were still only a restricted number of outlets. The number of persons and entities that required monitoring remained limited. Previous media access controls (e.g., press passes, visas) remained sufficient to limit the newly expanded foreign press.

By contrast, the Internet poses an unprecedented threat to governmental ability to control information flow. This is in part because the CCP wants China to have broad access to the Internet. It is a key means of conducting business; China could not hope to participate in the modern global economy if it did not have ready connectivity with global information networks. It also easily accesses the global wealth of knowledge, an essential means for improving China at relatively low cost.

But access is a two-way street. Expanding linkage to the global information network raises the potential vulnerability of Chinese networks to significant criminal activity. China regularly argues that it is among the most-hacked nations in the world. In 2012, for example, the Chinese reported that 22,000 phishing websites had targeted Chinese netizens, while 14 million mainframes in China had been hijacked by various Trojan horses and botnets. Many of these are traced to foreign websites, "with the United States being the largest source of such hacking activities."[70]

Moreover, just as Chinese authorities use the Internet to obtain information and to influence others, other players, including both state and nonstate adversaries, can use it to transmit information to Chinese audiences. Senior Chinese leaders including Deng Xiaoping, Jiang Zemin, and Hu Jintao have all warned of Western efforts to subvert China through "Westernization" and

"peaceful evolution," that is, eroding CCP legitimacy (leading to "peaceful evolution" away from CCP rule). As one observer astutely notes, *the entire basis* of the past three decades of Chinese economic reform has been

> to benefit from Western technology and from trade with the global market economy *without* converging into the West's liberal democratic governance model.[71]

Chinese authorities consider efforts to draw China into that Western model, whether conscious or not, a de facto form of political warfare. The introduction of the Internet only exacerbates them.

If the Chinese leadership is going to prevent an opponent from effectively applying various forms of information against the population and leadership, it must be able to control information flow across the Internet. Indeed, because the whole purpose of the Internet is to disseminate information, it constitutes a major challenge to central government efforts to maintain control, even as it helps to stimulate Chinese economic development by facilitating information sharing and access. Consequently, substantial sums and effort have been invested in controlling potential adversary access to the Chinese population and senior military and civilian leadership. These efforts coincide with a broader interest in maintaining control over the Chinese population, given the omnipresent risk of unrest. Managing this threat to regime control has therefore entailed highest-level attention and a multilayered approach.

Highest Political Levels Are Involved

The importance of controlling the Internet, as noted earlier, has involved various senior leaders in a range of different entities. These organizational gyrations reflect changes in Chinese priorities, whether in terms of relative emphasis accorded "informationization" versus broader economic modernization efforts or information security relative to other aspects of fostering informationization. It is also a result of the challenges posed by the dynamic nature of the information environment, as information technology has rapidly evolved.

Xi Jinping appears to have concluded that information security and control of the Internet will be a central priority for his tenure (through 2022). In February 2014, the latest iteration of these efforts emerged, "the Central Internet Security and Informationization Leading [Small] Group." This group, according to the Chinese press, "is designed to lead and coordinate Internet security and informationization work among different sectors [of the Chinese government], as well as draft national strategies, development plans, and major policies in this

field."[72] The group will develop comprehensive plans for policing cyber security, while promoting the broader use of information technology.

This leading small group is led by Xi Jinping himself, while Premier Li Keqiang and Liu Yunshan, both members of the Politburo Standing Committee, are his deputies, making the group the most senior ever established for informationization.[73] The official presence of three of the seven members of the Politburo Standing Committee reflects the priority accorded to its tasks.

Xi's remarks at the inaugural meeting of the group clearly expressed his concerns. Information security and informationization, he observed, were two aspects of a single whole, requiring unified planning, unified advancement, and unified implementation. Similarly, information security is an integral part of national security. "Without information security, there can be no national security."[74]

The General Office of the Central Internet Security and Informationization Leading Group is responsible for the day-to-day operations of the leading group, as well as preparing meetings, agenda setting, and so on. The director of that office therefore wields substantial authority in implementing Chinese policies on Internet security. Xi Jinping decided to appoint Lu Wei as the head of the general office. Significantly, Lu is also the head of the State Internet Information Office (SIIO), also known as the China Cyberspace Administration.

Lu's early career had largely been with the state-run Xinhua News Agency, where he had been bureau chief for Guangxi Province and later secretary-general and deputy director of the entire agency.[75] He then became vice mayor of Beijing (equivalent of being a vice governor) and head of Beijing's Municipal Propaganda Department. In 2013, he became the second head of the SIIO, which had been created by the State Council Information Office in May 2011, with responsibility for all Internet-related information activities. His career path paralleled his predecessor's at SIIO, Wang Chen. Wang had also risen through the ranks of the Chinese news media (although mainly *People's Daily,* rather than Xinhua). Both Wang and Lu therefore are intimately familiar with China's propaganda system and legacy information control organizations and procedures. As important, they had both long practiced controlling information flow.

By appointing Lu to this central position, Xi was making clear that Internet security would be closely enforced by state agencies, including the SIIO. When established, the SIIO was expected to streamline the various bureaucracies that oversaw the Chinese Internet. It was to "direct, coordinate, and supervise online content management, and handle administrative approval of businesses related to online news reporting," as well as "investigate and punish websites violating laws and regulations."[76] Senior SIIO members included a vice minister of public security, Zhang Xinfeng. The security role was sharpened when the State Council issued a circular in August 2014 announcing the

reauthorization of the SIIO. The circular noted that the SIIO's roles and responsibilities include the healthy and orderly development of the Internet, protection of the citizenry, and maintenance of national security and public interest.[77]

Current Internet Governance Is Challenged

One of the themes that Lu has repeatedly invoked, constituting the first layer of China's approach to protecting itself from the Internet, is the concept of Internet sovereignty. As Lu stated in 2014 at the World Economic Forum in Davos, "So we must have a public [international] order. And this public order cannot impact any particular local order."[78] Lu's comments reiterate Beijing's long-standing calls for extending national sovereignty across the Internet. For the Chinese leadership, only by altering the international Internet governance structure, revising underlying assumptions, and gaining acceptance of "Internet sovereignty" can China defend itself from Internet-borne threats to information control. By delegitimizing the free flow of information, Chinese authorities would justify efforts to control what information can flow across state boundaries and could even seek assistance from other states in constricting that flow.

From Beijing's perspective, determining who has a voice in managing the Internet is vital, as that can limit who can access the Internet. For the Chinese leadership, Internet governance is a reflection of national authority and power. The Chinese argue that Internet management should be limited to nation-states, reiterating this position in various official documents, such as the "2006–2020 National Strategy for Informationization Development" and the 2010 Chinese white paper on the Internet, as well as speeches by officials such as Lu Wei and Xi Jinping.

As important, the ability to authorize Internet names and addresses is also the ability to manage a strategic resource, since those names and addresses determine how one accesses the Internet (and how others access you). Given its importance, the ability to authorize Internet names and addresses cannot be left in the hands of foreigners.[79] Nor can it be lightly granted to nonstate actors who might challenge Beijing's authority.

There are a host of entities that the CCP has sought to mute and does not want to have unfettered access to the Internet. For example, it does not want to cede any kind of cyberspace naming authority to Taiwan. Indeed, one Chinese consideration about Internet governance is its desire to restrict the online voice of the authorities in Taipei, to ensure that they have no more prospect of international support in cyberspace than they do in the current political environment. As troubling for the CCP is the ability of groups such as the Tibetan government in exile or Falun Gong to voice adversarial positions and challenges to Beijing via the Internet.

This Chinese interest in preserving national sovereignty on the Internet, including maintaining control over how "China" is represented in cyberspace, has led to fundamental antagonism toward the current structure of Internet governance. When the Internet first began to grow beyond a handful of educational and governmental institutions, the United States vested its administration in the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit entity.

In order to reach a website, a computer user must enter an address in cyberspace. This address is a unique name or number (or combination). The ICANN staff administers the "domain name system" (DNS), which links the names of various websites, computers, and so on, with their numerical Internet protocol (IP) addresses. This includes authorizing and accrediting the highest-level lists of names, referred to as the "top-level domain" (gTLD) name registrars, who in turn can authorize other entities to grant names (and register them).[80] In essence, since its establishment in 1998, ICANN has had the authority to determine who can obtain the unique identifiers, or IP addresses, that allow others to access one's information on the World Wide Web.

ICANN policy has been grounded in the "multistakeholder" model. This system seats governments alongside other elements of global society, including academia, business, civil society (e.g., religions, nongovernmental organizations), and industry, managing the Internet as a whole through a consensus-based process. Individuals, as well as larger organized groups, are represented, none of them enjoying a privileged place at the table. The objective is to sustain the Internet as a borderless realm, where information flows freely.

Not surprisingly, the Chinese have opposed this multistakeholder approach, preferring a much more state-centered one. Ideally, from Beijing's perspective, Internet governance should be exercised primarily by governments, who would establish the rules for Internet activity, including the ability to apportion Internet addresses (and generally manage its activity) within their national borders. In short, state sovereignty would be extended to cyberspace. China objects to ICANN at a fundamental level—a state-centric governance model can hardly be managed by a nonstate actor, much less one that views other nonstate elements as coequals.

More practically, China has long had suspicions that ICANN is a creature of the United States. This has been exacerbated by ICANN's failure to accept Beijing as the sole legitimate voice for all Chinese-related entities—including Taiwan. The granting of a domain name (—.tw) to Taiwan implied that it was a separate entity, at least in cyberspace, from China (which has the domain name—.cn). The inclusion of Taiwan in the governmental committee (in effect treating it as a state) further alienated Beijing and resulted in Chinese boycotting of the ICANN "Governmental Advisory Committee" from 2001

to 2009.[81] Only when Taiwan's delegation was renamed as "Chinese Taipei" in 2009 did Beijing agree to send representatives to the committee.

Given these problems, the Chinese, as well as other authoritarian states such as Russia, have wanted to see Internet governance transferred from ICANN to the International Telecommunications Union (ITU), an agency of the United Nations. China formally proposed this at the 2005 UN-sponsored World Summit on the Information Society (WSIS). In September 2011, China and Russia, along with Tajikistan and Uzbekistan, submitted a proposal for an "International Code of Conduct on Information Security" to the UN Security Council that would enlarge the role of the ITU at the expense of ICANN.[82]

The submission was a clear attempt to shift Internet governance toward states. One clause, for example, sought to

> reaffirm all the rights and responsibilities of States to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack, and sabotage.[83]

This clause would justify restrictions on any dissident groups that governments (including Beijing) assessed as threatening their "information space." It would also ensure that entities such as Taiwan would not have their own domain name, except in the unlikely event that the governing state (i.e., China) would agree. As the proposal also noted, governments were to "lead all elements of society . . . to understand their roles and responsibilities with regard to information security."[84] The state, in short, would have "policy authority for Internet-related public issues," eclipsing all other players, unlike in the multistakeholder model. (An updated version, although still holding largely to the same points, was subsequently submitted in January 2015 by the original four states, now joined by Kazakhstan and Kyrgyzstan.[85])

Meanwhile, Chinese authorities have sought to undermine the multistakeholder approach in other ways. There are five Regional Internet Registries (RIRs), which help in the assignment of IP addresses. The RIRs (one each for Africa, Asia, North and South America, and Europe) are private not-for-profit corporations, like ICANN. Within the Asia-Pacific Network Information Center (APNIC) purview are several National Internet Registries (NIRs), intended to address unique national requirements. These NIRs are also authorized to issue IP addresses and register names, like the RIRs and ICANN in general.

The Chinese NIR, the China Internet Network Information Center (CNNIC), however, has sought to control the issuance of addresses within China, pressing Chinese companies and Internet service providers (ISPs) to go

through themselves, rather than through the APNIC. In 2004, Houlin Zhao, the then director of the ITU's Telecommunications Standardization Bureau, pushed for national authorities to manage the allocation of at least a portion of the new IPv6 (Internet protocol version 6) addresses, rather than relying on the RIRs.[86] Zhao, who has since risen to secretary-general of the ITU, acknowledges that he has a different vision for Internet governance, noting that ITU is often seen as pursuing a more top-down approach.[87]

Domestic Legal Controls on the Internet

In addition to seeking to modify the international Internet governance structure, the Chinese have been steadily creating a domestic legal and regulatory framework that firmly extends the state's grip over all parts of China's internal cyber community. This effort began almost as soon as China linked to the Internet, and even before commercial access was made available to the broader Chinese public. In February 1994, the State Council issued State Council Order 147, "Regulations for the Safety Protection of Computer Information Systems." This vested the Ministry of Public Security (MPS) with responsibility for supervising computer information in China.[88] This was further supplemented by State Council Order 195, issued in February 1996, which listed specific Internet governance regulations. Beijing has since issued an array of regulations, laws, and directives discouraging "inappropriate" use of the Internet and its information.

In December 1997, the MPS issued regulations for computer network use relating to preservation of social order and stability. These regulations included provisions that forbade individuals from using the Internet to jeopardize Chinese national security, to "harm the interests of the State, of society, or of a group" or to tamper with computer information networks and the data residing therein. The regulations also bar using the Internet to create, replicate, retrieve, or transmit information that:

- Incites resistance to the Chinese constitution, laws, or administrative regulations;
- Incites overthrow of the government or socialist system;
- Incites division of the country or harms national unification;
- Incites hatred or discrimination among nationalities or harms their unity;
- Distorts the truth, spreads rumors, or destroys social order;
- Promotes feudal superstitions, sexually suggestive material, gambling, violence, or murder;
- Furthers terrorism, incites others to criminal activity, or openly insults or slanders other people;

- Injures the reputation of state entities; or
- Promotes other activities that violate the constitution, laws, or administrative regulations.[89]

This range of prohibited activities encompasses such potential avenues for political warfare as advocating independence for Taiwan, Tibet, or Xinjiang; engaging in religious proselytization (which might destroy social order or promote "feudal superstition"); or criticizing elements of the government (injuring the reputation of state entities).

Three years later, the Chinese National People's Congress (NPC), the national legislature, issued the "Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security." In the interests of "promoting what is beneficial and eliminating what is harmful," while preserving state security, the 2000 decision (effectively a law) delineated what constituted criminal activity in the realm of computer activities. As with previous regulations, the first section of the law again emphasized the importance of information security. It prohibited such acts as "invading the computer data system of State affairs, national defence [*sic*] buildup, or the sophisticated realms of science and technology," intentionally spreading computer viruses or otherwise adversely affecting the normal operations of the state's computer networks.

In addition, the decision made clear that criminal acts that threatened the security of the state or social stability were also punishable. Such acts included using computer networks:

1. To spread rumors, libels, or publicize or disseminate harmful information to whip up attempts to subvert state power, to overthrow the socialist system, or to split the country and undermine unification of the state;
2. To steal or divulge state secrets, intelligence, or military secrets;
3. To stir up ethnic hostility or discrimination and thereby undermining national unity; or
4. To form cult organizations or contact members of cult organizations and obstructing implementation of state laws and administrative regulations.[90]

Supplementing earlier MPS regulations, the NPC decision also dictates that using computer networks to violate the administration of public security even if it "does not constitute a crime shall be punished by the public security organ."[91]

Additional government policies supplement and refine Chinese information security policy by specifying standards and requirements for Chinese information security management and systems. In 2003, the "National

Coordinating Small Group for Cyber and Information Security" promulgated "Document #27" (presumably denoting the 27th official document this group issued in 2003), formally entitled, "Views of the Leading Small Group Regarding the Strengthening of Information Security and Safeguarding Work." This document reportedly marked the first time that information security was explicitly incorporated into planning for economic development, social stability maintenance, safeguarding national security, and strengthening cultural development.[92]

The "Multi-Level Protection Scheme" (MLPS) was laid out in 2007 in the "Methods of Tiered Protection and Management of Information Security," or Document #43 of that year.[93] This was issued jointly by the Ministry of Public Security, the State Secrecy Bureau, the State Cryptography Administration, and the State Council Information Office. The MLPS reflects senior-level interest across multiple bureaucracies in ensuring that Chinese information security software remains firmly in the hands of Chinese-owned companies. According to the MLPS, a variety of governmental and nongovernment entities deemed central to national security or strategic interests can only use information security products that originate in China. These entities included banks, transportation, and energy firms, as well as state agencies associated with customs, commerce, telecommunications and broadcasting, or national security.[94] It now also includes Chinese ISP firms.

In 2010, the Chinese began to send inspectors to the field to verify compliance with the MLPS. Non-Chinese firms such as Microsoft reportedly have had their access to the Chinese market extremely curtailed. The restrictions on outside access may have been motivated in part by the desire to create a protected market for China's information security firms, but it also restricted a potential line of vulnerability by limiting foreign ability to reach Chinese computers.[95] In 2012, the State Council issued "Several State Council Views on Emphasizing and Pushing Informationization Development and Realizing the Safeguarding of Information Security" (also referred to as "Document #23"). This document again emphasized the need to strengthen information and network security, especially for government information systems.[96]

Chinese efforts to restrict foreign access likely gained impetus after the 2013 revelations about American cyberespionage by Edward Snowden. In 2014, the Chinese government reportedly excluded foreign antivirus companies Symantec and Kaspersky from bidding on Chinese government contracts.[97]

Central government efforts to control information flow are not solely aimed at users. ISPs, cybercafes, and other access providers are also closely scrutinized. The State Council has issued various regulations to govern online businesses. ISPs and Internet content providers (ICPs) were licensed by the

Ministry of Information Industry (MII), and now by the Ministry of Industry and Information Technology (MIIT), which absorbed MII in 2008. ISPs are also expected to adhere to the "Public Pledge on Self-Discipline for China's Internet Industry" and are "encouraged" to join the Internet Society of China, a governmentally backed "nongovernmental organization," which disseminates the latest guidelines on censored topics, terms, and so on.[98]

These entities and pledges help promote "self-regulation." Private companies such as ISPs are expected to enforce legal requirements, whether use of Chinese software for information security or monitoring their own traffic and networks for dangerous or malicious behavior. ISPs, cybercafes, and other providers are responsible for ensuring that all users register with their real names, a centerpiece of many Chinese efforts to limit anonymity on the Chinese Internet. At the same time, as will be discussed later in this chapter, ISPs are also part of the human censor network that backstops technical censorship methods.

As cybersecurity is more explicitly linked to national security, pressure on these companies will grow. Article 25 of the 2015 Chinese National Security Law specifies that the state's national security responsibilities include maintaining national network and information security, stopping "unlawful and criminal activity," including "dissemination of unlawful and harmful information," as well as "maintaining cyberspace sovereignty, security, and development interests." It specifically includes national security reviews and oversight management of "Internet information technology products and services."[99] The censors employed by many ISPs and other cyber companies are kept busy by these requirements.

Meanwhile, the Chinese cybersecurity law that came into effect on January 1, 2016, will further complicate matters. This legislation will not require foreign companies to keep local user data in China and did not require installation of government-accessible backdoors in software (as had been proposed in earlier drafts). It *does* require all telecommunications and Internet companies doing business in China to cooperate with Chinese law enforcement and security organizations. This includes controlling information flow in defense of cyberspace sovereignty, as well as information network security and development efforts. The legislation requires all companies to provide "technical assistance," including decryption of user data, in support of "counterterrorist" activities.[100]

Technological Means of Limiting Access

While Chinese diplomats strive to extend national sovereignty to cyberspace and Chinese legislators and party officials design legal controls over domestic Internet behavior, Chinese engineers have sought to technologically limit and monitor data flowing into China. This is facilitated by Beijing's limiting connections to the broader global information networks

(and therefore global access into China). Fiber-optic cables enter China at only three points—the Beijing–Tianjin region; Shanghai; and Guangzhou. There are only a limited number of Internet exchange points (IXPs) running via these cables, most controlled by the Chinese government. This leads to congestion and a slower Internet speed for Chinese users accessing the outside world but eases the government's ability to monitor traffic entering and leaving China.

As important, the Chinese government has long supported research in additional programs and measures that limit information flow. The 2000 decision on preserving computer network security charges the government at all levels to "support research and development of the technology for computer network security and enhance the ability of maintaining security of the network."[101] A high priority has been filtering foreign content, in terms of not only what outsiders can send into China but also what Chinese netizens can access.

A centerpiece of this effort is the "Great Firewall of China" (GFWC). This "on-path" system is the first line of technical defense, monitoring traffic across the three portals that link the Chinese portion of the Internet to the rest of the world. It also has some capacity to monitor internal Chinese computer activity, although this is sometimes conflated with the "Golden Shield" project, which is more focused on monitoring domestic Chinese online behavior. The avowed purpose of the GFWC is to keep outsiders from being able to attack Chinese Internet users. In reality, the GFWC has demonstrated an ability to censor websites and even individual web pages and images, limiting Chinese citizens' ability to access the global Internet. Theoretically, the GFWC could shut down connectivity between China and the rest of the global Internet entirely, if necessary.

The GFWC employs a variety of methods to prevent Chinese netizens from accessing information that might contradict or challenge the government's preferred line. IP addresses may be blocked, or attempts to connect to them may be misdirected. In addition, in a different application of typical intrusion detection systems, the GFWC undertakes data inspection and filtering to examine uniform resource locators (URLs), or web addresses, as well as the numeric IP addresses. It can also examine actual content, in order to more precisely filter out individual web pages and images.

The GFWC's purpose is not simply to block content and limit access to forbidden sites; it also seeks to make such content and access more complicated and frustrating, so that users will avoid them. Thus, the GFWC typically tries to limit the degree to which its censorship is noticeable to the average user. While the GFWC will block access to some websites (or even individual pages or images), it does not necessarily interfere with access to other parts of the Internet. A user may therefore not realize that his or her search has been blocked but may instead assume that a website is no longer operating or is being modified.

The GFWC is meant to complement various other measures, such as real-name registration and human censors, as well as broader laws and pronouncements regarding unacceptable or dangerous behavior (not just online), to discourage efforts to access forbidden information. It is estimated, for example, that less than 10 percent of China's netizens engage in political discourse on the Internet at all.[102] Although this remains an enormous number (since China has over 500 million users), this makes censorship and information control more manageable.

HOW THE GREAT FIREWALL OF CHINA WORKS

For a Chinese user seeking to access a foreign website, his or her computer must connect with a domain name server (DNS), which will seek out the desired Internet protocol (IP) address. The IP address is the unique 32-digit (in IPv4) or 128-digit (in IPv6) "location" on the Internet.

The DNS server, in turn, will either provide the address or query other authoritative name servers for the desired location of the specific IP address. This information will then be transmitted to the Chinese user's computer. A query may have to travel through several layers of domestic servers to reach one of the three international exchange points (the portals where China's Internet links to the broader, global structure).

In China, authoritative name servers and DNS servers are run by either Chinese companies or the government. As such, they are incorporated into the Internet filtering process that constitutes the Great Firewall of China (GFWC). These filters employ similar software to security firewall programs. But where other firewalls are designed to detect malicious software and efforts to infect computers, the GFWC is intended to detect and halt dangerous ideas and information.

The GFWC is also different from most firewall systems because it is an *on-path* system. Most firewalls are an "*in-path* barrier between two networks: all traffic between the networks must flow through the firewall."[103] The GFWC, on the other hand, "mirrors" inbound and outbound data packets to what are believed to be separate clusters of government-run computers, reassembling the data to some extent, in order to examine their destinations and even their content. The GFWC then employs several methods to keep China's population insulated from potentially dangerous information.

- *Blocking IP addresses*. One of the most basic methods for the GFWC to limit access is to prevent a user's computer from connecting to a given IP address. The GFWC retains a list of banned IP addresses. When a user seeks to connect with one of these at a foreign server, the GFWC refuses to allow it through the intervening connections.

  The social media site Facebook, for example, has a website, facebook.com, which is located at a given IP address, which is known and fixed. Any effort to connect to that address will be broken automatically by the GFWC. This is similar to how parental controls work and is common to many commercial firewall programs.

- *Misdirecting IP addresses.* This is also known as "DNS poisoning." In some cases, the Chinese may not forbid access to a given IP address but may misdirect a connection attempt instead. In order for a query to reach its destination, it must have a proper address. Thus, the DNS and authoritative name servers are expected to have up-to-date address lists in order to route messages to their proper destination. With the GFWC, however, China's various name servers will either withhold an answer when queried or give an incorrect answer. The querying computer will be directed to a different website's IP address or to a warning page (e.g., a page stating that the query is into a sensitive area).
- *Data inspection and filtering.* This is also known as "deep packet filtering." The Chinese authorities not only examine requests to connect (which typically require one data packet) but also the responses, by reassembling response packets. Thus, in many cases the GFWC can examine the contents of web pages and block pages based on that content rather than the IP address. Similarly, in some cases the GFWC has been even more precise, filtering out certain web pages or certain images, rather than blocking an entire website. The GFWC has also demonstrated that it can censor pages based on URLs or address name if it contains forbidden terms, such as "Falun Gong," the banned religious movement (which the Chinese characterize as a cult).

While the GFWC may sometimes simply prevent a connection between a Chinese requesting computer and a foreign website, at other times, it may disrupt the connectivity through other means. Some of these methods involve the transmission control protocol (TCP). Whereas the IP deals with data packets, the TCP essentially is the means by which programs exchange those data packets and establish network conversations. The TCP, in conjunction with the IP, defines how computers will communicate with each other (hence the commonly used abbreviation TCP/IP).

When a banned IP address is requested, the GFWC will sometimes drop the request (blocking the address) and substitute a series of false "TCP Reset" packets. The GFWC essentially informs the requester and the destination computer that the request could not be completed or was in error. By indicating to requester and destination that he or she has "dialed a wrong number," the GFWC causes the request to be rejected, breaking the connection. If the user persists in making the same request, the GFCW automatically blocks him or her and may do so for up to an hour.

Another TCP-related method for disrupting communications is for the GFWC to send data packets (which it has already intercepted) to the foreign-sourced website out of sequence. The foreign site, receiving requests that appear to be out of order, then cannot synchronize valid server requests that are arriving at the same time as the invalid (i.e., out of sequence) requests from the GFWC.

Not surprisingly, a number of efforts have emerged to try to circumvent the GFWC, which in turn have led to Chinese government counter-countermeasures. For example, Chinese and foreign computer users have tried to foster "virtual private networks" (VPNs) to allow less fettered access to the global Internet. VPNs establish secure connections between a user's computer and

a separate network, so that the user's computer is treated as though it were part of that local network (even if it is physically separated). One can then access any information that the local network might contain.

VPNs are often set up by large companies to allow widely separated locations to share files and access each other's data. Through "tunneling protocols," they can establish secure links even in the face of blockages, such as those imposed by the GFWC. VPNs have been of particular interest to foreign companies that have subsidiaries in China; establishing a VPN can help make internal communications more secure.

A VPN not only allows sharing data that resides on the network but also allows users access to anything that the network can "see." For Chinese users, a VPN provides a potential link to the broader Internet outside China. By joining a commercial VPN provider, they can link to that provider's network located outside China, which would then provide access to Google, Facebook, and other sites that are currently blocked by the GFWC.

Chinese authorities began to develop tools to crack down on the use of VPN as soon as they began to gain popularity. Some commercial VPN sites were entirely blocked. Another counter to established VPN connections was emplaced in 2012, with updates to the GFWC allowing it to "learn, discover, and block VPN protocols automatically."[104] It is believed that, through "deep packet inspection," the GFWC can at least determine whether packets are encrypted, even if their content remains inaccessible to the censors. If a substantial amount of encrypted traffic is detected bound for a particular network, the GFWC may then block that path.

By 2014, commercial VPN companies that serve Chinese clients reported even more extensive interference with their services.[105] Whereas earlier versions had blocked OpenVPN, the least sophisticated tunneling protocol, further upgrades to the GFWC are now apparently affecting more advanced tunneling protocols, such as PPTP (Point-to-Point Tunneling Protocol) and SSh2 (Secure Shell-2), making it ever harder to establish and maintain VPN connections through the GFWC.

Supplementing the GFWC is the additional layer of surveillance imposed by the "Golden Shield" project. Managed by the Ministry of Public Security, this is a nationwide digital surveillance network that correlates Chinese citizens' online behavior with information obtained via other means such as telephone monitoring and closed circuit television feeds, citizen tax data, and purchasing habits (derived from monitoring credit card use and other electronic monetary transfers). The goal is to provide both local and national authorities with a complete profile on any persons of interest.

The GFWC, supported by human censors, operates at the network level. The Chinese authorities, however, have also sought to extend their reach to the level of individual computers. In 2009, the Chinese leadership attempted

to require the installation of "Green Dam" software on all computers sold in China. The program would use a combination of image recognition technology and text filtering to limit access to "vulgar" sites and images. While ostensibly intended to protect children from pornography and other adult sites, according to one study, "Green Dam" software would in fact block access to religious and political sites. More important, it would embed itself deep within the computer's operating system and actively monitor "individual computer behavior, such that a wide range of programs including word processing and email can be suddenly terminated if content algorithm detects inappropriate speech."[106] This would have effectively extended Chinese censorship to individual computers and affected many programs that were beyond the reach of the GFWC. For example, Green Dam could prevent users from accessing or transferring information via CDs, DVDs, or flash drives/memory sticks by stopping the computer from reading such media.

The requirement that all personal computers sold in China incorporate this software was extremely controversial, and even Chinese state media questioned the viability of this program (including whether it would be reliable or would interfere with other programs).[107] The decision was eventually rescinded, but the concept is indicative of Chinese officials' desire to technologically control and constrain access to information.

Human Censors Supplement Censorship Efforts

In addition to the automated censorship of the GFWC and the "big data"–based surveillance provided by the "Golden Shield," there is a human element in Chinese efforts to control the Internet. Those Chinese citizens who wish to circumvent the Golden Shield of domestic Internet surveillance, as well as the GFWC, have shown a facility in finding ways to bypass the automated censor systems. Discussions of the Tiananmen massacre, which occurred on June 4, 1989, for example, have sometimes included references to May 35th, April 65th, and March 96th.[108] By avoiding specific reference to "six-four," that is, June 4th, such references could avoid detection by the algorithms put in place.

Such efforts are facilitated by the plethora of homophones in Chinese. An entire lexicon of such terms has emerged, including "river crab" (a homophone for "harmony," a long-standing CCP-touted virtue) and "grass mud horse" (a homophone for a crude sexual act involving one's mother), as Chinese netizens express unhappiness with various policies or lampoon government figures.

Moreover, global developments can create subversive concepts and memes more rapidly than automated algorithms can adjust. When the Arab Spring exploded in 2011, the government was forced to rapidly censor terms such as "jasmine," a symbol used by various Middle East protestors.

Recognizing that human ingenuity, coupled with current events, is likely to outpace automated search systems' ability to curtail dissemination of forbidden information, the Chinese authorities have created a network of human censors to further enforce restrictions.

The human censorship effort relies heavily on the ISPs. Because the Chinese government holds to the position of "intermediary liability," that is, "one is responsible for what one publishes," Chinese ISPs are incentivized to limit potential posting or discussion of forbidden topics.[109] As a result, not only have most ISPs installed various filtering systems to detect (and eliminate) sensitive words and phrases, but they also field teams of employees and volunteers who monitor chat rooms, review blogs and web pages, and otherwise help ensure that what is published via the ISP does not trouble the authorities.[110]

These, in turn, are supported by the government's own cyber police. In 2004, this was estimated to already number some 30,000 members.[111] A decade later, reports suggest that China may have 100,000 to two million government censors, tracking both Internet and social media (including microblog) posts and comments.[112]

Government Control of Social Media

The rise of social media poses an additional problem for Chinese efforts to control information flow and dissemination. The proliferation of video and photos further expanded the forms of information now available, while enhancing its credibility. Indeed, social media have become a major part of the Chinese information environment, as much of China's netizenry accesses the Internet via mobile phones and social media platforms. Chinese microblogging sites such as Sina Weibo, Sohu, and Tencent, the PRC counterparts to Twitter, have 200 million subscribers.[113] They are the "primary space for Chinese netizens to voice opinion or discuss taboo subjects."[114] Not surprisingly, this has led to a range of additional controls on information dissemination.

In 1999, China reorganized its telecommunications organization and began to offer cell phone services. By 2004, Chinese were opening up five million new cell phone lines every month, totaling some 350 million cell phone users by the next year.[115]

The proliferation of cell phones allowed China to rapidly modernize and expand its communications networks, without having to invest massively in physical (copper or fiber-optic) telephone lines. At the same time, it also created a new form of connectivity, through text messages. Chinese cell phone users transmitted some 200 billion text messages (SMS, or "short message service") in 2003, averaging 651 per user, at a rate of nearly 7,000 per second.[116] For Chinese authorities, the introduction and rapid proliferation of

cell phones, and the consequent ability to employ text messaging, constituted a major new challenge to controlling information flow.

Indeed, even as this new communications form was taking off, Chinese authorities realized that it constituted a major threat to the state's monopoly on information and its dissemination. This was highlighted by the 2002–2003 severe acute respiratory syndrome (SARS) crisis in China. "While China's government-controlled media was prohibited from reporting on the warning, the news circulated via mobile phones, e-mail, and the Internet."[117] Information propagated far faster than central authorities intended—which meant rumors and misinformation spread rapidly as well. Public confidence in the government rapidly eroded, exacerbated when Dr Jiang Yanyong, a retired military surgeon, e-mailed two Chinese TV stations that the Chinese health minister was lying when the latter declared SARS was under control in the PRC. While the Chinese news media did not report on Dr Jiang's comments, his views were reported in the foreign press, from which it rapidly disseminated back within China.

Although the PRC eventually got SARS under control, central authorities now recognized that social media and cell phones constituted a major threat to governmental information control. This led to several efforts to reestablish tight control over these new forms of information dissemination. By July 2004, barely four months after Dr Jiang's e-mail, Chinese authorities were already policing the cell phone system, fining and shutting down cell phone providers who were not monitoring text messages passing over their systems.[118]

The Chinese leadership appears even more worried about how social media had been exploited by forces for political and social change abroad. Beginning with the "Rose Revolution" in Georgia in 2003, and the subsequent 2004 Ukrainian "Orange Revolution" and 2005 Kyrgyz "Tulip [or Pink] Revolution," a number of former Soviet republics underwent political upheaval. In all of these "color revolutions," popular forces demanded democracy and more representative government. Other protests rocked Serbia and Lebanon. Many protests in these countries were organized through social media such as e-mails and text messages. This new form of communications allowed organizers to address large groups simultaneously, a vital tool for rapidly creating demonstrations and other public challenges to regime authority.

By contrast, governmental crackdowns in the face of public protests were often ineffectual, since governments in Cairo and Tunis could not control the social media networks that protestors were exploiting. Companies such as Twitter and Facebook were based abroad, and not vulnerable to local pressure. Moreover, governments could not cut off access to social media without also affecting their own connectivity to the global Internet.

To stem such possibilities, the Chinese have extended the comprehensive array of countermeasures against the free flow of information to various social

media networks. Rather than eliminating all social media, as in North Korea, the Chinese leadership has redirected the public's access to domestic companies, excluding foreign platforms.

The Chinese control of popular access to social media was amply demonstrated in 2009, as wholesale restrictions were placed on YouTube access. While only individual YouTube videos had previously been blocked, the Chinese now claimed that the service had posted fake videos of monks being beaten in Lhasa, Tibet, and therefore was undermining Chinese internal security.[119] Since then, the government has largely restricted access to YouTube; other foreign social media sites were soon similarly excluded from the Chinese market.

The Chinese authorities did not try to deny the Chinese people the benefits of social media, such as video sharing, however. Instead, they channeled popular demand for social media and attendant opportunities for information exchange and access toward domestic companies, programs, and platforms. Even as the GFWC blocked access to foreign social media programs such as Facebook and YouTube, domestic counterparts were allowed to rise in their stead. Initial efforts at such "electronic import substitution" began in the late 1990s and had begun to bear fruit by 2000. Just as China's physical information networks would be built from Chinese equipment, China's appetite for social media would be met by Chinese companies.

Today, Chinese computer users search the Internet with Baidu, instead of Google. They share videos through Youku, rather than YouTube, and they don't Tweet but microblog across Sina Weibo and Tencent. Chinese online shoppers browse Taobao and pay with Alipay. All of these products and platforms are managed by Chinese companies, and while the companies may not be state owned, they clearly cooperate with censors and submit to broader government control, much like the commercial news media in China. Indeed, as Weibo's public filings at the time of its initial public offering (IPO) noted, failure to comply with government demands for censorship "may subject us to liabilities and penalties and may even result in the temporary blockage or complete shutdown of our online operations."[120] Consequently, should the Chinese public try to organize themselves as Middle East populations did during the 2009 Iranian Green Movement, 2010 "Jasmine Revolution," and 2011 "Arab Spring," the Chinese authorities have the ability to mute and neutralize such efforts.

The Chinese response to various critical incidents has demonstrated these capabilities. In 2008, riots in Tibet led to restrictions on local Internet access and text messaging. Greater restrictions were imposed on Xinjiang after ethnic unrest turned deadly in July 2009. The government claims some 200 died and nearly 1,400 were injured in various riots and demonstrations.[121] Officially, the Chinese government stated that the "terrorists used the Internet and SMS messaging."[122] Chinese authorities promptly shut down all Internet and

mobile text messaging in the region, yet maintained cell phone connectivity. This separation of functions had been engineered into Chinese telecommunications networks.

This nearly total information blockade lasted for several months, and it was not until the following May that full Internet and SMS was resumed. Subsequent Uighur-related incidents, however, such as the 2013 attack in Tiananmen Square, the 2013 outbreak of rioting in Turpan Prefecture, Xinjiang, and 2014 incidents in Kashgar Prefecture, Xinjiang, led to the prompt reinstitution of these information blackouts.

Tight controls on social media are not only imposed due to ethnic unrest, however. In 2012, when Chongqing party secretary Bo Xilai was rumored to be organizing a coup attempt against the central government, Chinese media companies Tencent Holdings (which manages QQ and WeChat) and Sina Corporation (which manages Weibo) both shut down their commenting functions to limit any discussion.[123] In November 2014, when the U.S. embassy in Beijing began providing regular readings of air pollution on its grounds, often contradicting official claims of clear skies and clean air, Chinese smartphones stopped linking to that information.[124]

More seriously, in 2014, Hong Kong residents protested when Chinese authorities appeared to be reneging on their pledge to allow universal suffrage in local elections. Beijing chose to interpret Hong Kong's Basic Law (the local equivalent of the Constitution) as allowing the people of Hong Kong to vote for their local government, *but* allowing Beijing the ability to determine who could qualify as a candidate for those votes. The result was the "Occupy Central" movement, as students and civic leaders protested Beijing's decision.

This, in turn, led to widespread censorship of news about Hong Kong on Chinese social networks and further restrictions on access to foreign programs and apps. Instagram, the Android-based photo-sharing system for cell phones, was suddenly inaccessible in China. At the same time, Sina Weibo's microblog and Tencent's WeChat began to delete references to Hong Kong demonstrations and Occupy Central gatherings.[125]

Such draconian steps of openly shutting down parts of the social media infrastructure seem to be invoked primarily in crises. For day-to-day oversight, Chinese authorities rely more on an overlapping array of measures that are less overtly intrusive but that shape and mold users' experiences. Much of this is implemented by social media sites, rather than the government per se. On Sina Weibo, one of the main Chinese microblogging sites (comparable to Twitter), this array of mechanisms includes prophylactic, near-real-time, and retroactive measures.[126]

For Sina Weibo users, many search terms are simply not accessible via that platform. The company maintains a list of search terms that is prohibited for all users, which means that information flow across Sina Weibo is constrained

from the outset. It is not clear as to who determines which terms are off-limits, although the Central Propaganda Department almost certainly plays a major role, in conjunction with service providers and various other government agencies.

As with Internet censorship, social media are then subjected to an array of additional controls, complicating and frustrating attempts to propagate dangerous or forbidden information. Subscribers who seek to post comments on sensitive topics (which change in light of broader news, social, and political developments) are subjected to an array of near-real-time measures. These can take effect within minutes of items being posted. One test saw some items deleted within 8 minutes, and one-third of questionable content deleted within 30. Over 90 percent had been deleted within 24 hours.[127]

Some of the measures include:

- *Explicit filtering*. If a Weibo user tries to post comments that touch on sensitive topics or content, he or she receives a message warning that the content violates Weibo's rules or government rules.
- *Concealing or camouflaging posts*. Weibo will appear to post items, so that only the posting user, but no one else, will see it. No indication is given to the posting user that the message has not gone to a wider audience.
- *Implicit filtering*. Weibo employs its own group of censors, with one senior company official acknowledging at least 100, but other reports suggesting as many as 700.[128] These censors will apparently manually check some items; users posting items that are being examined may be informed that a review is under way. Some of the posts are eventually posted, while others are not.

The implicit filtering approach is striking, since it indicates that a significant part of Chinese social media censorship still relies on human intervention. Chinese willingness to devote significant manpower to such a task (e.g., to monitor even a fraction of the billions of microblog comments a year) reflects the seriousness with which the government views social media oversight and censorship.

To ease the burden and make more efficient use of their censors, Chinese social media companies try to exploit the larger pool of subscribers to help police their information flow. Since May 2012, for example, Sina Weibo has offered "user credit" points to community members who report sensitive, inappropriate, or rumor-based postings to administrators. This, in effect, alleviates the pressure on full-time censors by adding tens of thousands of additional informal watchdogs, who can then cue formal censors for specific action.

These steps may be undertaken in conjunction with the imposition of additional restrictions on users. Some users, especially ones who often raise

sensitive or censored topics, are subjected to additional review of their comments and posts. It is not clear, though, as to whether this is a policy or is imposed episodically. In some cases, a user may even be dropped entirely. During one analysis, nearly 10 percent of 3,500 observed user accounts were closed over two months (although not necessarily for political or even censorship reasons).[129]

These near-real-time filtering measures allow Sina Weibo and presumably comparable ones at other Chinese social media platforms, to restrict the flow of information on key subjects and terms, and to limit certain posters' impact. In addition, there are supplemental procedures in place to further constrain the flow of undesirable information that might leak through. Posted items are subsequent reviewed and removed if necessary. Such retroactive measures include "backward keyword search" and "backward reposts search."

Backward Keyword Search

Sina Weibo censors apparently regularly review messages to see if they contain words or phrases that had not been recognized as sensitive when posted. Because the Chinese language contains many homophones, posters can employ various phrases and characters that might not, in and of themselves, trigger deletion by automated programs but which a human would recognize. This is an updated computer version of a long-standing form of protest in China. In the days before Tiananmen, for example, some people deliberately broke small glass bottles in public spaces because Deng's given name, "Xiaoping," is a homophone for "little bottle." Thus, protestors were "breaking Deng" by breaking bottles.[130]

Researchers examining Weibo post deletions found that many posts that contained a newly restricted phrase (e.g., a homophone for "celestial empire" (*tianchao*; 天朝), itself a phrase intended to reference the government) were deleted. These deletions were made not only on the day the phrase was discovered (or recognized as derogatory) but from earlier days as well. In essence, those earlier posts were removed from the records so that no search would detect them. Another example noted that posts from two to five days preceding a decision to censor a given phrase were all removed, often within five minutes of each other. "Those 44 posts are from different users, have no common parent posts, and have no common pictures. The only plausible explanation for this concentrated deletion would appear to be a keyword-based deletion."[131]

Backward Reposts Search

According to several studies, not only are individual posts deleted when they touch on sensitive topics or terms, but *associated* posts are often also deleted as well. This occurs within a remarkably short time; "in our deleted posts

dataset over 82% of reposted posts have a standard deviation of less than 5 minutes for deletion time."[132] This means that, like in Oceania in George Orwell's *1984*, not only are certain items deleted from the record, but all reference and associated posts are deleted as well, in effect creating "uninformation." This makes it much more difficult, if not impossible, to detect that such a post had ever existed.

For the Chinese leadership, the ability to monitor information and control its flow is an essential prerequisite for waging informationized warfare. It is the foundation for establishing information dominance and involves both offensive and defensive actions. Offensive actions include political warfare measures to define and influence how others perceive events, personalities, and positions. Defensive efforts justify enormous expenditure of human and financial capital, as they prevent adversaries from exploiting a major vulnerability.

4 Chapter

Information Warfare: Waging Information Campaigns in the Next War

While informationized warfare applies information to all aspects of modern warfare, and extends the concept of warfare to such arenas as the legal and public opinion realms, the PLA will also engage in "information warfare" (*xinxi zhan;* 信息战). This is the struggle for information dominance within the more traditional military arena. Indeed, some Chinese analyses conclude that information warfare is the main operational form of informationized warfare, directly affecting all other combat activities and goals.[1]

Information warfare entails specific efforts by the PLA to secure information dominance over the adversary's military forces. This emphasis on information dominance arose as the military gained greater exposure to joint operations, which the PLA has assessed as central to future wars. Indeed, information is intimately linked to China's understanding of joint operations, which will be a central part of fighting and winning future "local wars under informationized conditions."

The PLA's conception of joint operations has shifted from multiple, individual services operating together in a coordinated fashion in the same physical space to unified operations under a single command-and-control network. This focal shift corresponds to a comparable shift in the assessed importance of information. According to PLA analyses, successfully conducting joint operations at the campaign level elevates information's role to the same level as forces, time, and physical space as key, objective factors. Information is how participating forces relate to each other, as well as to time and space.[2]

GROWING EMPHASIS ON JOINT OPERATIONS

As noted in Chapter 2 ("Not Your Father's PLA"), the PLA began to focus on joint operations beginning in the mid-1990s, and codified this growing

emphasis on joint operations in the new operational regulations and platform promulgated in 1999. These new doctrinal documents are believed to have covered operational-level planning for the various services, as well as joint, interservice campaigns.

As the PLA increasingly trained for joint operations, however, its efforts to synergize encountered new challenges. The PLA realized that simply bringing forces into physical proximity, even under a single command structure and a single plan, provided only the most basic level of jointness. Chinese joint exercises of the early 2000s saw a steady increase in sophistication, as the military sought to improve the level of coordination.

The PLA had foreseen this. Its own writings demonstrate an understanding of different degrees of jointness and recognition that it had only undertaken initial forays. One Chinese article likened the process of increasing jointness to three eggs and a bowl. The first developmental phase was simply to put three eggs into a bowl. The second phase would see three eggs broken into a bowl. The third phase was to break three eggs into a bowl, and then scramble them.[3] As the PLA expanded its training efforts toward the equivalent of breaking three eggs into a bowl, going beyond physically placing forces together to forces actually *interoperating*, the requirements for success changed.

The first evolution was realizing that joint operations would be the norm in future "local wars under informationized conditions (*xinxihua tiaojian xia jubu zhanzheng*; 信息化条件下局部战争)." As the second edition of the PLA textbook *Science of Campaigns* observes, "In future local wars under informationized conditions, service-focused campaigns will be *subordinate to the joint campaign*."[4] The PLA reassessed the nature of future conflict, and how it should adjust its operating concepts.

The PLA subsequently overhauled its approach to jointness. According to one PLA analysis, the "unifying" (*yitihua;* 一体化) of PLA joint operations has four aspects:[5]

- The creation of a "unified operational theory" (*zuozhan lilun yitihua*; 作战理论一体化), in which different services share common operational concepts. Without a "unified, or consolidated, set of regulations" (*tongyi de tiaoling;* 统一的条令), different services' formations cannot act in a "unified, or consolidated, manner" (*tongyi xingdong;* 统一行动).
- A unified operational theory, in turn, requires "unified command" (*zhihui yitihua*; 指挥一体化) for implementation. Coordination cannot only involve highest levels and then rely on services implementing along their own lines. Instead, improving Chinese jointness required an appropriate "command system" (*zhihui tizhi;* 指挥体制) over all forces, capable of planning and executing operations across service lines.

- The unified command system can only manage joint operations through the creation of a "unified C3I system." This system links all participating forces together, not only at the top but throughout the chain of command.
- This unified command structure and C3I system creates "unified knowledge" (*zhishi yitihua*; 知识一体化). That is, it creates common situational awareness, as well as mutual understanding of each service's perspectives and approaches to warfare.

The earlier concept of coordinated joint operations had already brought together different forces under a single operational plan, with a single command-and-control structure. Since joint operations were the exception, though, the joint command-and-control structure was still not permanent. Moreover, forces operating in coordinated joint operations remained service oriented, brought together only for a specific operation. As a result, such joint operations were ultimately only additive. More forces (from different services) were brought into the same physical space, but synergies were limited. The result was "jointness in form but not in actual capability" (*xing ju er neng bu ju*; 形聚而能不聚).[6]

As the PLA increasingly planned and practiced joint operations throughout the 1990s and 2000s, it realized that maximizing synergistic effects requires more than just the ad hoc convergence of various forces. Instead, Chinese forces would have to integrate and meld with each other, forming a truly unified system-of-systems whole. If successful, effects would be mutually reinforcing—multiplicative, rather than additive.

This would involve more than sharing of pieces of information; it would require establishing a common informational base, and especially merging and linking various information systems. Command and decision-making networks especially must be linked, so that all commanders, at all levels, could share situational awareness and interoperate according to a unified situational picture. As one Chinese analysis observed, "mutually shared command information is the foundation for jointly operating forces complementing each other in their operations, allowing for improvements in operational effectiveness, and the means of ensuring the achievement of combat objectives."[7]

Indeed, the analysis notes, modern warfare involves many different services and branches operating together on the informationized battlefield, with various weapons platforms operating across a vast expanse from the bottom of the ocean to outer space and reaching into the electromagnetic and cyber realms. Consequently, successful joint operations cannot simply be comprised of coordinated, single-service operations. Instead, land, sea, air, space, electronic, and network forces must be melded into a unified whole, constituting

a "surpassing-joint" (*chao lianhe*; 超联合) force.[8] Merging these forces creates the systems of systems necessary for mutually supporting, unified joint operations. In particular, unified joint operations require unified, or integrated, combat systems of systems and combat activities.

"Unified combat systems of systems" (*zuozhan tixi yitihua*; 作战体系一体化) are ones where information can rapidly move among the various components and subsystems, allowing real-time data sharing. In these systems, barriers among the six major systems of reconnaissance and early warning; command and control; mobility; strike; defense; and safeguarding are minimized.[9]

"Unified combat activities" (*zuozhan xingdong yitihua*; 作战行动一体化) involve the ability to respond promptly to changing battlefield conditions, dynamically adjusting missions and force deployments. By employing networked information systems and integrated combat systems, commanders can rapidly assess situations and employ an accelerated "situational assessment-determination-unit activity" (*qingkuang panduan/juexin chuzhi/budui xingdong*; 情况判断/决心处置/部队行动) cycle.[10] Ideally, this will grant commanders information advantage, decision-making advantage, and allow them to act effectively, exploiting resulting opportunities.

Coupled with modern weapons' ability to strike precisely across the entire depth of the theater, the combination of unified combat system of systems and combat activities become a major force multiplier. The various participating forces will each contribute different capabilities, but each capability will be even more powerful because the forces are melded and fused. Undertaking "integrated operations" (*zhengti zuozhan*; 整体作战) with such joint forces will therefore be even more decisive.

To reap such benefits, these various unified weapons and operations require an information network linking them together. This network is the basic technological foundation for the command-and-control structure overseeing all participating forces. Without such a command-and-control structure, it would be impossible to create, implement, and regularly exercise the procedures and processes necessary for smooth interactions among participating forces. The success of unified joint operations depends upon a permanent joint command structure.

Such a structure in turn requires dedicated human, organizational, hardware, and software elements. As Chinese analyses note, a unified joint campaign command organizational structure must be staffed with personnel accustomed to thinking in joint terms, who have a holistic view of the mission and of participating forces, rather than a service or branch focus. Planners must think in terms of air, land, and sea operations, but also special operations, space operations, and operations in the electromagnetic domain. Similarly, planning for command, control, intelligence, communications, and defensive

countermeasures must incorporate this comprehensive, unified approach.[11] It also requires rapid and accurate management of massive amounts of information, including compilation, analysis, and dissemination.

Indeed, joint operations commanders and staff are challenged to incorporate information from all sources, including not only what services provide but also from local military commands, party officials, and civilian assets. Information systems must allow unencumbered sharing of information, entailing compatibility in both hardware and software terms. There must be many different communications channels, able to support the transfer of many different forms of information (e.g., video, audio, data), in various formats.[12] There must also be common procedures that span all services, so that any personnel assigned to any unified joint campaign command structure have a common understanding of staffing processes.

All these efforts ideally generate a common situational picture, one that can receive inputs from all participating forces and various platforms (including their weapons). Each input, in turn, will be shared near simultaneously by all participating forces. By generating such shared situational awareness, exploiting all available information sources, Chinese analysts expect a more rapidly cycling information flow. Commanders' decisions will more rapidly disseminate to subordinate units, facilitating flexible, tailored responses. Command will be in real time, and operations will be promptly adaptive.

This common situational picture will also allow commanders to better track not only adversary forces but also friendly units. This capacity is especially important given the involvement of forces drawn from different services, operating across multiple domains. As one Chinese analysis observed, even Sun Tzu had written that only by knowing oneself as well as the adversary can one hope to be ever victorious.[13] This would be even more true in the Information Age.

According to Chinese writings, the common situational picture is built upon several key pillars.

- *Real-time information.* Perhaps most important is the ability to obtain and transmit information on a real-time or near-real-time basis. Unlike in the Industrial Age, information systems now permeate the battlefield, allowing for near instantaneous capture and transmission of information. Moreover, because of advances in electronics and associated information technology, smaller, cheaper sensors can nonetheless collect and transmit enormous amounts of data. At the same time, modern warfare requires prompt access to information, because warfare under informationized conditions is both more rapid and more intense. Given the importance of establishing information dominance, it is vital that information be readily available.

- *Accurate data*. Complementing real-time availability is accuracy. In order to counter an adversary, Chinese analyses emphasize the need to assess overall adversary combat capabilities and to determine its likely courses of action, down to the individual unit level. This must include not only their equipment and manpower strength but also their physical reach, the radius of action within a given time period, and quality of forces.[14] Inaccurate information will lead to wrong determinations, which will lead to flawed decisions and failure. Similarly, information about one's own forces' disposition and capabilities must be both timely and accurate. Chinese assessments presume that information will stem from many different sources, including an array of sensors, open source information, and cyber intelligence. Such a diverse set of sources provides a more comprehensive, more accurate picture of friendly and enemy forces. It may also complicate an adversary's attempt to undertake camouflage, concealment, and deception measures (CCD), since these efforts would have to be mutually consistent to successfully fool intelligence analysts.
- *Collection of many different kinds of information for many different users*. Political and military commanders will access information collected from many different domains, including land, sea, air, outer space, and electromagnetic spectrum. This scale of information collection will maximize the effectiveness of weapons, while also granting commanders an unprecedented degree of situational awareness. They will have insight not only into the physical deployments of forces but potentially into the adversary's decision-making processes and preferences. Consequently, political and military commanders will enjoy a single, integrated situational picture that incorporates friendly and adversary dispositions, overall environment, and intended operational goals and methods.
- *Intelligent information processing*. The sheer scale of collected information will allow military commanders to be much more efficient, tailoring numbers and types of weapons precisely against any given target set. Information processing capabilities on sensor platforms and integrated into weapons will help manage the information flow, allowing analysts to focus on essentials, while accelerating analysis (by preprocessing some of the data). As platforms themselves become more intelligent, provided information will be better tailored to the individual user, avoiding information overload despite the volume collected.[15]
- *Reliable communications*. Secure, reliable, high-bandwidth communications are essential for creating the common situational picture. Indeed, in the Chinese view, all of the information that forms the common situational picture relies upon reliable communications for transmission

> and exploitation. Every aspect of the joint force, including navigation, force coordination within the same echelons, and between front lines and rear areas, as well as command and intelligence functions, depends on establishing reliable, secure communications.

By developing a common situational picture, PLA commanders and their subordinate forces will integrate their operations. Enemy vulnerabilities can be rapidly identified, all available friendly forces can be deployed to exploit them, and strikes from a variety of locations can be coordinated to maximum effect. At the same time, better information will allow more sustained operations, so PLA forces can engage in unrelenting operations that exploit newly arising opportunities, while preventing the adversary from regrouping. Rather than a linear progression, operations will proceed in parallel, across the depth and breadth of a theater, with precise attacks paralyzing an adversary, rather than brute force bludgeoning it into submission.[16]

From the Chinese perspective, the American-led coalition's operations against Iraq in 2003 clearly demonstrated what such information sharing can achieve. Because coalition forces had superior C4ISR capabilities, they forged a truly joint operational approach, with smooth communications and data sharing among the various forces. This marked a major advance over what had been undertaken in the Gulf War, a decade previously, where coalition ground forces had some difficulties coordinating with naval and air forces.[17]

Information War at the Campaign Level

The PLA believes informationized warfare has blurred past conceptual boundaries and distinctions among offensive and defensive operations; forward and rear areas; and positional, mobile, and guerrilla warfare. It has also accelerated the evolution of joint operations from multiple services coordinating individual operations in time or space, to "unified (sometimes translated as integrated) joint operations" (*yitihua lianhe zuozhan*; 一体化联合作战) and "unified strength" (*yitihua liliang*; 一体化力量).

This shift magnifies the role of information at the campaign level of war. Future "local wars under informationized conditions" will revolve around dominating the information domain. According to PLA analyses, the ability to successfully conduct campaign-level operations now requires the ability to handle and share information, which will determine how well participating forces can interoperate, and exploit time and space factors.[18] Information is elevated to the same importance as physical forces, time, and physical space as key, objective factors. The side that is creates and maintains a smooth flow of information will rapidly enjoy an "information

advantage" (*xinxi youshi*; 信息优势), and set the stage for paralyzing and defeating the enemy.

In the Chinese view, establishing smooth information flow in turn requires creating a suitable command-and-control structure. The shift from discrete, coordinated forces to fully merged or melded forces acting in a unified ways leads to "an emphasis on the use of command decision-making to form and shape the entire whole."[19] Informationized warfare essentially exploits the incorporation of advanced information technology into command-and-control capacity, as the means of assuring smooth information flow. This leads to the creation of a common situational picture, allowing generation of additional combat power by having all forces implementing a unified plan.

The PLA has assessed that unified joint operations, with mutually supporting, mutually reliant, mutually compensating forces, are the only way of achieving victory.[20] Unified joint operations are the expression of the characteristics associated with informationized warfare, the basic "operational form" (*zuozhan xingshi*; 作战形式) of conflict in the Information Age.[21] Gaining the information advantage will be the central focus of "information war at the campaign level" (*zhanyi xinxi zhan*; 战役信息战).

Along these lines, no single service, no single system, can dominate the battlefield of the future. PLA writings regularly reiterate that integrated, unified joint operations are not a form of "*systems* warfare" (*xitong zuozhan*; 系统作战), but "*system-of-systems* warfare" (*tixi zuozhan*; 体系作战).[22] Because information technologies create networks and multiply linkages, Chinese analysts believe that conflicts are no longer decided by the balance in platform-versus-platform performance, nor even "system" (*xitong*; 系统) against system. Instead, it is the ability of rival arrays of systems, "systems of systems" (*tixi*; 体系), to outperform each other that is decisive.[23]

Systems of systems are the product of integration through information flow. Success in future conflicts will require all systems (information gathering, communications, command and control, weapons, logistics), drawn from all participating services and operating across various domains, to work together, in both human and technical terms. Developing and adopting common software, standards, and engineering facilitates this process. It allows both weapons and command systems to operate as a relatively seamless whole and behave as a truly joint organization.[24]

These systems of systems not only link combat forces but also tie combat, combat support, and combat service support functions together. Informationization, for example, has a significant impact on logistics. As information technology has become widely incorporated, logisticians can keep better track of their supplies, so depots can be more dispersed (reducing vulnerability to enemy attack) while still supplying combat forces in a timely manner. Proliferation

of information technology also allows tracking of both unit requirements and consumption rates of various supplies. This allows logisticians to *push* supplies to units, rather than simply respond to demand *pull,* making logistical support more flexible yet still responsive.

Given previously noted requirements for reliable, accurate, multisourced information, the core of system of systems dominating future battlefields are "the three major systems" (*sanda xitong*; 三大系统):[25]

- *A battlefield sensor system*. This will be rooted in integrated ground–air–space surveillance networks, incorporating reconnaissance satellites, navigation and positioning satellites, and aerial reconnaissance systems, including manned and unmanned vehicles.
- *A battlefield information transmission system.* Employing satellites, mobile stations, digitized communications and data relay networks, this system must be able to rapidly and securely transfer data from sensors to analysts and then to shooters.
- *A battlefield command-and-control system*. This will include elements of both strategic and tactical C4 (command, control, communications, and computer) systems.

When linked together, the three will form a system of systems that will provide the common situational picture through real-time, rapid, precise information collection, management, and transmission. Smooth information flow is what will allow the rapid, accurate movement of resources, the coalescing of joint forces, and coordination of joint activities, in manner that outpaces that of the adversary.[26]

If victory or defeat is based upon the ability of systems of systems to function properly, then the struggle to pass information smoothly while preventing an adversary from doing the same will be a central part of future campaigns. Weaknesses in any individual system need not be fatal, as strengths in other systems and forces can compensate. However, if certain key nodes and linkages among the systems are attacked, the overall array of systems of systems may decohere, leading to systems paralysis. Identifying and nullifying these nodes is a vital part of systems-of-systems warfare.

It is also a fundamentally different approach. Opponents in "local wars under modern conditions," that is, Industrial Age warfare, focused on annihilating an adversary through the infliction of massive casualties. Adversaries in "local wars under informationized conditions" focus on breaking down the enemy's information flow, disrupting the smooth operation of their system of systems, and paralyzing the enemy. Indeed, some PLA analysts argue that information has displaced physical material as the core resource for determining victory, and is what distinguishes unified joint operations from the preceding coordinated joint operations.[27]

Information war at the campaign level therefore fundamentally entails safeguarding one's own information networks, including those relating to information gathering, communications, and management and decision making while degrading the adversary's corresponding networks.[28] The side retaining superior abilities to gather, use, and control information, the core of information dominance, will triumph.[29]

Each side's "three systems" will be a "center of gravity," in Clausewitzian terms, in future local wars under informationized conditions. Countering and preserving the "three systems" are essential means of establishing "information dominance" at the operational level of war, much as successfully waging political warfare is a central means of achieving "information dominance" at the strategic level.

INFORMATION DOMINANCE AND SEIZING THE INITIATIVE

For PLA analysts, information dominance is a means, not ends, for military campaigns. Achieving it allows one to make better decisions and employ weapons more effectively, but it is not sufficient by itself for victory. Similarly, while denying an adversary information dominance will paralyze it, the adversary may still not surrender. Moreover, information dominance is rarely absolute or permanent. While one should target an adversary's information systems, that targeting must be sustained throughout the course of the campaign. Similarly, one's own systems will be attacked, and must be protected, for the duration of the conflict.

This effort is somewhat eased if one can seize and retain the initiative. The importance of assuming an active stance and seizing the initiative (*zhudong quan*; 主动权) is embodied in the Chinese concept of the "Active Defense" (*jiji fangyu*; 积极防御). The PLA's conception of the idea is rooted in Mao Zedong's military thinking. Mao discussed the concept of "Active Defense" in 1936, and compared it favorably to "passive defense," which he dismissed as "actually a spurious kind of defence [sic], and the only real defence is active defence, defence for the purpose of counter-attacking, and taking the offensive."[30] Today's PLA continues to abide by the "military strategic guideline (*junshi zhanlue fangzhen*; 军事战略方针) of the 'Active Defense,'" as detailed in the 2015 Chinese defense white paper.[31] Like Clausewitz's conception of defense as a "shield of blows," the Chinese envision the Active Defense as a defensive stance that nonetheless incorporates offensive actions.

The active stance is emphasized because the adversary must be forced into the reactive mode. As Mao observed, staying on the defensive accepts a passive role, ceding to the adversary the time and place where action will occur.

It cannot be decisive. Only by undertaking offensive actions, at least at the operational and tactical level, can one influence the outcome of the conflict.

At the same time, retaining the initiative also enhances one's own morale. Since the PLA has often been technologically and materially inferior to its adversaries, including the Nationalist forces and the Japanese in World War II, it had limited abilities to dictate the conditions or occurrence of battles. Assuming a purely or predominantly reactive posture would only enhance the enemy's apparent ability to dictate the conflict's terms. This inevitably erodes military and popular morale. The PLA has long held that securing and maintaining the initiative at strategic, operational, and tactical levels is victory's foundation, and remains its view today.[32]

Information technology's central role in modern warfare has opened a new path the PLA to seize the initiative. Better ability to collect, manage, exploit and transmit information more rapidly, more accurately than the adversary, that is, establishing information dominance, creates a faster observe–orient–decide–act (OODA) loop than the adversary. For PLA analysts, the side with information dominance of the battlefield (which would extend from outer space to the ocean depths, and would include the rear areas of all combatants) compels the other side to react.[33]

It is important to note that the Chinese do not argue that one needs to be able to have a *faster* OODA loop. The side with information dominance can achieve the same effect of securing and retaining the initiative *if one can slow the adversary's OODA loop*. Whether through computer network attacks, physical destruction of key nodes, or psychological warfare, one can disrupt the enemy's systems of systems, denying them the ability to make and implement decisions in a timely fashion, and therefore lose the initiative.

The Chinese military in the Information Era, unlike historically, can get in "on the ground floor." Whether conventionally or in nuclear terms, China has long been relatively weaker than the United States or Soviet Union. But the Information Age has arisen when China has had more financial, human, and technological resources available to compete with. Moreover, at least in the Chinese view, the Information Age changes the basis for warfighting power. It does not make older capabilities obsolete, but it substantially overshadows them (yet it also allows older systems to be upgraded and made more capable).

Information technology's emergence as the key arbiter of combat power is analogous to the rise of the all-big-gun battleship in its tectonic impact. When Sir Jackie Fisher introduced the HMS *Dreadnought*, it made all other battleships obsolete in a stroke. This applied not only to German, French, and American warships but to the *British* battle line as well. In effect, *Dreadnought* reset the global naval balance to zero, placing everyone at the same starting point. Computer networks, telecommunications networks, and systems of

systems are similarly reshaping military capabilities globally. Every military, whether American, Chinese, Russian, or Japanese, is affected, with past investments and extant capabilities no longer necessarily determinative of future standing.

In this reordering, securing initiative will depend less on traditional land, sea, and air power, or upon sheer mass. Instead, the Chinese believe it will rest, foremost, on establishing information dominance. Understanding the battlefield situation, planning responses, communicating those plans and coordinating forces to implement them, more rapidly and accurately, will leave the adversary unable to catch up. Through information dominance, one can secure air, naval, and space dominance, which further constrains the enemy and maintains one's grip on the initiative.[34]

INFORMATION DOMINANCE AND THE CAMPAIGN GUIDING THOUGHT

As a military steeped in Marxism–Leninism, the PLA views war as a science, with governing laws and principles like any other science. In the theoretical hierarchy, there are military strategic guidelines (i.e., the military strategy), campaign guiding concepts, and basic guiding principles. In the Information Age, Chinese writings have incorporated information dominance into the "campaign guiding concept" (*zhanyi zhidao sixiang*; 战役指导思想). The campaign guiding thought is the expression of the military strategic guideline (i.e., the military strategy) at the operational level of war. It provides broad guidance regarding key wartime missions. Current campaign guiding thoughts focus on "local wars under informationized conditions."

In the 2000 edition of the PLA textbook *The Science of Campaigns*, the campaign basic guiding concept was characterized as "integrated operations, key point strikes (*zhengti zuozhan, zhongdian daji*; 整体作战, 重点打击)." It focused on promoting interservice cooperation while undertaking concentrated attacks against essential adversary targets. In the 2006 edition, the campaign guiding concept was modified to "integrated operations, constrain the enemy with precision strikes (*zhengti zuozhan, jingda zhidi*; 整体作战, 精打制敌)," shifting emphasis toward better exploiting information resources.

"Integrated Operations"[35]

In this new formulation, "integrated operations" builds upon the previous concepts of integrating various forces, domains, and offensive and defensive activities, and now incorporates information technologies and an "informationized" perspective into all operations. This elevates new approaches, such as "soft-kill" capabilities, and links firepower attacks to special operations

missions as well as psychological strikes. These integrated forces and capabilities should focus on disrupting the adversary's ability to communicate and command effectively. Moreover, integrated operations must concentrate battlefield sensors, information transmission systems, as well as rapid mobility and precision-strike capacity, to generate "unified operational strength" (*yitihua de zuozhan liliang tixi*; 一体化的作战力量体系).[36] Commanders should not strive to mass forces physically, but to mass effects by exploiting information networks. The unified plan should maximize the impact of participating elements by integrating them into a coherent whole.

The new campaign guiding concept views the entire battlespace as a unified whole. Outer space, the electromagnetic realm, and the psychological realm join the traditional domains of land, sea, and air as decisive arenas. Especially important are the space and psychological battlefields. The former is described as the new "strategic high ground" (*zhanlue zhigao dian*; 战略制高点). The latter reflects the human factor in warfare, and requires careful exploitation so as to attrit the enemy's will. They are central for both accessing and processing information.

Whereas the earlier guiding concept had directed "integrating campaign phases and activities," informationization has now also transformed operational activities and styles, with wholly new operational styles and concepts now possible. Commanders are expected to unify various types of wartime operations, including information warfare, firepower warfare, mobile warfare, positional warfare, psychological warfare, special operations, and network warfare, into a unified campaign plan. They must also combine conventional and irregular warfare, offense and defense, hard- and soft-kill, and physical strikes with psychological attacks. By applying so many different methods the adversary is kept off balance, facilitating seizure of the initiative. But unifying operations requires careful planning and prioritization, so command-and-control systems are central.

The revised campaign guiding concept also emphasizes "safeguarding" or "support" (*baozhang*; 保障), especially in a joint manner. The Chinese concept of "operational support" (*zuozhan baozhang*; 作战保障) is roughly analogous to combat support and combat service support functions. It embodies reconnaissance and intelligence; communications; information defense, including information security and facilities security; engineering activities; transportation; surveys; meteorological and hydrographic support; electromagnetic spectrum management; and other such activities.[37] Safeguarding or support sometimes incorporates logistical functions; it emphasizes security and secrecy.

In the revised *Science of Campaigns,* many aspects of safeguarding are discussed, including safeguarding of forces, of capabilities, and of tasks (e.g., operational safeguarding, logistics safeguarding, and equipment safeguarding).

Unified operations require a consolidated "safeguarding command structure" (*zhihui baozhang tizhi*; 指挥保障体制), to oversee the various safeguarding missions throughout the course of the campaign, across all battlespaces. Safeguarding of information is especially important, as it includes safeguarding not only data itself but the physical infrastructure of information networks.

Chinese forces following the campaign guiding thought will not only integrate their own forces and operations but attack the adversary's integration efforts. The enemy must not be allowed to forge its operational systems into an "integrated operational capability" (*zhengti zuozhan nengli*; 整体作战能力). Consequently, Chinese commanders will try to disrupt the enemy's systems architecture by identifying and attacking its key nodes. By generating a cascading set of failures, the adversary's system of systems can be paralyzed. Examples include attacking the enemy's command-and-control systems, information systems, weapons systems, and vital safeguarding systems.[38]

The campaign basic guiding concept envisions future Chinese operations in local wars under informationized conditions as resembling a symphony. Like the orchestra's woodwinds, brass, percussion, and stringed sections, the constituent elements of the Chinese armed forces, including the militia and the People's Armed Police as well as PLA land forces, naval forces, missiles, special operations units, will each contribute to the "performance" of integrated operations. Success requires the orchestra operate under a unified headquarters serving as conductor, according to the sheet music of the unified plan. But in this analogy, the individual sections and musicians may be in isolated booths or wearing blinders and headphones. The ability to get the proper score to all of the musicians, and for the various musicians to know their cues and be alert to changes in tempo, is dependent upon establishing information dominance.

"Constrain the Enemy with Precision Strikes"[39]

The other half of the revised campaign basic guiding concept calls for constraining or limiting the enemy through "precision attacks" (*jingda zhidi*; 精打制敌). Such attacks incorporate high technology firepower and precision munitions, but are also part of "precision operations" (*jingque zuozhan*; 精确作战).[40] These operations require precise selection of targets, forces, tactics and techniques, and conflict intensity and progress. Without precise and effective command and control, one cannot have precision strikes and operations.[41] Creating a suitable joint campaign command structure is essential. It must treat available forces as a unified whole, create a single integrated set of operational plans, and wield the entire available force as a unified entity.[42]

The command structure must identify "key enemy targets" (*di yaohai mubiao*; 敌要害目标), including military facilities and political and economic

systems "that help support enemy operations" (*di zuozhan tizhi qi weixi zuoyong*; 敌作战体制起维系作用), especially in the information, air and maritime domains. Identifying and killing such targets are a central means of paralyzing the enemy's "combat system-of-systems structures" (*zuozhan tixi jiegou*; 作战体系结构), shaking morale and disrupting interoperability among systems and subsystems.

The adversary's information systems are core operational enablers and therefore must be priority targets from the campaign outset. "The early destruction of the enemy's information systems will induce paralysis in their entire combat system, thereby achieving the greatest victory at the lowest price."[43] Because informationized battlefields are enormously complex, destroying or degrading the enemy's information management facilities and systems will inevitably reduce its ability to exploit information resources and operate effectively. The effects will propagate throughout their forces, reinforcing synergies, allowing the PLA to achieve "comprehensive information dominance" (*quanmian de zhi xinxi quan*; 全面的制信息权).[44]

Precision target selection involves not only identifying which enemy systems are most vulnerable but also "weaponeering." That is, in the PLA view, one must also take into account the capabilities at one's own disposal, ensuring that every target is not only serviced but serviced efficiently. This is especially important when selecting the initial target set. The objective is to maximize disruption over the course of the campaign, not necessarily destruction at the outset.

Therefore, some targets may involve "soft-kill" (e.g., jamming) rather than "hard-kill" methods. Others may be deferred for subsequent attacks, if they are also sources of important intelligence, or are likely to become more salient over time. Similarly, as the campaign progresses, the campaign command must adjust their targeting, maintaining a responsive approach while remaining focused on the ultimate campaign objectives.

Commanders are also advised to concentrate their best forces, to maximize the effectiveness of attacks. Even though a force may be generally qualitatively inferior to an opponent, it may forge local superiority by concentrating advanced weapons and elite troops and wrest superiority for some period of time. In particular, one's best forces should be weighted toward the "main direction" (*zhuyao fangxiang*; 主要方向), at "key areas" (*zhongdian diqu*; 重点地区), and at "key times" (*guanjian shijie*; 关键时节), creating local superiority at decisive times and places.[45]

ESTABLISHING INFORMATION DOMINANCE

For the Chinese commander, information dominance is a central means of fulfilling the campaign guiding thought of "integrated operations, constrain

the enemy with precision strike." Because all operations require information, information dominance allows forces to operate at their full potential. Conversely, without information dominance, there can be no air, land, sea, or outer space dominance—victory becomes difficult if not outright impossible. Information dominance supports and safeguards the other dominances.[46] To this end, PLA analysts assume that both sides will be constantly striving to weaken and undermine the adversary's information networks, while preserving their own.

Offensive actions are essential. Information dominance cannot be achieved through solely defensive, reactive measures. Indeed, as one PLA analysis observes, "it is more important to emphasize the offensive with regards to the information domain than it is in the traditional land, sea, and air domains."[47] Sustained offensive actions against the adversary's information networks, command-and-control infrastructure, and key combat forces are the core of "information warfare" (*xinxi zhan*; 信息战).[48]

Only neutralizing the adversary can protect one's own networks and systems of systems. Successful information warfare efforts will reduce the adversary's traditional combat forces to an Industrial Age capacity. They may remain locally potent, but will have only limited strategic or operational impact if their supporting information networks are disrupted, paralyzed, or destroyed.[49] In both the Gulf War and the Balkan conflict in Kosovo, the Iraqi and Serbian frontline combat forces, respectively, suffered relatively few casualties. The destruction of their "three major systems," though, meant that the remainder had no decisive impact.

In those conflicts, the America-led coalition forces had an overwhelming set of advantages, including far more extensive information resources than the Iraqis or Serbs could field. In a more balanced fight, Chinese analyses suggest that information dominance will be localized and temporary. Pervasive, resilient information networks make establishing permanent information dominance difficult. Consequently, by constantly and actively concentrating their information warfare resources, the weaker side can nonetheless achieve at least local information superiority and advantage. By maximally exploiting these local conditions in the offensive, the enemy can still be paralyzed and defeated.

Whether one has achieved information dominance or not, one must also constantly undertake defensive efforts to preserve the integrity of one's own systems of systems. For the side that is technologically inferior, this will be difficult, as the adversary may well exploit paths and approaches that one either had not conceived of or had insufficiently prepared defenses for. Attacking the adversary's information networks must therefore be part of one's defensive efforts, even if one is weaker, both to deny the adversary the initiative and to

alleviate pressure on one's own systems. Taking the offensive allows the weaker side to compensate, and can unbalance a stronger enemy.[50]

In the Chinese assessment, whether in defense or offense, priority targets when conducting information warfare and pursuing information dominance include the adversary's intelligence and surveillance systems; their high technology weapons platforms and bases where they are located; their safeguarding infrastructure, systems, and forces; and their command, control, and communications networks.[51] The side that retains a relatively more intact set of system of systems, that maintains better connectivity among the "three big systems," will win.

Achieving information dominance in the face of this maelstrom of hard-kill and soft-kill weapons and tactics is not solely or even predominantly a matter of computer network attack (or defense). Instead, the Chinese concept of information warfare at the campaign level comprises several key lines of operations, including electronic warfare, network warfare, psychological warfare, and increasingly command-and-control warfare and intelligence warfare.

Electronic Warfare (*dianzi zhan;* 电子战)

Electronic warfare is one of the earliest forms of information warfare. It was widely used in World War II (e.g., use of chaff by Allied bombers to blind German air defense radars; exploitation of cryptanalysis by all sides to outmaneuver their adversaries), and has become increasingly sophisticated and important in the intervening decades.

Electronic warfare is the degradation and disruption of the adversary's electronic systems, while preserving one's own.[52] It occurs in the "electromagnetic space" (*dianci kongjian*; 电磁空间), or the electromagnetic spectrum, ranging from super low frequency to ultraviolet, including the visible light spectrum. Chinese analysts see the electromagnetic space as the fifth domain of warfare, alongside land, sea, air, and outer space.[53] Indeed, electronic warfare is actually a struggle to dominate the electromagnetic spectrum, as part of establishing information dominance.

When electronic warfare is successfully waged, it affects the vast majority of systems that collect, transmit, or exploit information. Electronic systems permeate informationized warfare; land, sea, air, and space operations depend on them. Electronic warfare conceptually affects sensors (e.g., radars), communications systems (e.g., radios), as well as weapons control and guidance systems. Therefore, as one Chinese assessment notes, the side better able to wage electronic warfare will more likely establish the "three dominates."[54]

The centrality of electronic systems is reflected in the proportion of weapons costs they now represent. Some of the most expensive elements of modern

warships and combat aircraft are onboard electronics, rather than the fuselage or hull. As one PLA analysis notes, electronics represent 20 percent of the cost of modern warships, 24 percent of armored fighting vehicles, 33 percent of military aircraft, 45 percent of missiles, and 66 percent of satellites.[55]

The wartime electronic environment has become steadily more complex, as both sides field an array of sensors, communications systems, and other electronic systems. Even without the two sides striving to erode the others' electronic systems, combat forces emit an enormous amount of electromagnetic energy, with the potential for mutual interference.

Understanding the electromagnetic battlefield is further complicated by interference among electronic systems. This includes not only both sides' efforts to interfere with the adversary's electronic systems but also interference generated by one's own forces and by natural effects. An essential part of electronic warfare is reconciling and coordinating electronic activities among one's own various forces through frequency and spectrum management by the joint campaign command.[56]

As the Chinese observe, some nations define electronic warfare narrowly. One Chinese volume sees the Russians as predominantly relying on software attacks against the adversary's electronic systems.[57] Another assessment concludes that the U.S. military is focused on the electromagnetic means, in attack and defense. In this assessment, the American approach neglects several important additional means of neutralizing the adversary's electronic systems, including:

- Human agents or physical weapons to physically attack electronic systems;
- Propaganda and psychological warfare techniques to degrade the perceived effectiveness of electronic systems; and
- Nonelectromagnetic systems to counter electronic equipment.[58]

By contrast, the PLA adopts a much more expansive definition of electronic warfare. According to Chinese analyses, electronic warfare embodies the range of activities that maximize one's ability to exploit the electromagnetic spectrum, while also eroding the adversary's abilities to do the same.[59] Electronic warfare, from the Chinese perspective, includes not only electronic-based weapons but the conduct of electronic reconnaissance and counterreconnaissance; interference and preservation measures for electronic information; and all efforts at disrupting and countering disruption of electronic systems. Electronic warfare measures include attacks on enemy communications landlines; radio networks; microwave transmission networks; and position, navigation, and timing (PNT) systems.[60] They incorporate not only soft-kill techniques such as jamming and electronic interference and suppression

but also hard-kill approaches. The latter includes artillery barrages, aerial bombardment, and other firepower strikes against key electronic systems.

While electronic warfare has historically been mainly a tactical issue (e.g., provision of jamming assets in support of individual bombing raids), the Chinese believe electronic warfare will constitute a campaign-level activity in future local wars under informationized conditions. Proliferation of electronic warfare tools and weapons across land, sea, air, and space platforms, and development of electronic weapons whose effects span dozens or even hundreds of kilometers, will expand the volume affected by orders of magnitude. In particular, the capacity to undertake electronic warfare against space-based communications; reconnaissance and surveillance; PNT; and meteorological assets will be a vital means of establishing electromagnetic dominance.[61]

Campaign-level electronic warfare, in the Chinese view, will be comprised of three broad mission areas: electronic reconnaissance, electronic attack, and electronic defense.[62]

Electronic Reconnaissance (*dianzi zhencha; 电子侦察*)

The Chinese concept of electronic reconnaissance parallels the Western idea of electronic intelligence, or ELINT. Key targets of electronic reconnaissance include communications networks, radars, electro-optical systems, and sonar and hydrologic systems. It entails collecting intelligence about these electronic systems, including identification and surveillance of key facilities, collecting and identifying types of signals and emissions, as well as identifying patterns of unit operations and behavior as they use various types of equipment. It establishes both a unit and electronic order of battle. Electronic reconnaissance allows staffs to determine when and where adversary units are deploying and supports technical and tactical staff efforts in formulating countermeasures to the adversary's electronic capabilities. It provides the foundation for both electronic attack and electronic defense.

Electronic reconnaissance must occur in peacetime as well as wartime, in order to establish the baseline informational requirements and provide decision makers with timely information.

Electronic Attack (*dianzi jingong; 电子进攻*)

Electronic attack erodes or paralyzes support from informationized equipment, through disruption, interference, or destruction, emphasizing the latter two elements. Interference involves blocking the adversary's ability to effectively employ certain frequencies, that is, jamming, or otherwise preventing normal equipment operation. It is commonly employed against enemy communications, radars, electro-optical systems, and sonar and hydrographic

systems. Electronic attack can also physically disrupt or destroy the enemy's electronic equipment. This has the benefit of imposing greater costs and typically can have a more protracted effect. Physically destructive means include not only the panoply of bombs, rockets, and artillery but also antiradiation missiles and both nuclear and non-nuclear electromagnetic pulse weapons.

One Chinese analysis suggests four broad categories of electronic attack targets.[63]

- Information itself, whereby deception, counterencryption, and other such techniques are employed to access information. The implication is that targeted information can then be altered, destroyed, or otherwise damaged.
- Electronic systems that directly carry information, such as radios and telecommunications networks. These can be subjected to electronic interference or disruption, including various types of cyberattacks.
- Facilities and physical infrastructure that house key electronic systems, such as radar sites, server farms, and headquarters facilities. These are likely to be targeted through kinetic means, such as antiradiation missiles and cruise and ballistic missiles. They would also be vulnerable to various types of electromagnetic pulse and directed energy weapons.
- Systems that employ information, which include the vast majority of weapons, which could be attacked by a variety of means.

It is worth noting that this Chinese concept of "electronic attack" is more a reference to what is *being attacked* than the means of conducting such attacks. That is, missiles, bombers, special operations forces are all seen as potential aspects of electronic attack, because they can be help establish electromagnetic dominance.

Electronic Defense (*dianzi fangyu; 电子防御*)

Electronic defense embodies efforts to minimize the adversary's ability to degrade the operation or effectiveness of one's own electronic systems. Chinese electronic defense efforts counter the adversary's electronic reconnaissance, electronic interference, and electronic destruction. While it includes the concept of "electronic counter-countermeasures" (*dianzi fanduikang*; 电子反对抗), it is goes beyond them.[64]

Instead, the Chinese approach to electronic defense includes steps to prevent the enemy from detecting electromagnetic signals and emissions, key electronic warfare units, or the technical parameters of key electronic equipment. It also includes safeguarding measures to prevent the enemy from destroying or damaging those systems physically or electronically. It therefore includes aspects of counterespionage, information security, and physical

security, as well as electronic counter-countermeasures, tactical maneuver, concealment and deception, and physical defense.

Network Warfare (*wangluo zhan*; 网络战)

Network warfare is the partner of electronic warfare. Also termed "network conflict" (*wangluo duikang*; 网络对抗), it covers the range of activities that occur within networked information space, as the two sides attack each other's networks while preserving their own.[65] Like electronic warfare, it includes not only offensive and defensive components but also reconnaissance of the adversary and others' networks.

Network warfare occurs in the realm of "network space" (*wangluo kongjian*; 网络空间), a term that roughly parallels that of "cyberspace." However, the Chinese concept of network warfare moves beyond just computer networks, although computer network warfare remains an integral element of network warfare. In relation to information warfare at the campaign level, it occurs within networks that are part of the overall battlefield (which can extend to outer space and deep into the two sides' homelands as part of the command and control, and logistical and support infrastructures).[66]

The purpose of network warfare is to establish "network dominance" (*zhi wangluo quan*; 制网络权). When one enjoys network dominance, the full range of networks (not just computer networks) can operate smoothly. Information on those networks is safeguarded while rapidly moved and applied, whereas an adversary's networks are prevented from doing the same. Some networks that are integral to network warfare include the command-and-control network, intelligence information network, and air defense network.[67] Some Chinese analyses consider network space as the sixth domain (alongside land, sea, air, outer space, and electromagnetic spectrum); others consider it part of the electromagnetic spectrum.

Because these various networks are vital to unified joint operations, network warfare is considered by the Chinese as inevitably a central part of future local wars under informationized conditions. They are especially effective means for the weaker side to balance the stronger side's advantages. One Chinese analysis observes that in the 1990s Balkan conflicts, although NATO generally outmatched Serbian forces, the Serbs were nonetheless able to repeatedly penetrate various NATO networks and degrade their operations. The Chinese write that the Serbs penetrated networks aboard the aircraft carrier USS *Theodore Roosevelt* and in the British Meteorological Office, affecting air operations.[68] Another Chinese analysis similarly observes that disparities in conventional strength between NATO and Serbia were not paralleled on the Internet, where Serbian forces successfully attacked various NATO and individual member states' websites.[69]

Network warfare includes network reconnaissance, network attack, and network defense. These three missions are closely interlinked, so drawing specific boundaries between them is difficult.

Network Reconnaissance (*wangluo zhencha; 网络侦察*)

Network reconnaissance involves the use of various methods to reconnoiter the adversary's networks, mapping its connections and learning its operating procedures. It also involves examining data residing on those networks and the programming that manages and maintains those networks. Network reconnaissance also includes analysis of all this information, to derive intelligence about how enemy networks operate at both procedural and technical levels.[70]

Network Attack (*wangluo jingong; 网络进攻*)

Network attack involves operations against both information networks and networked information; that is, it works against data within various networks as well as the networks themselves. It applies malware, logic bombs, hackers and other such means to disrupt various networked systems, impede their operation, and damage or destroy information they contain. As one Chinese analysis notes, the essence of network warfare is interference and disruption of the enemy's networked information systems, in which the networks themselves are conveying the interference and disruption methods.[71]

Ironically, this suggests that the various information systems comprising the backbone of the systems of systems embody the potential seeds for their own defeat. In particular, the software that runs them may contain various vulnerabilities such as "zero-day exploits," backdoors, or Trojan horse subroutines. Thus, networks may have inherent weaknesses that a smart adversary can rapidly exploit to massive effect, leading to disruption or paralysis of key systems. Given the interlinked nature of systems of systems, the very interconnectivity that generates synergies can lead to cascading failures. An essential part of network warfare, in the Chinese conception, is to ferret out such vulnerabilities in peacetime, in order to exploit them in crisis or war.[72]

For this reason, the Chinese believe that network attack is closely tied to network reconnaissance. The difference between network reconnaissance and network attack may simply be a few keystrokes. Once one has penetrated an adversary's network, it is possible to destroy data or disrupt connections. This makes network warfare different from electronic warfare and very different from more traditional methods of warfare. Differentiating between network attack and network reconnaissance is very difficult, since there may be no distinction until the last moment.

As with electronic warfare, the Chinese see attacks against physical and human elements of networks as additional means of conducting network warfare. Indeed, the Chinese have developed the concept of "integrated information–firepower warfare" (*xinhuo yiti zhan*; 信火一体战), merging operations in information space (including network space) with those in physical space. Just as kinetic attacks and human vectors can be used against an adversary's electronic systems, the same applies to network warfare. Server farms, key routers, data fusion centers therefore might be targeted by missiles, bombs, or special operations units. China is building special operations forces which can undertake both hard-kill attacks against key network nodes and soft-kill operations through hacker and other network activities.[73]

Network Defense (*wangluo fanghu; 网络防护*)

Network defense efforts aim to ensure the smooth operation of one's network systems and facilities. It includes those measures to secure networked information systems and the information that resides or passes over them. Network defense methods include preventing an adversary from accessing one's own network, disrupting network operations, or jeopardizing the integrity of information on those systems.[74]

Integrated Network and Electronic Warfare (*wangdian yiti zhan; 网电一体战*)

A central aspect of the Chinese concept of unified joint operations in future local wars under informationized conditions is the merging of network and electronic warfare. As network warfare expands and electronic warfare systems are networked, the Chinese see the two as inextricably linked. Indeed, Chinese military theorists were among the earliest adopters of the concept of "integrated network–electronic warfare (INEW)" and see INEW as a fundamental characteristic of information warfare and the informationized battlefield.[75]

The PLA defines the INEW concept (which it at times translates as "network–electronic integration warfare") as "information attacks against the enemy's networked information systems through highly melded electronic warfare and network warfare."[76] It includes information warfare methods that combine electronic warfare and network warfare techniques to attrit and disrupt the adversary's networked information systems, while defending one's own, to secure information dominance over the battlefield. It is the main expression of information warfare.[77]

As one Chinese analysis notes, in future conflicts, the electromagnetic spectrum will be the key influence upon the operation of network space. Network and electronic warfare will be organically linked, operating under

a single unified direction.[78] Network warfare will be affected by efforts to dominate the electromagnetic spectrum, while electronic systems operations will be directly influenced by efforts to penetrate and damage networks. Network and electronic warfare mutually complement the unified effort to degrade the enemy's system of systems. Neither alone can comprehensively disrupt that system of systems, but given their mutually supporting nature in terms of attack concepts, attack methods, and operating environments, they constitute a highly effective integrated attack methodology.

Another Chinese volume observes:

> From a technical angle, electronic warfare and network warfare can be greatly complementary. Electronic warfare emphasizes attacking the signal layer, with the use of strong electromagnetic energy to drown out target signals. Network warfare emphasizes attacking the information layer, using disruptive information flow, transported into the enemy's network systems, as the means of attack.[79]

INEW is an effort to unify the physical and virtual aspects of information warfare, merging them into a single concept of operations.[80] INEW envisions using electromagnetic attack and defense and information attack to degrade the adversary's ability to gather and exploit information, treating networked information systems as the domain of operations. Successful conduct of INEW should lead to dominance of the entire "battlefield information space" (*zhanchang xinxi kongjian*; 战场信息空间).

INEW is more than simply adding electronic warfare techniques to network warfare. The central point of the Chinese conception of INEW is incorporating targeting and defense of physical elements of information networks into network warfare. It expands information warfare beyond the predominantly virtual world of data to the physical, tangible world of sensors, routers, and radios. INEW is envisioned as an archetype of the new kind of unified jointness necessary to successfully fight local wars under informationized conditions.[81]

Psychological Warfare (*xinli zhan;* 心理战)

While psychological warfare occupies a vital position as part of strategic political warfare, it also has an operational and tactical role. At the campaign level, the PLA conceives of psychological warfare as using various types of information, consistent with an overall campaign plan, to influence the adversary's thoughts, emotions, knowledge, perspectives, and attitudes.[82] By applying various forms of information, psychological warfare can alter the adversary's interpretations of information, including its context and frame of reference, as well as undermine its will.[83] Often, this information is specially prepared or particularly presented, to maximize effect.[84]

At the operational level, psychological warfare aims to buckle the adversary's will and martial spirit, induce confusion in its command and decision-making processes, and shake its confidence, reducing its combat effectiveness.[85] Unlike at the strategic level, psychological warfare at the campaign level focuses on targets and aspects that will help the military achieve its goals (although this may involve political and economic targets).[86]

Unlike electronic warfare and network warfare, psychological warfare was not spawned by the Information Age. Influencing the adversary's perceptions and eroding its will to fight, while strengthening one's own, have been a long-standing element of warfare. Similarly, "stratagem" (*moulue*; 谋略), employing deception and misleading techniques, has long been part of warfare. It, too, is rooted in an understanding and exploitation of human psychology.

In past wars, psychological warfare methods could only affect a limited audience, such as enemy forces in direct contact. Its impact was therefore often largely tactical. With the growth in information technology, however, psychological warfare efforts can attack the adversary's psychology in new ways, making it more broadly applicable and much more effective. Fusing information operations and psychological warfare, such as through social media and information networks, provides new means of affecting the adversary. Specialized psychological warfare weapons and techniques create new means to confuse and otherwise distract an adversary. At the same time, commanders must devote more energy to countering the adversary's psychological warfare efforts.

As one Chinese analysis notes, stratagem will play as important a role as technology in securing information dominance. This is because information dominance involves not only information technology and information systems (*xinxi jishu xitong*; 信息技术系统) but also "cognitive systems" (*renzhi xitong*; 认知系统).[87] Information is interpreted and eventually acted upon by human decision makers. The human mind is the ultimate destination for all information; how that mind perceives and interprets information is therefore as much a part of information warfare as the networks and electronics that gather and transmit information to that mind. As another Chinese analysis observes, the Information Age affords the opportunity to affect not just the adversary's perceptions but its very cognition and understanding. It is a crucial element that differentiates informationized warfare from previous Industrial Age warfare.[88]

*Psychological Reconnaissance (*xinli zhencha; 心理侦察*)*

To successfully influence the enemy's forces and decision makers, psychological warfare efforts, even at the operational level, must blur traditional lines between wartime and peacetime. Understanding the adversary's

psychology, and implanting long-term influences to affect perceptions, cannot wait for the formal commencement of hostilities. As at the strategic level, operational-level psychological warfare must be a long-term effort. Psychological reconnaissance therefore includes collecting and analyzing the adversary's television, telephone, e-mail, and computer information, as well as its newspapers, journals, and books, in order to understand its strengths and weaknesses.[89]

From the Chinese perspective, the last several "local wars," including the first Gulf War, the Balkan conflicts of the 1990s, and the American advance to Baghdad and toppling of Saddam Hussein, reflect the power of modern psychological warfare. In the first Gulf War, for example, the Chinese assess that the American deployment of various weapons psychologically intimidated the Iraqi military, making them afraid to employ their radars and other sensors to determine where Coalition forces were deploying. The Iraqi military was effectively deaf and blind, psychologically isolated and made to feel helpless. Exploiting this advantage through the dissemination of additional propaganda, in coordination with massive aerial attacks such as by B-52s, the Iraqi military's will to resist was thoroughly undermined.[90]

Even more effective, in the Chinese view, was the unrelenting psychological warfare effort against the Saddam Hussein regime from the end of the first Gulf War (1990–1991) until the 2003 war. Through large scale, protracted use of propaganda and threats of overwhelming force, and by exploiting the psychological effects of extended information blockades (in addition to economic sanctions and other isolating measures) the United States was able to undermine both popular support for the regime and military will to resist. Such efforts were redoubled in the run-up to the 2003 invasion, including the use of special operations forces.[91] Consequently, the Iraqi military failed to defend the regime. When the war began, resistance was minimal, so the United States scored a major victory at minimal price.

*Psychological Offense and Defense (*xinli jingong yu fangyu; 心理进攻与防御*)*

"Offensive psychological warfare" (*xinli zhan jingong*; 心理战进攻) typically employs specially prepared information and attendant media and other transmissions to influence the adversary's decision making and reduce its will to fight. The goal is to sway the will of the enemy's military, leadership, and population, minimizing the cost of victory.[92] Ideally, offensive psychological warfare will induce an adversary to surrender without fighting. Various methods include psychological propaganda, psychological deception, psychological deterrence and coercion, and psychological influencing and alteration. It often employs electronic and network warfare to disseminate information or enhance effects.

"Defensive psychological warfare" (*xinli zhan fangyu*; 心理战防御) counters and fends off the enemy's psychological attacks, steeling one's own psychological defenses. Proper defense requires countering the adversary's likely psychological warfare methods. Because the enemy's psychological warfare efforts are likely to begin well in advance of actual hostilities and will target not only military but political, economic, cultural, religious, technical, and societal elements, Chinese analysts see defensive psychological warfare as a complex piece of systems engineering, requiring a long-term, detailed approach.[93]

Just as electronic warfare and network warfare are seen as an integrated whole, many Chinese writings also specifically note the existence of "network psychological warfare" (*wangluo xinli zhan*; 网络心理战). A subset of psychological warfare, it involves computer networks as the means of undertaking psychological warfare, ranging from dissemination of propaganda to psychological deception and intimidation.[94] Like other types of psychological warfare, network psychological warfare's ultimate goal is undermining the adversary's will and creating dissent and problems in the enemy's camp. Similarly, the PLA sees "cyberelectromagnetic space" (*wangluo dianci kongjian*; 网络电磁空间) as melding the physical, information, and cognitive realms.[95]

EMERGING FORMS OF INFORMATION WARFARE? COMMAND-AND-CONTROL WARFARE AND INTELLIGENCE WARFARE

In addition to electronic warfare, network warfare, and psychological warfare, there has been growing discussion in Chinese literature of "command-and-control warfare" and "intelligence warfare." This suggests that PLA views of how to achieve information dominance are still evolving.

The Chinese shift from focusing on "local wars under high technology conditions" to "local wars under informationized conditions" reflected a PLA conclusion that not all high technology is equally consequential; information-related technologies are of paramount importance. Similarly, Chinese analysts seem to be concluding that the networks, electronics, and commanders that undertake command and control and intelligence functions must be prioritized, if one is to successfully establish information dominance.

Indeed, given Chinese conceptions of future local wars under informationized conditions as systems-on-systems conflict, focusing on command-and-control warfare and intelligence warfare are logical outgrowths. Both entail key nodes that are themselves systems of systems, linking together a variety of other systems. Attacking and degrading either or both the command-and-control and intelligence systems would therefore generate wide-ranging effects.

Command-and-Control Warfare (*zhihui kongzhi zhan;* 指挥控制战)

Insofar as unified joint operations are the cornerstone of future local wars under informationized conditions, effectively implementing command and control (C2) of various forces is vital. These forces will span battlefields that incorporate outer space and the virtual reality of network space. The various systems of systems must be effectively directed and coordinated. As Chinese

CHINESE CONCEPTS OF COMMAND AND CONTROL

The Chinese define "command relationship" (*zhihui guanxi*; 指挥关系) as the relationship between the commander and his command organs on the one hand, and the assigned units that operate underneath him.[97] It is typically based upon how the force is organized, and organizational relationships that result. In some instances, a command relationship may be more ad hoc, for example, if a senior commander allocates specific missions or responsibilities to a particular subordinate or otherwise alters an organization.

The Chinese define "control relationship" (*kongzhi guanxi*; 控制关系) as the relationship between the commander and his command organs on the one hand, and those forces operating within a given operational area that are not normally subordinate to that commander.[98] A control relationship is based upon assignments by the highest-level authority conducting an operation. The PLA volume on terminology notes that control relationships often only refer to activities of units providing support.

For the Chinese, the most important aspects of command and control are:[99]

- "Setting the ultimate goals and aims," for which command and control are exercised;
- "Collecting and assessing information," to effectively implement command and control;
- "Determining missions and assigning responsibilities" for subordinate forces, as well as determining relationships between and among those forces; and
- "Determining rules and limitations" governing subordinate forces' activities while fulfilling missions in pursuit of established goals and aims. This would include establishing rules of engagement.

The Chinese concepts clearly resemble, but are not congruent with, the U.S. military's definitions of these terms.[100] The U.S. military defines "command" as "the authority that a commander in the armed forces lawfully exercises over subordinates by virtue of rank or assignment."

It defines "command relationships" as "the interrelated responsibilities between commanders, as well as the operational authority exercised by commanders in the chain of command; defined further as combatant command (command authority), operational control, tactical control, or support."[101]

It defines "operational control" as "the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative mission direct necessary to accomplish the mission."[102]

analyses conclude, C2 systems and networks must smoothly operate for the effective employment of physical and virtual capabilities and forces.[96]

With the development of improved information technologies, commanders and their staffs are now better enabled to share information and engage in the C2 activities necessary for unified joint operations. At the same time, however, both sides' C2 structures will be priority targets.

This dilemma underlies the Chinese concept of command-and-control warfare. As the Chinese define it, "command-and-control warfare" (*zhihui kongzhi zhan*; 指挥控制战) is the comprehensive use of various means, including electronic warfare, network warfare, psychological warfare, military deception, firepower attacks, as well as safeguarding one's own plans and information, to attack and degrade the enemy's ability to undertake command and control, while preventing them from doing the same to oneself.[103] Chinese analysts see command-and-control warfare as a refined expression of "information conflict" (*xinxi duikang*; 信息对抗).[104]

The rise of command-and-control warfare reflects the larger Chinese realization that joint operations are no longer a matter of *physical jointness*, where forces interoperate within the same physical space but instead requires *informational jointness*, where information can be shared among all commanders, of whatever service, level of command, or operational role.[105] Indeed, information is most melded and fused within the joint C2 structure, as disparate types of information drawn from a range of sources are combined and analytically related to each other by various command organs, staffs, and personnel.[106] The commander and staff is the ultimate node in informationized warfare.

Ideally, successful command-and-control warfare attacks the adversary's ability to employ the information it possesses by influencing, attriting, and destroying their ability to make decisions, exercise command, and control information flow. The enemy will be unable to understand the battlefield situation; even if it can, its decision making will be retarded and its abilities to plan and communicate will be hindered. This will cripple the enemy's ability to plan actions or respond to developments. At a minimum, the enemy will lack the command capacity to effectively challenge one's own efforts to secure the initiative. If very successful, command-and-control warfare will paralyze the enemy and compel it to submit.

In many ways, command-and-control warfare is the next step in establishing information dominance. As noted earlier, a core concept underlying the Chinese view of future local wars under informationized conditions is forging shared operational pictures across participating forces. This requires establishing a smooth flow of information.[107] In particular, from the Chinese perspective, that flow must be unimpeded among the various C2 elements, so that the various decision makers (i.e., commanders and command organs) can understand the situation, formulate plans, and order

their implementation. Only in this manner can one effectively and efficiently employ all the available resources.

Command-and-control warfare strives to prevent an adversary from exercising effective command and control by denying them the information flow necessary to effect the OODA Loop. While it encompasses various aspects of network warfare, it targets more than just computer networks.[108] Rather, command-and-control warfare operations try to disrupt the entire array of the adversary's command-and-control systems, from the national strategic information and C2 systems to battlefield sensors.[109] Denied the smooth flow of information, effective C2 is impossible, as decisions cannot be accurately made, promptly disseminated, and properly implemented. Individual forces cannot share their knowledge, nor act in a coordinated, much less unified, fashion. They face defeat in detail or else are made irrelevant to the larger campaign.

In addition to hindering information flow to key decision makers, command-and-control warfare prevents accurate decision making. Since the goal is to prevent effective control of forces, inducing bad decisions, even if good information is available, is a metric of success in command-and-control warfare. As Chinese analysts have observed, effective C2 capabilities are necessary to exploit the informationized nature of weapons, their long-range striking capability, or to make accurate judgments and convert those judgments into action.[110] Command-and-control warfare strikes all the components of the OODA Loop.

Chinese analysts believe that recent "local wars under informationized conditions" have already foreshadowed the rise of command-and-control warfare. According to one PLA assessment of the 2003 Iraq War, the United States recognized that information warfare would directly affect the enemy's command-and-control and early warning systems, attriting the "enemy's integrated combat capability" (*di zhengti zuozhan nengli*; 敌整体作战能力), and creating the conditions for smoothly implementing America's own operational plans.[111]

In that conflict, a major element of the American effort, from the Chinese view, was the effort to decapitate the Iraqi military and political leadership, including targeting Saddam and his top advisors. The Chinese believe that this reflects a fundamental reality of informationized conflict in general but especially how the United States conducts such conflicts. "In the course of undertaking information warfare . . . one should obey the principle of 'decapitation,'" which entails:

- Striking first, against the enemy's national command structure, joint military staffs, and war-zone commands;
- Paralyzing the enemy's command systems, including battlefield information and reconnaissance systems, information management centers, and decision-making networks;

- Disrupting all enemy information channels, including telephones, radio and television broadcasting systems; and
- Preventing the enemy from using third-party communications networks, including communications satellites.[112]

Other Chinese assessments similarly conclude that, in any future conflict, the enemy will employ precision munitions, electronic and network attack methods first and foremost against C2 networks and systems, as well as weapons control and guidance systems (e.g., air defense network command centers), and logistics and safeguarding systems.[113] If successful, decapitating strikes will neutralize C2 systems and associated communications and information networks, and effectively paralyze the force. While recovery is possible, in the interim, there would be mass confusion, leading to loss of control and coordination, and a general loss in operational effectiveness.[114]

Command-and-control warfare is not envisioned as an alternative to electronic warfare, network warfare, and psychological warfare. Rather, it helps achieve information dominance, in conjunction with these other approaches, reducing the adversary's overall ability to gather and exploit information through battlefield observation, decision making, and C2 activities.[115]

Command-and-control warfare is just more precisely focused, prioritizing electronics, networks, and psychologies associated with command for targeting and defense. For example, command-and-control warfare would still apply INEW methods but would concentrate on those networks and electronics that support the enemy's commander and staff.[116] The widespread connectivity engendered by the Internet, and general dual-use nature of a nation's computer networks, makes it far easier for hackers to deploy logic bombs and engage in offensive information activities, in the Chinese view.[117]

At the same time, command-and-control warfare, as with the broader information warfare concept, still incorporates physical attacks and destruction. Special operations forces, precision munitions, long-range strike platforms such as bombers and cruise missiles are seen as useful means of degrading the adversary's command-and-control systems every bit as much as jamming and computer viruses.

Intelligence Warfare (*qingbao zhan;* 情报战)

The ability of commanders to properly identify and respond to the adversary's actions, allocate and deploy friendly forces in response, and coordinate its actions effectively will depend upon obtaining timely intelligence. Only by determining the adversary's intended activities and plans, understanding its characteristics and nature, and accurately analyzing its structures, organization, and personnel, can one effectively target their command-and-control systems and formulate effective attacks.[118] This is the essence of intelligence warfare.

The PLA defines "intelligence warfare" (*qingbao zhan*; 情报战), also referred to as "intelligence conflict" (*qingbao douzheng*; 情报斗争), as encompassing both sides' efforts to safeguard one's intelligence information while acquiring it from the other.[119] It complements command-and-control warfare, since it provides commanders and their staffs with essential information needed for proper campaign planning and coordination.

According to the PLA, intelligence warfare, in the narrow sense, is focused on military activities to obtain information but may include information about not only the adversary's military but also its political and economic situation.[120] Intelligence warfare will include assets that are land-based; sea-based, including surface and subsurface platforms; aerial; and space-based.[121] It includes electronic intelligence, signals intelligence, and intelligence about the enemy's various networks. It also includes accurate, prompt analysis of collected information. (In the broader sense, any effort to obtain information about almost any aspect of an adversary, including political, economic, military, scientific and technological, cultural, or diplomatic information may be considered part of "intelligence warfare.")

Since the targeted information, even in the narrow sense of "information warfare," goes beyond the purely military realm into economics and politics, Chinese reference to "military activities" refers to the types of personnel and means used, rather than the types of operations such intelligence is intended to support.

Elements of intelligence warfare include:

- Collection and analysis of information, regarding both enemy forces and battlefield conditions;
- Determining the main operational direction, to prioritize information collection and effecting deception;
- Determining the methods and targets for information collection and implementing deception operations;
- Formulating plans for disseminating false and misleading indicators and activities;
- Organizing and undertaking such dissemination efforts; and
- Monitoring the results of such efforts, and implementing adjustments and modifications.[122]

Intelligence warfare therefore encompasses all the various policies, strategies, plans, and activities involved in both gathering information for oneself and denying it to an adversary, as part of the larger set of operational efforts associated with local wars under informationized conditions.

Wars throughout history have seen the two sides struggle to learn more about the adversary's location, composition, plans, and capabilities, while

preventing it from doing the same. However, in the Chinese view, the proliferation of information and information technology has been so extensive, and the role of information is now so salient, that this struggle has become a separate style of warfare. Commanders now have an unprecedented ability to understand the battlefield and shape developments, due to the availability of near-real-time intelligence.[123] Intelligence has shifted from primarily a supporting function undertaken in advance of conflict to an integral part of ongoing operations.[124]

Real-time information flow allows prompt exploitation of intelligence, and midcourse corrections of ongoing joint operations. Consequently, acquisition and denial of intelligence will be decisive, and there will be intense struggles not only at the strategic level (as has long been the case) but in support of operational and tactical operations. All of the activities that are part of intelligence warfare, in the Chinese view, must be implemented in a deliberate, planned manner, in coordination with other activities (maneuver, attack, defense), if one is to better collect more accurate intelligence in a timely manner, while denying an adversary the same.

Along with command-and-control warfare, intelligence warfare focuses electronic warfare, network warfare, and psychological warfare operations against a particular subset of capabilities and targets. Indeed, intelligence warfare and command-and-control warfare are fundamentally complementary and very much intertwined.

Intelligence Warfare Straddles Peace and War

Because the pace of informationized warfare is so accelerated, and requirements for intelligence are so much greater, intelligence warfare cannot wait for the formal commencement of hostilities to begin. Vulnerabilities must be identified well in advance if they are to be fully exploited. Also, it is vital to map the adversary's chains of command and decision-making processes, in order to identify key nodes, decision makers, and potential informational choke points to attack.

Such information can only be derived through extended study of the adversary and extensive analysis of that information. Not surprisingly, Chinese analyses emphasize that establishing information dominance requires collecting and analyzing intelligence well before hostilities commence, and sustaining these efforts throughout the course of the conflict.[125] Indeed, intelligence warfare is seen as so intense and unrelenting that obtaining "intelligence advantage" (*qingbao youshi*; 情报优势) requires unceasing information gathering, and both reconnaissance and counterreconnaissance activities.[126]

Interestingly, Chinese authors also suggest that intelligence warfare can serve as a deterrent to conventional warfare. Intelligence information can now

strike the enemy's goals, as well as support other military operations. One may exploit intelligence to create an advantage, such as by revealing the adversary's intentions or activities, thereby disrupting its plans, creating suspicion among third parties or allies, and sowing doubt about prospects of success. As important, one can undertake "intelligence deterrence," or "intelligence coercion," through a clear display of one's superior intelligence capabilities. This can create psychological pressures to influence adversary and third-party assessments.[127]

Key Intelligence Warfare Tasks

Successful intelligence warfare applies electronic warfare, network warfare, and psychological warfare, organizing it to obtain information about the adversary, while denying it to the enemy.

In waging intelligence warfare, Chinese analyses emphasize certain additional aspects.

Obtaining reliable information in a timely fashion. The intelligence required for unified joint operations obviously must be reliable, but it must also be timely. Intelligence assets must locate and monitor the enemy forces, activities, and plans, and under a variety of conditions at all times. This, in turn, requires that intelligence be collected from a variety of sources including land, sea, air, space, and cyber; throughout the day and night and under all weather conditions; and incorporate various means, including microwave, infrared, as well as visible light, sounds, and hydrographic. Only a diverse array of collection methods can support reconnaissance and surveillance under all conditions.

As important, a varied collection platforms and systems complicates an adversary's attempts at deception and information denial, since the enemy must consistently deny information across all the various means. It is one thing to counter electro-optical sensors; it is more difficult to also conceal the object from synthetic aperture radars, infrared sensors, and electronic surveillance methods.

Intelligence warfare requires reliable information about not only enemy forces but also battlefield conditions. An integral part of intelligence warfare is gathering and analyzing information about the battlefield environment. Meteorological and hydrographic information must be up to date. Geodesy data, including slight shifts in the earth's magnetic and gravitational fields, will affect missile trajectories, especially over longer ranges. Differences in water temperature can create layers and thermoclines, which will influence sonar receptivity. Atmospheric conditions and space weather can affect electromagnetic propagation, especially for systems such as over-the-horizon backscatter radars but also for radios and radars.

In addition, it is necessary to understand the virtual environment of network space. This is difficult even in peacetime, as new nodes are added,

passwords change, servers and routers go offline. An adversary's network space will likely rapidly change and potentially become less vulnerable, once it is in crisis mode. Previous vulnerabilities may no longer be exploitable if the adversary severs connections to the broader Internet, activates previously dormant networks, or implements new security protocols.

Intelligence must be rapidly and precisely transmitted. Successful intelligence requires prompt collection and exploitation of information. Analysts need access to all this information to properly assess it, and the resulting conclusions must be rapidly forwarded to relevant decision makers. This information flow must be prompt yet secure, since the longer the intervals between collection, analysis, and dissemination, the less accurate and relevant the final product will be.[128]

In order to successfully conduct information warfare, intelligence networks and systems must have sufficient bandwidth to meet the demands for reconnaissance, early warning, command, coordination, and safeguarding, even when confronted by enemy action.[129] It does little good to collect information, if one is then stymied in transmitting it from collector to analyst, or from analyst to commander and staff.

Intelligence information and associated networks must be safeguarded. An essential part of intelligence warfare is ensuring that one's own information is kept secret; denying an adversary access is a top priority. Information security measures, for example, keeping classified materials secure to concealment and deception measures, are fundamental parts of intelligence warfare.

In addition, maintaining communications and data relay connectivity and integrity is a prerequisite for successful intelligence warfare. Those networks must be secure from enemy physical, electronic, and network penetration. At the same time, information transmitted across those networks must also be protected from adversary interference, including alteration, deletion, as well as interception. Defensive INEW is intimately linked with intelligence warfare.

*Counterintelligence Activities (*fan qingbao huodong; 反情报活动*)*

Chinese discussion of intelligence warfare often emphasizes counterintelligence activities. Denying information about oneself is as important as obtaining intelligence about the adversary. Information collection and denial measures must be coordinated but, when they work in tandem, are mutually supporting. Thus, a better ability to collect intelligence about the enemy, for example, can reveal one's own security failures and vulnerabilities.

The 2007 edition of the *PLA Encyclopedia*'s volume on military intelligence specifies that there are two counterintelligence activities components; an offensive and a defensive one.[130]

Offensive counterintelligence activities involve offensive operations against the adversary's intelligence collection and analysis networks and systems. One element of this is the deliberate effort to mislead an adversary. The concept of stratagem (*moulue*; 谋略) occupies a central place in both command-and-control warfare and intelligence warfare; indeed, it is a key link that ties the two elements together.

As Chinese writings note, through effective intelligence collection, one can identify the adversary's biases and perceptual blind spots.[131] The planning and organization of deceptions can then exploit these vulnerabilities, making deception more believable. This was part of the success of Allied deception efforts supporting the Normandy invasion. Because both Hitler and the German General Staff were convinced that any invasion would require the seizure of a suitable harbor, Allied deception efforts pointing toward Calais as the ultimate invasion site found easy acceptance.[132]

Once an adversary's intelligence collection plans and activities are identified, offensive counterintelligence activities will seek to actively disrupt them by attacking the collection assets, intelligence centers and networks, and communications systems. This can be through firepower attacks, INEW, human agents, and so on. Such disruptions and attacks must be carefully coordinated, however, since those same efforts, networks, and systems are paths for channeling false and inaccurate information to enemy commanders.

Defensive counterintelligence activities comprise measures to ensure the security of one's information, protection of facilities, and otherwise frustrating adversary intelligence collection. The goal is to mislead the enemy regarding one's capabilities and intentions. In some cases, this may lead them to overestimate, in other cases, it may try to make them underestimate. Stealth, deception, camouflage are all aspects of defensive counterintelligence activities, which also include limits on electronic emissions and concealment of heat signatures, as well as more traditional physical concealment and camouflage.

Preventing an adversary from accessing and exploiting one's information networks, and limiting damage should they nonetheless succeed, is also vital to defensive counterintelligence. Thus, the Chinese see electronic and network deception, as well as data encryption, as vital parts of defensive counterintelligence activities.[133] Network warfare is especially powerful, because it can affect the entire adversary society.

Both offensive and defensive counterintelligence operations must be properly orchestrated in order to mislead the enemy's military decision makers and its broader society.[134] They must be mutually supporting and not contradictory. They must also support the larger array of military operations and ultimately must serve to help achieve the operational and strategic goals of the conflict.

ASSESSING CHINESE VIEWS OF INFORMATION WARFARE

For the PLA, information warfare brings together various disparate trends that have emerged since the first Gulf War. It reflects the evolution of warfare from the Industrial Era to the Information Age. The need to operate jointly, across multiple domains, to incorporate a variety of high technology, especially information technology, to handle vast amounts of information simultaneously, poses a daunting challenge to the Chinese military leadership. This is exacerbated by the lack of combat experience, as the PLA has not fought a war since 1979.

As the PLA has sought to modernize itself and accommodate the major changes in the conduct of warfare, it has often found itself failing to keep up with the accelerating pace of change. Even as the PLA was assessing the first Gulf War, the NATO intervention in the Balkans provided a very different model of how future wars might be conducted. Similarly, the American invasion of Afghanistan and the toppling of the Taliban, and the American invasion of Iraq in 2003, each followed a different pattern than what had occurred in the first Gulf War or the Balkan intervention.

Nonetheless, based upon a close examination of the common characteristics among these previous "local wars under informationized conditions," the Chinese have concluded that establishing information dominance is the key to winning such wars. From the Chinese perspective, the common denominator linking these conflicts is information dominance. The side best able to dominate information collection, transmission, and exploitation is the one that attains victory. As a result, not only have they devoted a substantial effort to parsing the types of efforts necessary to establish information dominance (e.g., integrated network and electronic warfare), but they have also been practicing various types of information operations in peacetime, in expectation of having to conduct them in wartime.

5 Chapter

Information Operations: Putting Theory into Practice

Chinese concepts of informationized warfare and information warfare emphasize establishing information dominance, while denying an adversary the ability to do the same. Information dominance first requires information support for the PLA's own military activities. The PLA will also have to conduct offensive information operations against adversaries, to deny them the ability to exploit information. At the same time, the PLA will be engaging in defensive information operations to ensure the continued availability of information support to its own forces. Finally, as part of the portfolio of information operations, the PLA must also be able to undertake information deterrence activities.

All of these information operations incorporate elements of electronic warfare, network warfare, and psychological warfare, undertaken in coordinated fashion with each other and with other military activities on land, sea, air, and outer space. Information operations support broader offensive and defensive activities, as well as logistics and safeguarding operations. Similarly, they will be incorporated in PLA activities ranging from positional defense to guerrilla warfare or mobile operations.

INFORMATION SUPPORT OPERATIONS

In order to establish information dominance, Chinese analysts stress the importance of managing the enormous amount of information obtained and generated by advanced electronics and sensor networks. Joint campaigns under informationized conditions will require smoothly and effectively gathering and applying available information. This requires comprehensive yet accurate information that is usable by decision makers.

Information support operations will therefore demand an extensive array of information collection, transmission, and exploitation means, including sensors and communications equipment. They will also require creating standardized databases and other information storage and management methods, so that all participating forces and personnel can access and use available information, regardless of source. This is essential, since rapid examination and application of information is essential in joint campaigns.

Information management needs to be flexible and responsive, as battlefield conditions evolve. More perishable information needs to be promptly forwarded, while it is still relevant to battlefield developments. At the same time, old information must be removed from the system, so that it does not clutter or obscure incoming data. Prompt absorption and supplementing of information is central for establishing and maintaining information dominance.[1] Consequently, there must be standardization of joint campaign information databases, so that all the participating forces and personnel can use the information, regardless of its original source.

Components of Military Information Systems[2]

PLA writings suggest that it categorizes "military information systems" (*junshi xinxi xitong*; 军事信息系统) in several different ways. One is by the system's location in the course of information flow. Thus, there are information collection systems, information transmission systems, information management systems, and information display systems.

Information Collection Systems

Information collection systems provide commanders with the means to assess battlefield developments and make suitable decisions. They comprise the intelligence networks that monitor land, sea (including subsurface), air, space, and network space domains. These span the gamut from fixed information collection sites and radars to reconnaissance vehicles, intelligence-gathering ships and aircraft, unmanned aerial vehicles, and reconnaissance and missile early warning satellites.[3]

Information Transmission Systems

Information transmission systems link collection systems to analysts and then to decision makers and operators. These systems include communications networks, data networks for air defense system (including SAMs, interceptors, antiaircraft artillery), and logistics support structures. Given the General Political Department (GPD) role in managing the PLA, as well as its responsibility for overseeing military political reliability, it is possible that it may have a dedicated, discrete information transmission systems.

Information Management Systems

Information management systems convert raw data into useful information that commanders and operators can act upon. These systems join, categorize, archive, update, analyze, and coordinate information gained from various information collection systems. The information management system also includes the commanders and staffs who are making decisions. This system is the core of military information systems of systems. Their smooth operation will be decisive in obtaining information dominance.

Information Display Systems

Information must be expressed in ways useful to both analysts and users. Consequently, knowing how to display information is an important part of information management. Information display includes graphics, spreadsheets, images, as well as words. Depending upon the audience, information display also includes aspects of information dissemination (which, in turn, makes it relevant to political warfare efforts); thus, information display systems also include television programs, movies, newspapers, and Internet content.

Alternatively, PLA analysts categorize information systems by types of supported missions and activities. These include command and control; intelligence, surveillance, and reconnaissance; military communications; navigation and positioning; battlefield support and safeguarding; and information security. The ability to conduct command-and-control warfare and intelligence warfare, as detailed in the previous chapter, ultimately rests on these various information systems operating normally.

Command-and-Control Systems

These are the most important of the military information systems, allowing commanders and staffs to control units and conduct battles. The command-and-control (C2) systems necessary for unified joint operations include an array of subsystems, including command facilities, combat support and combat service support functions, and civil–military linkages that civilian assets to supplement military functions. The various elements of information warfare, including electronic and network warfare as well as psychological warfare, are ultimately aimed at the C2 systems and the personnel who staff them.

Intelligence, Surveillance, and Reconnaissance Systems

Chinese analysts differentiate between intelligence-oriented reconnaissance systems and early warning and surveillance systems. Together, they provide commanders and staffs with information about the adversary and

battlefield conditions, including the enemy's deployments and activities, its command post locations, weapons numbers and capabilities, and electronic and physical signatures. In the Chinese view, modern information technology provides unprecedented opportunities for intelligence, surveillance, and reconnaissance systems to monitor the adversary and clear away much of the "fog of war." As components of "intelligence warfare," such systems are central to accurate command and decision making, and their smooth operation is essential to successful unified joint operations.

Military Communications Systems

While communications systems have long played a central role in military operations, the more complex modern battlefield, with its more intense pace of operations, elevates the importance of communications. Commanders and units must maintain communications channels if the former are to receive sufficient information to make decisions, and the latter are to obey orders and coordinate operations. Indeed, the core of unified joint operations is information sharing among units, which requires the smooth operation of communications networks.

Positioning, Navigation, and Timing Systems

The advent of satellite navigation constellations such as the American GPS and the Chinese Beidou allows unprecedented accuracy in navigation and positioning, under all weather conditions, day and night. These systems enable the precision strikes and operations called for in the Chinese strategic guiding thought by determining friendly and enemy locations with high accuracy. As important, they also provide timing signals for a range of functions such as frequency hopping radios and other secure communications methods. Not surprisingly, China has chosen to pursue an indigenous satellite navigation system.

Battlefield Support Systems

Battlefield support systems provide meteorological, hydrographic, and other information regarding the physical and electromagnetic battlefields. A thorough understanding of the physical battlefield, including prompt notification of changes, can decisively affect operational decisions. By systematically eliminating German weather ships and stations, Nazi planners were unable to make accurate weather forecasts. Allied meteorologists, accessing weather stations across the North Atlantic and North America, could forecast a break in the storms that were lashing the English Channel, allowing General Eisenhower to surprise the Germans by launching the Normandy invasion on June 6.

Safeguarding and Logistics Systems

In order to maintain the rapid operational tempo of unified joint operations and sustain participating forces in high-intensity combat, logistical support and safeguarding systems must be integrated into the overall information network. The PLA recognizes that unified joint operations require informationized logistics infrastructures, including medical, POL, transportation, and technical support. It is unclear, from the available literature, whether the General Logistics Department (GLD) maintained its own communications network; if it did, this would provide substantial redundancy for PLA operations.

Information Security Systems

Informationized warfare requires information systems and data be kept secure. Chinese analysts fully expect their information networks to be constantly attacked by both hard-kill and soft-kill systems. Consequently, information security systems are essential, in order to ensure that one's own information networks and data are protected from enemy attack.

Information support systems require not only modern, capable information equipment and networks but also a substantial amount of human capital. Chinese analyses recognize that most commanders will rarely, if ever, need to see original, "raw" information. Instead, the commander's staff must find the most essential pieces of information, weeding out both false and irrelevant data, so that the commander is presented with relevant, actionable information. Simply providing facts, without assessing their significance, is recognized as unhelpful.[4]

Consequently, successful implementation of information operations, including intelligence support, requires an extensive pool of properly trained personnel. For the PLA, intelligence analysts will operate alongside hackers and cybermilitia as part of the broader pool of human talent required for information dominance.

ESTABLISHING INFORMATION DOMINANCE

Even as the PLA supports its own operations with necessary information, it will also undertake a variety of offensive and defensive information operations to prevent an adversary from gathering and exploiting information. These efforts will include the collection, analysis, and exploitation of information about potential adversaries, as well as defense against comparable attempts to hinder Chinese efforts.

From the Chinese perspective, information operations aimed at establishing information dominance are part of unified joint operations. They must be coordinated with operations in the traditional domains of land, sea, and air as well as outer space. It must incorporate not only land, sea, and air forces but

also special operations forces and space forces. They must be consistent with broader strategic-level concerns, including political warfare efforts.

The PLA expects to conduct a number of information operations to attain information dominance. These comprise:

- Information reconnaissance operations;
- Offensive information operations;
- Defensive information operations;
- Information safeguarding operations; and
- Information deterrence operations.

For all of these mission areas, the PLA's responsibilities will probably extend beyond what Western analyses would consider "military." This is especially true for information reconnaissance operations, including the types of targets for both offensive and defensive information operations and information deterrence. This is in part because of the Chinese concept of "comprehensive national power" (*zonghe guojia liliang*; 综合国家力量).

The Chinese assess their overall national security as a function of more than just military elements but encompassing the spectrum of economic, political, diplomatic, and even cultural capabilities. Therefore, national security entails understanding not only adversaries' military capabilities (including weapons performance, military networks) but also economic capacities, and political, military, economic, and diplomatic decision-making processes. Consequently, information operations must be planned, and if necessary undertaken, against this full range of targets.

The PLA, as both a party army and national military, is responsible for more than just preserving China's physical territorial integrity. It is also responsible for deterring and defeating threats to the CCP's role as governing authority, including threats that may emerge from the information domain. Furthermore, the PLA is responsible for improving Chinese security, including promoting comprehensive national power.

As important, because information operations are an integral part of preparations for "local wars under informationized conditions," this suggests that they will rarely be stand-alone efforts. That is, while there may be focused efforts at various types of information operations, especially information reconnaissance, they are undertaken as part of larger, more coordinated efforts.

Information Reconnaissance Operations

Because modern warfare can occur on short or no notice, Chinese analysts believe the separation of wartime from peacetime is increasingly blurred. Combat preparations can no longer wait until the eve of war but must be part of peacetime activities. To support future joint operations, it is essential to

secure information about a host of topics. One Chinese volume lists six areas that information reconnaissance operations must address:

- Adversary guidance, plans, activities and deployments for information operations;
- Adversary reconnaissance and surveillance systems, including details about types, allocation, capabilities, and employment techniques;
- Key adversary information system nodes, including location, staffing, capabilities;
- Adversary methods, tactics, units, and procedures for offensive and defensive information operations; and
- Civilian information facilities, equipment, and personnel that might be mobilized by each side.[5]

The volume then specifically calls for active analysis of possible reactions to Chinese joint campaign information operations, as well as information reconnaissance of other aspects of national power, as necessary. This latter tasking is consistent with long-standing and widespread reporting about Chinese economic espionage, often attributed to Chinese military units. This is one reason why many "advanced persistent threats" are associated with Chinese network attack forces. Such forces engage in extended penetrations and attacks; they are not necessarily stealing money but are extracting corporate secrets or other information, and practicing tradecraft.[6]

CHINESE MILITARY CYBERESPIONAGE AGAINST NONMILITARY TARGETS

Many accusations of Chinese cyberespionage have observed that Chinese military and governmental cyber forces often target information not obviously related to military or even security concerns. The U.S. Department of Justice's indictment of five Chinese officers reportedly belonging to Unit 61398 of the PLA (labeled Advanced Persistent Threat-1, or APT-1, by the computer security firm Mandiant) accuses them of "computer hacking, economic espionage, and other offenses directed at six American victims in the U.S. nuclear power, metals, and solar products industries." The officers are specifically accused of stealing information "that would be useful to their competitors in China, including state-owned enterprises."[7]

The United States is not the sole target of Chinese economic cyberespionage. British officials have warned bankers and other businessmen that the Chinese military is actively employed in electronic espionage against them.[8] An attack on Canada's National Research Council in 2014 was assessed by one computer security specialist as undertaken by Unit 61486 of the PLA.[9]

The apparent use of military computer specialists for economic and technological espionage should not be surprising, as it is consistent with the PLA's national security role. Moreover, as a party army, the PLA is responsible for not

only defending the PRC but also maintaining the CCP's leadership role. Given that growing Chinese "comprehensive national power" is an essential means of maintaining CCP legitimacy, the PLA would naturally be employed in establishing a competitive advantage in the commercial and scientific realms. Similarly, the effort to gain "insight into the strategy and vulnerabilities of the American [commercial] entity," as the Department of Justice charges, are little different, except for target, from the same kinds of information that the PLA is expected to obtain about military and political targets. It is the PLA's job to identify "the strategy and vulnerabilities" of any and all adversaries.

From the Chinese perspective, the cornerstone and pre-requisite for all other efforts at winning future conflicts, including the grand strategic competition with other nations, begins with gaining a better understanding of the adversary's comprehensive national power, including both military and nonmilitary components. As Chinese analysts also believe that civilian and military information networks are "melded" or "fused" (*ronghe*; 融合), any effort at establishing information dominance will inevitably involve more than just military networks.

The intertwined nature of modern economies further pushes for a broad approach to gathering information. Reports of Chinese efforts to penetrate the computer reservation systems of American Airlines and United Airlines, two of the largest American air carriers, may be motivated by commercial concerns (e.g., learning how foreign computerized reservation and ticketing systems work), by an interest in human intelligence (e.g., tracking the travel patterns of certain individuals), or by an interest in strategic airlift (e.g., by monitoring the availability of passenger aircraft, especially those that might be activated as part of the Civil Reserve Air Fleet).

Similarly, given the need for psychological and other information, Chinese targeting of health care companies, including insurers such as Anthem and Premera Blue Cross could provide sensitive information about key individuals' health as well as possible ailments affecting other family members. The hacking of the online dating service Ashley Madison could provide information for recruiting or blackmailing officials, military personnel, and media figures.

In some cases, while the objective may not be military information, there is a clear national security component. In March 2009, the SecDev Group and Information Warfare Monitor identified "Ghostnet." This was a large-scale cyberespionage effort involving nearly 1300 computers in over 100 countries, apparently controlled from computers located in China. Among the targets were such sensitive political figures as the Dalai Lama, as well as computers in various foreign ministries and embassies.[10]

Some of the other groups and activities associated with Chinese computer operators include:

Deep Panda. This is a group of computer operators (advanced persistent threat), also known as "Shell Crew," which has targeted American think tanks, financial institutions, and defense industries since at least 2011. They have also been identified as attacking Anthem, the American healthcare insurance firm, and American experts analyzing the Iraqi security situation.[11] The group is also believed to have created a massive virtual private network (the Terracotta VPN) by infiltrating servers worldwide and hijacking them

for their own use. This includes using the VPN, in turn, to mount penetrations of various other networks by masquerading as a legitimate organization or network.[12]

Icefog. This is a group of computer operators (advanced persistent threat) believed to have infected a number of Taiwanese, South Korean, and Japanese computers. The targets include government institutions, mass media, high technology corporations, telecom operators, satellite operators, shipbuilding and maritime-related corporations, and military contractors. Through phishing e-mails and infected attachments, the Icefog controllers can upload basic system information about infected computers, which will then allow them to run commands on the infected system. The attacker is enabled to steal files and execute commands on certain types of servers (including accessing database contents). Unlike some other attacks, computers infected by Icefog do not automatically download files but are instead individually commanded. Furthermore, there are several hundred recorded infections of Apple machines running Mac OS X. Icefog activities were first identified in 2011.[13]

NetTraveler. This program was found to have infected at least 350 victims across 40 countries. These include government institutions, think tanks, the oil and gas industry, aerospace companies, embassies, and military contractors, as well as Tibetan and Uighur activists. Through phishing e-mails and infected attachments, the NetTraveler program gains access to the target computer, where it then creates a backdoor, and regularly downloads compressed files of data back to command-and-control servers in the United States, China, and Hong Kong. Since it apparently began operating in 2004, it is believed to have exfiltrated at least 22 gigabytes of data.[14]

Night Dragon. This is a group of computer operators believed to have targeted the petroleum and petrochemical sector beginning in 2008 or 2009. Its members are believed to have gained access to Greek, Kazakh, Taiwanese and American executives' accounts. The attackers sought to gain access to company databases, as well as market intelligence reports and production system details. They also tried to upload remote administration tools (RATs) that would make them the equivalent of system administrators, with complete access to the contents of all computers within the network.[15]

Operation Aurora. In December 2009, Google reported that it, along with 20–30 other companies including Adobe, had suffered a highly sophisticated attack aimed at corporate networks. The attackers had been trying to obtain proprietary information from these companies, including access to Google's Gmail servers. This attack, coupled with various Chinese restrictions on Google's operations in China (including censoring Internet search results for people using Google's China version), led the company to withdraw from the China market.[16]

Operation Shady RAT. Identified by McAfee Security systems in 2011, this malware intrusion involved the use of RATs to obtain information from a diverse group of targets including the International Olympic Committee, and Western think tanks, as well as the secretariat of the Association of Southeast Asian Nations (ASEAN).[17]

Titan Rain. This is a group of computer operators, believed to be based in Guangdong, who reportedly have targeted various American and other governments' computers, beginning in 2003 and operating through at least 2005. In one evening in 2004, these attackers reportedly struck the U.S. Army Information Systems Engineering Command, Defense Information Systems Agency, Naval Ocean Systems Center, and a U.S. Army Space and Strategic Defense installation.[18] It is possibly linked to a set of intrusions known as Byzantine Hades, which apparently targeted U.S. military programs.

Another Chinese volume enumerates ten main missions for information reconnaissance forces. These include the following:

- Understanding enemy information operations plans, principles, techniques, and forces, and determining its location and deployment.
- Determining the organization, allocation, and greatest vulnerabilities of adversary information operations forces, information assets, and associated networks, including key nodes such as server farms.
- Tracking information capabilities (and general capabilities) of the adversary's antisystems combat forces, early warning systems, command posts, and communications networks and support forces. The enemy's air defense forces are especially important.
- Determining the natural conditions of potential battlefields, including weather, electromagnetic, hydrographic, and other conditions.
- Determining civilian information structure, assets, and facilities that might be mobilized.
- Understanding adversary military and popular psychological stances. Especially important are views, habits, and characteristics of information operations forces and commanders.[19]

Since the PLA is tasked with undertaking information reconnaissance activities against this array of targets, it is responsible for more than simply reconnoitering potential adversaries' military networks and facilities. This expanded set of information reconnaissance targets reflects the more intertwined nature of informationized warfare, reflected in "comprehensive national power."

Since national power depends upon economic, political, and other elements, as well as military capabilities, it is essential for the PLA to maintain situational awareness about all of them, and if necessary to act against them. Just as strategically the Chinese regard the adversary's broad polity as an essential target for informationized attacks (i.e., political warfare), tactically, the PLA is responsible for holding more than just military networks and systems at risk.

Disrupting an adversary's financial networks can undermine their long-term sustainability and may divert military and political resources in the meantime to cope with resulting chaos. Few dedicated military networks can handle the volume of information informationized wars require; there will be some degree of reliance upon civilian communications infrastructure. This does not mean that the Chinese would necessarily attack an adversary's financial or civilian communications networks. It does suggest, though, that the PLA will be prepared, if necessary, to do so. This, in turn, means that the PLA must assemble the requisite intelligence in advance to successfully attack such networks, should it be ordered to do so.

An incident in April 2010 raised the possibility of very large-scale Chinese information reconnaissance. China Telecom, one of the largest telecommunications providers in China, announced electronically that its system was the preferred route for Internet traffic. For 18 minutes, some 37,000 routes, about 10 percent of the global total, were redirected along China Telecom's networks. (This does *not* mean that 10–15 percent of the world's traffic went through China Telecom, as some contemporary reports suggested. Routes may be heavily or lightly trafficked.) Any information that passed over that network would have been vulnerable. "Operators of those servers would have had the capability to read, delete, or edit unencrypted e-mail and other communications passing through those servers during that time."[20] While this incident was assessed to be a mistake, it suggests one means by which Chinese information warriors could access information (although it would be noticed).

Nonetheless, given the military challenges confronting the PLA, and the need to fight local wars under informationized conditions, traditional military targets are still a priority. Therefore, information reconnaissance activities in support of military operations still include a narrower set of military-related networks and information.

Chinese analysts seem to categorize these information reconnaissance efforts mainly by means employed, rather than type of data gathered. Thus, just as information warfare is divided into electronic warfare, network warfare, and psychological warfare, Chinese writings broadly group information reconnaissance appears into electronic reconnaissance, including radar-based reconnaissance; network reconnaissance, including communications and data reconnaissance efforts and computer network reconnaissance; and psychological or human factor reconnaissance.[21]

"Electronic reconnaissance" (*dianzi zhencha*; 电子侦察) involves various electronic probes and intercepts of adversary electronic emissions to determine their operating frequencies and assess their capabilities. It also includes gathering information through electronic means about potential battlefields. Electronic information reconnaissance targets the adversary's communications systems; electro-optical, infrared, and other sensors; hydrographic

information, such as the sonar characteristics of the adversary's submarines and surface combatants as well as its underwater weapons capabilities.

Electronic reconnaissance also seems to pay particular attention to adversary radar systems, including locations, frequencies, system capabilities, and tactical employment doctrine. In several different volumes of Chinese teaching materials, radar characteristics are specifically prioritized for information reconnaissance.

At the same time, the Chinese treat radar-based reconnaissance as one of the most important elements of electronic reconnaissance. This uses of a variety of different radars, including airborne radars, over-the-horizon radars, ground surveillance radars, artillery-locating radars, and the like, to undertake all-weather, real-time reconnaissance and surveillance of land, sea, and air environments. Increasing availability of synthetic aperture radar (SAR) satellites, such as the *Yaogan* series, supports radar-based reconnaissance much farther from China's shores. Paired with high-resolution imaging satellites, a powerful sensor combination is created for assessing infrastructure, military forces, and so on.

"Network reconnaissance" (*wangluo zhencha*; 网络侦察) activities use computer networks and battlefield sensor networks to collect intelligence information about the adversary. The Chinese assess this as one of the most common, and most important, forms of information reconnaissance activities.[22] Communications and data reconnaissance are especially important, encompassing electronic intelligence (ELINT), signals intelligence (SIGINT), and measurement and signature intelligence (MASINT) data, gathered by air, space, naval, and ground platforms, including unmanned aerial vehicles. Chinese writings differentiate communications and data reconnaissance from electronic reconnaissance by the purpose. Where electronic reconnaissance identifies specific platform characteristics, communications and data reconnaissance efforts are oriented toward determining the structure of command-and-control systems, identifying when and where forces are deploying, and otherwise mapping broader organizational structures that manage various platforms.

Network reconnaissance also penetrates and maps the adversary's computer networks. This can involve exploitation of open source information about the adversary's computer hardware, software and networks, as well as actually penetrating their computer networks, whether through trusted insiders or hacking and decryption. Computer network reconnaissance identifies key enemy computer networks, communications protocols, network administration techniques and procedures, network coordination mechanisms, security protocols, and so on. It also locates and extracts documents and other data for examination, alteration, or elimination.

While network reconnaissance activities may incorporate open source information, it is focused on information that is not publicly available.[23] In

particular, they try to identify the characteristics and weaknesses of the adversary's computer networks, in support of wartime computer attacks, including computer virus deployment. "Only by grasping these types of intelligence can one focus on research and development of 'viruses' to strike enemy networks or focus on implementing defenses."[24]

Chinese information reconnaissance operations also include "psychological reconnaissance" (*xinli zhencha*; 心理侦察). This determines weaknesses in the individual and group psychological outlooks that can be exploited by offensive psychological operations. It includes gathering basic intelligence about individuals, such as biographical details, family circumstances, and career highlights. In addition, psychological reconnaissance about key enemy officers and political leaders will try to determine and assess their self-respect, political views and reliability, and behavior under fire.

Psychological reconnaissance will also try to determine these officers' position and habits within various social networks and decision-making structures. This entails reading and analyzing open media coverage of the individual, books and articles they may have authored, watching interviews they have given, as well as examining private documents and other information (e.g., social media). It also includes, where possible, interacting with specific targets, to gain a better "feel" for their psychological makeup.

Complementing psychological information about individuals is determining the characteristics of the broader social networks that individuals belong to, and which underlie and support various information and electronic networks. The combination of "big data" and data analysis allows analysts to determine relational networks among people, such as who knows whom and who reports to whom.

Psychological reconnaissance also tries to understand the adversary's psychological warfare training, including efforts to build psychological defenses. In particular, peacetime psychological reconnaissance will carefully analyze the adversary's responses to major events, including policies, but also popular perspectives, customs, lines of argument, and perception. Identifying these elements in peacetime is essential for formulating effective lines of attack in wartime.

Offensive Information Operations

Offensive information operations, or information offense, will be among the opening moves in any joint operations, and are the main technique for information warfare.[25] They involve attacks against the enemy's information resources, especially those related to command-and-control systems, information systems, and intelligence systems, in order to leave it blind, deaf, and dumb.

Offensive information operations will block, disrupt, degrade, or destroy the enemy's information collection, transmission, and management systems. The objective is to degrade enemy decision-making capabilities, thereby hampering and retarding its ability to conduct military operations.[26] Offensive information operations are seen by PLA analysts as an essential means of securing information dominance, seizing and retaining the initiative, and ultimately attaining victory.

Because the enemy's information resources are part of a system of systems, offensive information operations are seen holistically. They include attacks against information collection systems, as well as attacks against transmission methods, databases, and key decision makers and decision-making organizations (e.g., staffs). Therefore, they encompass a broad range of activities, including electronic interference, electronic deception, computer network attack, physical attacks, and psychological attacks to assault the enemy's information systems.

When conducting offensive information operations, a foremost task is disrupting all adversary information operations. One priority is preventing the enemy's information networks from effectively collecting, transmitting, or exploiting information. Especially important are reconnaissance and early warning networks; command, control, and communications systems; air defense and ballistic missile systems. Electronic and network offensive operations must be combined with psychological offensive operations and firepower attacks, to maximize synergies. The various offensive information operations must also complement other parts of the overall joint campaign, supporting outer space, air, and maritime dominance efforts.

Ideally, Chinese offensive information operations would impose an information blockade around an adversary. The enemy's ability to gather, analyze, transmit, and exploit information would be so systematically degraded that, while individual systems may function close to normal, its overall situational awareness would be severely impaired. Similarly, while individual units may still retain some effectiveness, the ability to coordinate operations to counter Chinese actions, much less challenge the PLA for information dominance or battlefield initiative, would be a forlorn hope.

Key Considerations for Offensive Information Operations

Chinese writings suggest that, in undertaking offensive information operations, commanders must keep in mind certain considerations.[27]

Offensive information operations will play a leading role within larger joint operations. Because joint operations require more information support, securing information dominance must be a top priority. Therefore, the joint campaign headquarters must thoroughly prepare to seize and retain information

dominance. Undertaking offensive information operations will be the opening move in future unified joint operations. These will include offensive operations as part of all elements of information warfare, that is, electronic warfare, network warfare, intelligence warfare, psychological warfare, and command-and-control warfare.

Offensive information operations will be necessary throughout the course of a conflict. Offensive information operations will be necessary to support all other campaign activities, to help assure their success. Indeed, "it may be said that all operational activities and operational environments will require the support and assurance of offensive information activities."[28] In addition, the Chinese believe information dominance is a dynamic, not static, condition. As the two sides interact, there will be a constant need to counter the adversary's attempts at achieving information dominance by launching regular offensive information operations to keep them off-balance and degrade its information operations.

Offensive information operations will permeate all elements of future local wars under informationized conditions. The Chinese do not expect offensive information operations to be limited to certain targets, certain weapons, certain parts of the battlefield, or a specific period. Instead, such operations will be a fundamental part of all unified joint operations, and therefore electronic warfare, network warfare, psychological warfare activities will be integrated into all other battlefield activities. Thus, offensive information operations will be part of broader offensive and defensive operations, will be incorporated into positional defense, mobile operations, guerrilla warfare or irregular warfare operations, and are part of logistics and safeguarding activities as well as frontline combat. Conversely, the Chinese do not seem to envision information operations occurring in isolation; that is, there is no evidence that the PLA will conduct only offensive information operations without attendant kinetic activities. While there may be phases of operations where offensive information operations dominate, unless the adversary promptly concedes at the outset, other military operations will also occur.

These considerations should be part of all offensive information operations include offensive electronic operations, offensive network operations, offensive psychological operations, and integrated information–firepower attacks against the enemy's information systems.

Offensive Electronic Operations

One of the first moves to establish information dominance will be offensive electronic operations, which the Chinese believe will be decisive in determining a conflict's course and outcome.[29] The ability to dominate the electromagnetic spectrum will allow friendly forces to collect, transmit, and

manage information more freely than the adversary, which will in turn lead to dominance of the land, sea, air, and outerspace domains.

Offensive electronic operations will be intense, requiring extensive coordination among all participating forces (not just electronic warfare forces), both to establish dominance and to minimize interference among friendly forces and activities. Key activities in offensive electronic operations will include electronic interference, physical destruction of key enemy systems, and electronic deception.

Chinese commanders undertaking offensive electronic operations are likely to follow certain guiding principles.[30] A central theme is careful, extensive planning under a unified command. The electronic warfare attack efforts will follow a carefully laid down plan, at least initially, integrated with other elements of the joint operational plan. Since Chinese electronic systems must operate at the same time the enemy's systems are being attacked, jamming systems (especially barrage jamming) and friendly emitters must be deconflicted. Similarly, some enemy electronic networks may have been penetrated by friendly network warfare forces. Physically destroying such systems may close off a source of intelligence or may be less useful than employing offensive network operations. Adopting integrated network–electronic warfare and integrated information–firepower warfare rather than a purely electronic warfare-focused approach, is essential.

From the Chinese perspective, electronic systems include emitter arrays (antennae, radar dishes); the transmitting and receiving instruments; and signals management technology (mainly software). Offensive electronic operations are those which affect any or all of these elements.[31] In each case, the Chinese will undertake a combination of active and passive measures, incorporating hard-kill and soft-kill techniques, against each of the components to degrade and disrupt their operational capability.[32]

Chinese offensive electronic operations will concentrate on adversary *radar networks*, while preserving their own. Countering the enemy's radar networks include destroying as well as jamming them. The Chinese manufacture a variety of antiradiation missiles (ARMs), such as the YJ-91, believed to be a Chinese version of the Russian KH-31 (NATO designation: AS-17 "Krypton"), and the CM-102. The latter is reportedly an indigenously designed, supersonic missile with seven-meter accuracy, making it capable of targeting shipborne radars such as AEGIS as well as fixed land sites.[33]

Efforts to counter the adversary's radar systems also include measures to avoid detection by their radar systems in the first place. Both Chinese combat aircraft and surface combatants have increasingly integrated stealth into their designs, and are believed to incorporate low observable materials in their manufacture. Countering radar systems also involves tactics such as deceptive routing, modifying target profiles so that their radar signature is altered, or

otherwise misleading an adversary's radar networks about a target's identity, course, and intentions.

Another priority target for offensive electronic operations is the adversary's *communications networks*. Given the centrality of smooth communications to command-and-control warfare and intelligence warfare, their disruption is essential. Offensive operations against those networks can include broad efforts to degrade the entire network, such as barrage jamming and other suppressive efforts; focused attacks against individual sites and nodes, including both physical and electronic means; and otherwise blocking the function of certain communications paths.

The ability to precisely attack targets, but also to coordinate force movements across vast expanses, relies upon modern *navigation systems* providing constant, accurate data. By denying or obstructing an adversary's access to accurate navigational information, one can disrupt both weapons operations and broader tactical and even operational maneuvers, significantly reducing their effectiveness.

Offensive information operations against navigational systems includes jamming and dazzling navigation systems, providing spurious navigation information, or destroying sources of navigational data. China markets a variety of commercial GPS jammers. In 2014, the U.S. Federal Communications Commission (FCC) filed a complaint against C.T.S. Technology of Shenzhen, charging that this one company marketed 300 models of GPS jammers within the United States alone.[34] The Chinese could also mount attacks against the enemy's navigation satellite constellations; its tracking, telemetry, and control networks; and its satellite mission control centers.

Against such priority targets, PLA writings emphasize the need to commit the best available forces. The Chinese do not expect to secure permanent advantage in the electromagnetic spectrum. Instead, they hope to create periods of significant advantage, forcing gaps through which forces can penetrate or otherwise operate relatively unhindered. This will depend on creating conditions of local superiority, by massing their best forces, weapons, and capabilities.[35]

Offensive Network Operations

Consistent with INEW, offensive network operations will complement offensive electronic operations. The Chinese concept of offensive network operations does not completely align with American concepts of computer network attack. For the United States, computer network exploitation, cyberespionage, is often considered separate from computer network attack. The latter is presumed to include destruction or alteration of data or operating systems, and is different from eavesdropping or spying. The difference, however, may be indistinguishable until the last moment.

Chinese analyses, on the one hand, also recognize that the distinction between network reconnaissance operations and offensive network operations

may simply be a matter of a few key strokes or lines of code. However, the Chinese have a more integrated view of computer network operations in general, without an absolute divide between network reconnaissance activities and offensive network operations. Some types of reconnaissance activities (e.g., identifying key people, mapping networks) may be necessary for offensive network operations, while offensive network operations, such as active measures to penetrate adversary networks, open the way for further reconnaissance activities.

One Chinese analysis suggests that offensive network operations involve four distinct targets, each involving a different approach.[36] The first is to penetrate the security "walls," breaking through firewalls and other security barriers protecting key information networks, such as command-and-control systems. Engaging in phishing attacks to obtain passwords; exploiting Trojan horses, backdoors, and other implanted holes in security systems; or employing virtual private networks (VPNs) to tunnel through or under firewalls are all part of the network offensive operations portfolio, laying the groundwork for other, potentially more decisive measures.

Another approach is to break apart the "network," preventing the adversary's networks from operating as an integrated, unified whole. By disrupting network operations, the enemy's combat forces and combat activities cannot effectively share information or coordinate activities. Particularly vulnerable will be nodes that link different national forces (when confronting a multinational force) or different services (e.g., those serving a joint force headquarters). Disrupting such network components will have greater impact than disrupting those between tactical formations, and should be a high priority.[37]

The system of systems construct can also be attacked by undermining the network's "resources." By attacking supporting communications, power, and other associated networks, the larger system of systems is deprived of electricity, communications channels, and so on, potentially shutting them down. Similarly, by attacking adversary reconnaissance and early warning system, the enemy cannot obtain intelligence, leaving commanders uninformed about situational developments, and therefore unable to coordinate responses.

Securing "points" to control the network can also reap important rewards. If one can shut down or control parts of the adversary's network in advance, then one can disrupt the entire system, in turn affecting the overall system of systems. Ideally, one can take direct control of all or part of a network after gaining access. Depending on the level of control, this can effectively place some or all of the network's normal functions at one's own disposal. Those portions can then be shut down, or be used to attack yet other networks, especially within a system of systems construct.

One means of controlling, or at least affecting, foreign networks may have been accidentally initiated in 2010. From March 3 to 25, a root server based in China (one of the backbone servers supporting the Internet), conforming

to Chinese censorship rules, gave inaccurate addresses to queries for banned sites such as Facebook and Twitter. While this mostly affected Chinese Internet users, it eventually affected large numbers of South Korean, Australian, and Indonesian users.[38] Foreign users of Facebook and other such programs were effectively subjected to Chinese censorship in their own countries. While this incident is generally seen as an accident, it suggests one possible method of attack, should such redirection be deliberately implemented.

It is also possible to exploit network access to damage hardware components at various "points." The Stuxnet attack against Iranian nuclear reprocessing facilities, for example, involved the insertion of software into the supervisory control and data acquisition (SCADA) systems, which in turn caused the facilities centrifuges to malfunction.[39]

Such efforts can be facilitated by employing various types of computer malware. Since the advent of computer viruses in the 1980s, computer malware has become steadily more dangerous. One PLA assessment describes malware as "lethal weapons," capable of destroying or paralyzing single machines or entire networks. It categorized malware into four broad types:

- Worms, which can paralyze networks
- Trojan horses, which allow outsiders to penetrate networks
- Logic bombs, which can release viruses or generate other negative effects
- Interceptions, which can divert or copy and forward sensitive information including passwords and other data to an adversary[40]

Creating or exploiting entire networks of computers allows distributed denial-of-service (DDoS) attacks, long part of offensive network warfare. By instructing hundreds, thousands, or more computers to simultaneously message a target network, one can implement the computer equivalent of barrage jamming. The sheer volume of messages overwhelms the target network's ability to respond, preventing it from receiving legitimate queries and effectively blocking its interaction with the larger Internet or other networks.

One recent innovation by Chinese computer network experts uses a program dubbed by Western analysts as the "Great Cannon." This operates in conjunction with the Great Firewall of China (GFWC) to redirect legitimate queries against specific computers and targets. As discussed earlier, the GFWC is used to prohibit Chinese Internet users' access to parts of the Internet. The Great Cannon goes further, redirecting some of the traffic that typically goes to Baidu (a Chinese-run search engine that is one of the most visited sites in the Chinese portion of the Internet) against specific Internet addresses. (There is no evidence that Baidu was necessarily aware of the Great Cannon's redirection of queries to its website; Western analysts have indicated that the Great Cannon could have used any Chinese website for this redirection.)

CHINA'S GREAT CANNON[41]

GreatFire is an organization whose website, GreatFire.org, provides Chinese users access to censored information such as the *New York Times* Chinese language page. GreatFire set up a "mirror" site on GitHub.com, a repository for open source projects and one of the top 100 sites on the entire Internet, so that one could still obtain access, even if its site was busy or blocked. Because there are some 10–12 million GitHub users, including Chinese ones, entirely blocking access to it is beyond even the Chinese government's ability (due to negative Chinese as well as foreign reactions).

In 2015, however, the GreatFire.org site, and the specific mirror sites housed on GitHub, suffered a major distributed-denial-of-service (DDoS) attack. This attack was eventually attributed to a new Chinese entity that hijacks third-party computers and redirects them to attack the intended target. This entity was dubbed the "Great Cannon."

According to analyses by Swedish and Canadian cybersecurity firms Netresec and CitizenLab, the Great Cannon roughly follows this procedure.

- A web user, typically outside China, browses the Internet and visits a Chinese site.
- While browsing the Chinese site, the web user's computer accesses certain embedded Java scripts, such as Baidu Analytics' visitor tracking scripts. These scripts are a normal part of many websites (e.g., Google, Amazon), as they help set advertising rates (typically based on number of visitor hits).
- The user's request (which the user himself or herself typically is unaware of, as it is simply part of normal web browsing) for the Baidu Analytics script is detected by the Great Cannon as it transits the GFWC. While the trigger in this case was a Java script used by Baidu, in theory, any script from any site in China could have been exploited in this manner. (Some reports suggest that the initial attacks against GitHub and GreatFire shifted from Baidu scripts to Sina.com scripts.)
- Rather than allowing the request for the Baidu script to proceed, the Great Cannon inserts itself into the process (constituting a "man-in-the-middle" attack). The Great Cannon drops the request (so Baidu Analytics never receives it) and instead sends back a malicious response.
- This response from the Great Cannon redirects the web user's computer to constantly request pages from GreatFire.org or the specific GitHub.com mirror sites used by GreatFire.

Subsequent analyses concluded that the Great Cannon is hosted by China Unicom (one of the major Chinese telecommunications providers) and is "located" close to the GFWC.

According to these analyses, not every request for Baidu Analytics was hijacked. Instead, only some 1–2 percent of requests were apparently redirected. This was nonetheless sufficient to generate several million queries, constituting a highly effective DDoS attack. Theoretically, a higher proportion of queries could have been redirected, for an even more extensive attack. Similarly, while this attack was focused on a nongovernmental organization trying to bypass Chinese censorship, future attacks could target against any website or computer network.

According to Citizen Lab, a Canadian computer network research group, for two months in 2015, whenever a non-Chinese inquiry accessed certain scripts (e.g., those that log numbers of visits) used by the Chinese Baidu search engine, the Great Cannon would sometimes replace the legitimate script with a series of instructions for the non-Chinese inquirer's computer to repeatedly visit specific different sites.

Initially, they were redirected to GreatFire.org, a site helping Chinese netizens to circumvent the GFWC and access such sites as the Chinese language edition of the *New York Times*. Because GreatFire.org used the hosting service GitHub to house a mirror site for its instructions for bypassing the GFWC, the Great Cannon's managers subsequently shifted their attacks to GitHub. This led to what GitHub managers reported was the largest DDoS attack in the service's history.

At its height, GitHub servers reportedly logged some 2.6 billion requests per hour.[42] Because of how the Great Cannon was programmed, many of these requests were traced to non-Chinese computers. In effect, the Great Cannon converted a portion of the mass of Internet users that queried Chinese addresses into unwitting participants in DDoS attacks against targets of Beijing's choosing. As one computer security firm observed, the Great Cannon, in conjunction with the GFWC, "cannot be considered just a technology for inspecting and censoring the Internet traffic of Chinese citizens, but also a platform for conducting DDoS attacks against targets world-wide with help of innocent users visiting Chinese websites."[43]

Another Chinese innovation in offensive network operations has been using virtual private networks (VPNs) to mask penetration activities and mislead victims as to both line of attack and who might be responsible. The Chinese advanced persistent threat "Deep Panda," also known as the "Shell Crew," are believed to have created the Terracotta VPN, one of the first Chinese-based VPNs. They appear to have populated it not only with legitimate servers around the world but also hijacked servers from other companies and entities, including a major international hotel chain, foreign universities, and even foreign governmental computer networks.[44]

This effort not only helps Deep Panda save money but provides it with a concealed line of attack. By using hijacked servers, when penetration attempts by "Deep Panda" are discovered, they are traced to non-Chinese computers that are part of unsuspecting, legitimate networks. This will delay responses and divert resources away from actual vulnerabilities.

In short, Chinese network warriors have been converting what are typically considered *defensive* network technologies (firewalls to defend against intrusions, VPNs to allow secure communications) into *offensive* weapons. Both the Great Cannon and the Terracotta network demonstrate that

China can undertake offensive network warfare against a variety of targets while exploiting unsuspecting third parties. In event of conflict, such attacks could prove very disruptive, if only because the source would be difficult to pinpoint.

Offensive Psychological Operations

The human factor is a central element of informationized warfare, including information operations. Chinese information operations make great efforts to influence an adversary's outlook and framework of perceptions. Consequently, offensive psychological operations complement and enhance offensive electronic and network operations when conducted in tandem.

Chinese offensive psychological operations include appeals to mutual interest, ethnic bonds (e.g., among overseas Chinese), and friendship or kinship. Such efforts will emphasize the presumed lack of reasons for conflict. There will also typically be efforts at psychological coercion and deception, in order to intimidate adversaries.

Electronic warfare and network warfare operations reinforce offensive psychological operations. An adversary whose electronic systems are malfunctioning and is experiencing obvious penetrations of its various networks is vulnerable to psychological pressures. Degradation of radar networks and communications systems raise doubts about security and vulnerability. Electronic warfare may create a sense of being outmatched, especially if complemented by Chinese reporting on military activities or news coverage of Chinese mobilization efforts. Psychological operations can also include economic and diplomatic channels. Chinese analyses view American and Western economic sanctions against Iraq as key factors inducing a sense of isolation. Their impact is as great as the denial of Iraqi access. As the authors note in the 2013 edition of *The Science of Military Strategy*, the ability to secure an advantageous position in terms of network combat, and thereby secure the initiative, will generate enormous "psychological shock and awe" (*xinli zhenshe*; 心理震慑) in the enemy.[45]

Similarly, integration of firepower and information warfare includes a psychological warfare dimension. One example, according to Chinese analyses, was the announcement of impending targets for B-52 strikes during Operation Desert Storm. Iraqi troops were warned that they would be the next target, and encouraged to surrender.[46] Such "combined arms" attacks can erode the enemy's morale, making firepower attacks that much more powerful. Conversely, one might choose to attack certain targets physically in order to heighten the psychological impact.

Integrated Information–Firepower Warfare
(xinhuo yiti zhan; 信火一体战)

Chinese concepts of information attack emphasize the incorporation of conventional firepower, from cruise missiles to artillery barrages, to complement electronic and network attacks by destroying adversary information resources and assets. Chinese writings term this "integrated (or unified) information–firepower warfare" (*xinhuo yiti zhan*; 信火一体战). Like INEW, this is a form of unified joint operations.

Integrated information–firepower warfare (IIFW) is considered the epitome of informationized warfare, embodying the basic operational guiding concept of "integrated operations, use precision to constrain the enemy."[47] It is defined as the merging of firepower strike capability with information operations capabilities to undertake complementary hard-kill and soft-kill attacks. Supported by networked information systems and exploiting advances in weapons and sensors, highly precise firepower strikes and INEW operations together implement long-range, precise, real-time attacks against the adversary, especially its C2 and intelligence networks.

This coupling of hard-kill and soft-kill methods is hard to defend against. Confusion induced by INEW disrupts countermeasures to one's physical attacks, while using physical attacks degrades the effectiveness of various networked systems. Moreover, items that are physically destroyed or damaged cannot be easily repaired, whereas systems that are jammed or otherwise subjected to soft-kill measures may be able to overcome those soft-kill effects and be re-employed. In addition, physical attacks have an immediate and measurable effect, so their impact can be promptly assessed.

IIFW is not a new concept. In many ways, it updates traditional cover, concealment, and deception (CC&D) measures, adding microelectronics to that old form of information warfare. While CC&D is often considered defensive, it can also serve offensive ends. Allied leaders exploited CC&D to mislead the Germans, for example, about where D-Day would occur, promoting the idea that it would be at the Pas de Calais when it was at Normandy. During the 1990 Gulf War, American commanders conducted information operations to mislead Iraqi planners about a marine invasion of the Kuwaiti coast.[48]

At the same time, IIFW can also take new forms. For example, Chinese military cyberespionage forces have been accused of stealing information regarding Israel's "Iron Dome" missile defense system.[49] Such an act does not presage Sino-Israeli conflict. But obtaining specifications for a premier rocket and missile defense system allows China to circumvent any such defenses that might appear, such as in support of American expeditionary forces. As important, understanding how various defenses work could be incorporated into Chinese artillery rocket and missile designs. This would make them more

effective against various nations, including Taiwan, Japan, and even India, whether they fielded "Iron Dome" or not.

IIFW does not mean that information operations can be employed tactically the way more traditional forces are, however. While electronic warfare systems (jammers, dazzling weapons) can be promptly applied and redirected, computer network warfare, in particular, requires an enormous investment in time and effort for prior development and emplacement. They are not a "maneuver force" in the traditional sense—the ability to create (versus activate) a computer virus or backdoor "on the fly" is a fixture of Hollywood but is almost certainly not currently possible.

Instead, attacks against computers and computer networks require identification of vulnerabilities and writing of suitable code to exploit those vulnerabilities. This requires significant efforts long in advance of hostilities. Moreover, there is a likelihood that peacetime vulnerabilities will be eliminated in time of crisis or wartime. Once a weakness is exploited, its existence is also revealed; opportunities to employ it again will be limited.

Given sufficient time and effort, new offensive electronic and network measures could be created and even emplaced. These would produce new synergies between information operations and traditional military means. But the shorter the conflict, the less likely such new capabilities can be developed and deployed in time.

Defensive Information Operations

Defensive and offensive information operations are not mutually exclusive but complement each other. One Chinese guiding principle for information warfare is that offense and defense are both important. While offensive electronic and network warfare are essential, establishing and maintaining information dominance still requires substantial defense of one's own information assets and capabilities. This includes not only physical defense and technical measures but also proper training of defending forces, to rapidly respond to any damage of information systems. Countering, attacking, and destroying the enemy's offensive information capabilities meanwhile helps protect one's own information resources, enhancing efforts at avoiding and fending off the enemy's attacks. As one Chinese source observes, "offense and defense are linked, offense aids defense."[50]

For the Chinese security establishment, defensive information operations are not limited to countering cyberespionage. Defensive measures extend from limiting the public's general ability to access information (limiting adversaries' ability to influence them) to preventing attacks against specific information and associated infrastructure targets, both military and civilian. Thus, as noted in Chapter 2, the Chinese leadership views many of its efforts to manage and control the Internet as strategic forms of defensive information operations.

Similarly, maintaining network security is as much a peacetime activity as a wartime one. The Chinese fully expect efforts to penetrate computer networks, even in peacetime, and certainly in wartime. Because information security is inextricably tied to national security, peacetime assurance of information security and information system stability ranks alongside wartime assurance of network dominance and retaining the initiative in network conflict.[51]

Successful defensive information operations ensure that the overall system of systems can operate as close to normal as possible, even in the face of the enemy's efforts. In the Chinese view, proliferated information systems make absolute information dominance throughout the course of a campaign or conflict an impossibility. Attacks and degradations in one's information systems are therefore inevitable. However, successful defensive information operations, coupled with effective offensive information operations, allow one's information systems and networks to operate effectively as an overall whole, even if individual platforms and even systems are disrupted for periods of time.

To this end, defensive information operations must ensure the security of information and data, as well as networks. From the Chinese perspective, defensive information operations include a range of activities that create a layered set of defenses. These begin by preventing an adversary from discovering information and networks, through deception and concealment of one's capabilities, including not operating systems at full capacity or masking the existence of certain types of units. This is supported by protection of the data, networks, and operators and decision makers from enemy action. Defensive information operations also encompass physical protection measures for both facilities and systems.

Protecting Military Information Systems

Given the integrated nature of modern information networks, defensive information operations must extend to the broader civilian infrastructure. However, there are also essential military systems that require dedicated protective measures, to maintain the integrity of military operations and C2. In order for information warfare, including command-and-control warfare and intelligence warfare, to succeed, the various command posts, military communications nodes and network nodes, and key military information transmission and relay platforms must be protected.

One of the guiding principles for Chinese information operations is maintaining stealth and surprise. Frustrating the enemy's efforts to locate various facilities and centers, as well as the decision makers employed there, is essential.[52] By concealing one's electronic warfare forces, and engaging in

tactical and technical deception, one can mislead an adversary about one's deployments and therefore objectives. Similarly, by concealing one's full range of capabilities at both a tactical and technical level, one can catch an adversary off-guard by disclosing hitherto unexpected capabilities. Such surprises will be difficult to counter in the short run, creating a period of relative superiority.

Limiting the enemy's ability to conduct network surveillance is also vital, especially for command-and-control networks. Because of their role in coordinating forces, these networks field many emitters which often cannot be turned off. Moreover, command posts and communications nodes often have physical as well as electronic signatures that make them relatively easy to identify unless extra care is taken to disguise and conceal them.

The Chinese try to frustrate peacetime surveillance measures, as well as in event of crisis and wartime. A constant, ongoing program of countering reconnaissance will more successfully mislead adversaries than one only implemented on the eve of conflict. Moreover, because the possibility of conflict at a moment's notice is ever present, one cannot assume significant lead time for implementing countersurveillance operations. Chinese efforts to politically pressure the United States into halting both its air and naval reconnaissance activities off China's coast and dangerous Chinese behavior around those planes and ships are part of this countersurveillance effort.

Because of the proliferation of surveillance methods, Chinese analyses recognize that countersurveillance is more involved than simply keeping foreign ships and aircraft farther from China's shores. The adversary will field electro-optical and infrared sensors aboard airborne and space-based systems, as well as employ such diverse techniques as signals intelligence and electronic intelligence to map and track C2 capabilities. Therefore, countersurveillance efforts must counter the gamut of potential efforts, and be integrated into peacetime operating procedures, equipment prototype testing, field exercises and training, as well as undertaken in crisis and wartime.

PLA authors suggest that there are a range of "tactical defensive measures" (*zhanshu fanghu fa*; 占术防护法) and "technical defensive measures" (*jishu fanghu fa*; 技术防护法) that can limit adversary surveillance and reconnaissance efforts. Tactical defensive measures emphasize forestalling or misleading the enemy's discovery of one's assets and systems. One important method is rigorous emissions control (EMCON), eliminating, or at least reducing, electronic transmissions of all sorts.[53] This must limit emissions in all wavelengths and formats, including not only radios and radars, for example, but also congregations of vehicles, cell phone calls, and so on. E-mail traffic to and from certain addresses or locales must also be limited. PLA authors acknowledge that such efforts may interfere with training and other operational activities; therefore, there must be constant planning and coordination of emissions, to reconcile competing security and readiness requirements.

Another essential method is physically hiding systems, such as through camouflage, or deploying systems in tunnels and caves and other physical features. Coupled with disseminating false and inaccurate information, this can greatly complicate the adversary's intelligence-gathering efforts. The adversary may strike at the wrong targets, wasting time and matériel while improving one's own survivability. Chinese analysts note that the Iraqi military had some success in this regard, successfully misdirecting coalition attention and diverting some airstrikes away from actual Iraqi forces.[54]

Concealment can be complemented by fielding multiple platforms, including reserve and backup systems, as well as increasing mobility, so systems are harder to track and can displace rapidly.[55] Revealing certain systems at particular times while maintaining concealment on others, coupled with hidden reserves and regular redeployment, can further complicate an adversary's attempt to determine one's location and numbers.

Some Chinese writings also propose peacetime employment of systems at less than normal or optimal capacity. A particular subsystem may be substituted for another, so that adversaries cannot accurately judge the full capabilities of the entire system.[56] Coupled with decoys and multiple platforms, this can frustrate efforts to construct a complete and accurate picture of Chinese capabilities.

Concealment and deception can be important technical as well as tactical means of countering the enemy's reconnaissance methods. Chinese writings on technical defensive measures suggest advanced technical means can limit the adversary's ability to locate or monitor one's forces. Where possible, for example, directional antennae or fiber optic cables should be used for communications; transmissions should be managed to reduce chances of electromagnetic leakage or other forms of detection or eavesdropping.

In event of crisis or wartime, more direct measures can be employed. Chinese concepts of defensive information operations include attacking the enemy's intelligence and reconnaissance systems to prevent information collection. China's demonstrated antisatellite capability provides the option of destroying overhead reconnaissance systems. Similarly, one can actively jam or intercept air-breathing reconnaissance systems.

Interestingly, Chinese writings heavily emphasize preserving radar networks, as part of both technical and tactical defensive measures. Counter-countermeasures for radar systems are the first topic mentioned in one PLA analysis of the importance of preserving electronic system viability.[57] Other writings also emphasize the need to protect radar and air defense networks. This suggests that Chinese air defense is a priority concern.

Defensive Psychological Operations

Defensive psychological warfare is another essential part of defensive information operations. For Chinese decision makers, identifying and

countering underlying psychological vulnerabilities before the onset of hostilities is vital, as is sustaining that effort after conflict begins. An adversary will exploit such weaknesses in both peacetime and wartime to undermine Chinese will and morale.

Foremost among these is *weaknesses of political indoctrination*. The Chinese see warfare through a political lens; consequently, an essential part of psychological preparation for war is indoctrinating the political roots of conflict and instilling faith in political authorities (i.e., the CCP). Confusion about the reasons for fighting, doubts about one's own justness, and potential societal vulnerabilities and weaknesses are all susceptible to enemy exploitation.

Another potential psychological vulnerability is *defeatism among the troops*. Despite an extended modernization effort spanning the last two decades, the PLA still sees itself as largely a "half-mechanized, half-informationized" military. Compared with the U.S. military, the Chinese military sees itself as qualitatively lacking (although this varies by specific domain and to different degrees). American forces' greater combat experience, and displays of American and western combat power that have plied the airwaves and Internet for the past quarter century, exacerbate this. PLA analysts are concerned that, in event of conflict, some troops will doubt their ability to prevail against a more experienced opponent.

Yet another concern is *psychological passivity among the masses*. Even if the military is psychologically defended, conflict and resistance can only last so long without broad popular support. Any effort at defensive informational operations, whether psychological or otherwise, must include measures to protect and influence the larger population. This includes ensuring public concerns are not eclipsed by private interests (including profiteering), sustaining martial spirit (including hatred of the enemy), and limiting defeatism or fear of the enemy.

In order to counter such psychological vulnerabilities, PLA analysts emphasize the need to enhance intelligence work, in order to understand and counter the enemy's offensive psychological warfare methods. This is highly complex, since different opponents will pursue different approaches (and enjoy different advantages). The United States, Russia, and India are likely to have different psychological warfare methods. Therefore, there cannot be a one-size-fits-all approach to defensive psychological warfare. By understanding the enemy's offensive psychological warfare methods, Chinese officers and troops can be educated and trained to withstand them. The PLA will strengthen its political awareness, so soldiers and officers will greet the enemy's messages with skepticism and suspicion.

At the same time, as of 2016 the PLA recognizes that it is still likely to sustain heavier losses and fight at a technological disadvantage against many potential adversaries. Therefore, an essential part of defensive psychological

warfare is preserving confidence in the party's leadership, among both military and civilian leaders and the broader mass of troops and people. Integral to defensive psychological warfare is military and civilian indoctrination to have faith in their superiors, in the CCP system, and the justice of China's cause.[58]

Like other psychological warfare activities, defensive measures cannot wait until hostilities begin. Instead, defensive psychological warfare is comparable to inoculating troops against the pathogens of both foreign influence and internal doubt. Consequently, it must be integrated into their training routine, alongside weapons proficiency training or maintenance activities.

Defensive psychological warfare is a key task of the PLA's General Political Department. Political officers at all levels are responsible for conducting political education and political warfare, in peacetime as well as wartime. A foremost task is bolstering political confidence of the officers and troops. This helps inculcate martial spirit and forestalls psychological stresses induced by modern warfare.

These measures are not only matters of education and propagandizing but also controlling information and information flow. Chinese writings emphasize the need to ruthlessly suppress rumors and defeatist talk. News media, social media, and the Internet in general must be tightly controlled and closely monitored. This is simplified by both state ownership of the media (including Internet service providers as well as newspapers and broadcasters) and the GFWC and other barriers to easy information flow.

Information and Network Safeguarding

Even the best efforts at preventing or limiting adversary surveillance and reconnaissance measures will not always succeed. Chinese analyses recognize that safeguarding networks and the data they contain is another vital part of defensive information operations. Such measures must counter both attempts to reconnoiter networks and steal information and more destructive attacks against the data and networks.

A Wide Range of Threats . . .

Chinese information security specialists confront a wide variety of threats. The United States is regularly invoked as a major source of malware and other attacks against Chinese networks, but potential or actual threats from Taiwan, India, Russia, and Japan, among other nation-state level threats, must also be countered. Moreover, Beijing must also deal with domestic and nonstate threats, such as Uighur and Tibetan nationalists, Falun Gong religious activists, and possible terrorist organizations such as the Islamic State.

This array of threatening actors in turn can employ a variety of measures. Chinese information and network safeguarding resources must counter

electronic interference with networks themselves, more focused attacks against the data on the networks, computer malware, embedded vulnerabilities, and unintentional leakages of information stemming from all these sources.[59]

Electronic interference encompasses efforts that degrade the operation of various electronic systems. It includes jamming of radars and communications systems, laser dazzling of electro-optical sensors, and interference with the smooth flow of data streams. DDoS attacks are, in some ways, a form of INEW attack that exploits both electronic and network attack profiles.

The Chinese concept of "network intrusions" (*wangluo ruqin*; 网络入侵) embodies several different threats. Hackers may make unauthorized entries into networks to map them or extract information from them. There may be deliberate attempts to disrupt normal network operations (which could overlap with electronic interference, such as DDoS attacks).

Chinese concerns about malware mirror those of computer security professionals everywhere. Chinese writings cite fears of computer worms, malware concealed in e-mail attachments, computer viruses, and other such threats.[60] This is no different from Western professionals' comparable concerns about computer viruses (e.g., file infectors, boot-sector viruses, and multipartite viruses), as well as network worms, ransomware, and threats to mobile devices.[61]

Some Chinese sources consider embedded and inherent vulnerabilities within software and hardware a separate threat category. The growing complexity of electronic systems and programs creates inherent gaps and weaknesses. Chinese analyses note Microsoft Windows code has steadily grown, from 3 million lines of code in Windows 3.1 to 15 million in Windows 95, 35 million in Windows XP, and 50 million in Windows Vista.[62] Such masses of code contain potential vulnerabilities simply due to their complexity and potentially sloppy coding. Hackers often exploit these undetected inherent security gaps (termed "zero-day exploits").

Similarly, electronic hardware may emit signals on various frequencies that can be eavesdropped upon. Wireless router signals can be intercepted and exploited, especially if they are not encrypted. Some types of displays similarly emit exploitable signals, which can be accessed from some distance.[63]

The challenge of embedded equipment and software flaws is exacerbated by possible deliberate incorporation of vulnerabilities within the mass of code, which would be even harder to detect. This includes backdoors, Trojan horses, and "logic bombs." Chinese sources specifically note the vulnerability posed by Microsoft Windows, with its dominant position in global computing. While some Windows security problems are due to technical shortcomings, Chinese analysts conclude "some are deliberate."[64] China has accused other major American technology firms such as Google, Apple, and Cisco of posing cybersecurity threats to Chinese users.[65] The revelations by Edward Snowden about U.S. National Security Agency (NSA) activities only further confirm these worries.

Similarly, physical hardware such as microprocessors and microchips may contain embedded instructions that allow external manipulation, access, or running of certain concealed programs. Chinese writings reflect concern about vulnerabilities stemming from both hardware and software supply chains. They note that imported weapons, for example, may contain concealed programs in the hardware that could cause associated information networks to cease functioning.[66]

These vulnerabilities are not mutually exclusive; indeed, they can be mutually reinforcing. Hackers can insert malware or exploit backdoors to create robot networks (botnets) which in turn can be used to undertake DDoS attacks and interfere with the operations of various networks. Attacks against satellite tracking and telemetry systems might prevent satellites from undertaking self-protection maneuvers, which in turn would enhance the effectiveness of laser dazzling attacks against their sensors.

. . . Requiring a Wide Range of Responses

Ensuring the smooth operation of various networks, as well as providing the necessary information to military and civilian leaders for accurate decision making, requires limiting adversary access to one's networks and data. This is a central task of defensive information operations. From the PLA's perspective, information is a strategic resource.[67] Therefore, safeguarding its smooth flow is no different than ensuring unimpeded movement of any vital resource, such as fuel or ammunition.

Network safeguarding measures ensure the integrity and security of the various networks, as well as sustaining the smooth flow of information across them. Chinese discussions of such measures often mirror Western concepts. Both include firewalls, intrusion detection systems, intrusion prevention systems, and honeypots.[68]

Firewalls control efforts to access and query networks and are among the most common techniques for safeguarding them. Firewalls segregate different portions of networks from each other and also separate the internal workings of a network from the broader Internet, thereby limiting access to certain types of information. They also often record all transits across them, which facilitates tracking of violation attempts and identification of those who might have accessed information within the network.

A firewall can incorporate the network equivalent of a "demilitarized zone," or "perimeter network," between internal and external firewalls. These are stand-alone subnetworks that link with untrusted systems that provide public services but that are isolated from one's main network. Like the broader concept of firewalls, network "demilitarized zones" decrease the likelihood of outsiders penetrating the heart of one's networks. Interestingly, the Chinese "Great Cannon" appears to reside within the equivalent of a

"demilitarized zone," between the broader, global Internet and the Chinese portion of the Internet.

Chinese writings recognize that firewalls are not foolproof; in particular, they are of limited utility against insider threats. One Chinese assessment concludes that 70 percent of attacks are from internal sources.[69] Therefore, networks must also incorporate intrusion detection systems and intrusion prevention systems, to limit damage by those who circumvent the firewalls or otherwise gain access to the network.

"Intrusion detection systems" (*wangluo ruqin jiance xitong*; 网络入侵检测系统) are the combination of hardware and software that identifies authorized and unauthorized users of network or computer assets. They provide immediate notification of external attacks or unauthorized entries, providing systems administrators with warning of an attempted entry. "Intrusion prevention systems" (*wangluo ruqin fangyu xitong*; 网络入侵防御系统) build upon intrusion detection systems, incorporating automated responses to redirect or otherwise neutralize attacks.

Such efforts incur a performance cost. A distinguishing characteristic of China's approach to network security is the willingness to accept performance degradations in favor of greater security. The overall speed of the Chinese portion of the Internet is believed to be slower, especially where it interacts with the rest of the global Internet, because of the intervening GFWC.

Chinese analyses also include deception efforts as part of network defenses. Misleading an adversary about a given network's role and importance is an additional layer of protection. A dedicated network for high priority users may have a constant stream of low-level information or even nonsensical messages moving across it in peacetime, to disguise its function and purpose. Honeypots are another type of deception, whereby attackers are lured away from the main target into a network dead end. Designed to exploit known vulnerabilities, they lure attackers into a "trap," where not only is there no useful data, but the attacker is likely to wind up wasting time. This diversion of enemy resources is considered an additional benefit to defenders.

Given the Chinese focus on INEW, network safeguarding also includes a range of electronic counter-countermeasures (ECCM). For example, radars and other transmitters can be produced with higher power settings that would help them burn through jamming and other interference. Frequency hopping in radios, or multiple radar frequencies in air defense networks, further complicate attempts to neutralize them. In addition, some electronic systems may incorporate software that can filter out jamming. There are also more advanced technical alternatives. For example, laser communications are both hard to detect and difficult to jam.[70]

Network safeguarding measures are complemented by information safeguarding measures, such as encryption and data integrity assurance. One

Chinese analysis describes data encryption as a core "weapon" for safeguarding information and communications security.[71] Such efforts frustrate an adversary's information reconnaissance efforts by making it harder to determine what is useful and what may be background noise or less important information.

Chinese discussions of information safeguarding techniques include analysis of traditional encryption methods, such as symmetric and asymmetric encryption (where the encoder and decoder have either the same or different encryption keys). They also include more advanced methods, such as steganography, whereby important information may be buried in a mass of low-value information or within "noise," in order to conceal its value.[72]

While not formally a type of encryption, Beijing has sought to further enhance data security by substituting domestic software products for foreign ones. From the Chinese perspective, relying on foreign software constitutes an important vulnerability, as it potentially allows easy access to computers and networks. As of 2014, some 70 percent of Chinese computers were reportedly running Microsoft XP, although the company was no longer supporting it with security updates.[73] Even without concerns about foreign espionage, such widespread reliance on an operating system (OS) that is no longer supported is an invitation to trouble.

Developing an alternative Chinese OS has reportedly been a high priority. In 2001, the Chinese military's National University of Defense Technology (NUDT) tried to produce a domestic OS. At the same time, the state-sponsored company Red Flag Computing produced a variation of the open source Linux software, known as Red Flag Linux. While Red Flag Computing apparently went out of business, its efforts were used by NUDT to create the Kylin program. NUDT then worked with China Standard Computing, a subsidiary of another state-owned enterprise, to improve Kylin, which led to NeoKylin.[74]

Apparently still based on Linux variants, including Ubuntu, the NeoKylin OS appears to emulate various aspects of Windows XP (which would ease any transition from the Microsoft product).[75] Greater use of NeoKylin, at least on government computer networks, would reduce the likelihood that backdoors or Trojan horses could be easily exploited on those systems. Reports indicate the OS was installed throughout the city of Siping in 2014 to test its viability, and was apparently considered a success.[76] Meanwhile, some 40 percent of Dell computers sold in China come preloaded with NeoKylin.

Another element of network and information safeguarding is physical security. This includes providing locks and security guards but also countering unintentional physical leakage of information. One element is limiting the ability of adversaries to eavesdrop on information leaked electromagnetically from computer displays and the like. One Chinese analysis notes that signal leakage from 20 sources could be monitored up to one kilometer away.[77] When

designing work-spaces, it is necessary to emplace additional physical layers and barriers between computer displays and potential eavesdroppers.

To maintain information security, the Chinese emphasize regularly reviewing and inspecting security plans and procedures. This includes periodic updates to information security software and other products, as well as reviews of physical security procedures for both information facilities and other physical components of networks. Different systems' access to certain types of information and to other networks should be strictly controlled. Such efforts must be undertaken in peacetime, and redoubled in event of crisis or wartime.[78]

The human component of information infrastructure must also be safeguarded. This includes "administrative defensive measures" (*xingzheng fanghu fa*; 行政防护法) to limit information access. In order to counter potential hacker attacks, for example, human signatures, identity verification, and passwords and other data entry means should be employed to allow only authorized personnel access.[79]

The networks and data must be protected not only from electronic and cyberattacks but also from integrated information–firepower warfare. As PLA writings emphasize, offensive information operations include using firepower to kill key personnel and disrupt C2 nodes and networks. Defensive information operations therefore incorporate physical protection measures against stand-off precision munitions, special operations forces, as well as general air, naval, and artillery strikes. For space-based systems, Chinese writings discuss the need for protective measures against directed energy weapons, whether aimed at sensors or solar panel arrays. Ground facilities must also be protected, to ensure smooth operations of various constellations. Physical protection also includes measures to sustain operations in the event of natural catastrophes (e.g., earthquakes, solar flares).

A central part of physical protection is undertaking "defensive engineering measures" (*gongcheng fanghu fa*; 工程防护法). Examples include incorporating deceptive and concealment measures into new construction, and hardening of facilities. There is a general Chinese interest in making facilities harder to destroy, a lesson derived from the various Middle East wars dating back to the 1967 Six-Day War and 1973 Yom Kippur War. In the 1960s, China reportedly constructed thousands of miles of tunnels; Chinese television has recently provided footage of some more recent tunnels.[80] Because the more recent tunnels are associated with the PLA Rocket Force (formerly the Second Artillery), they are assumed to have primarily nuclear-related missions.[81] However, these facilities may have broader C2 and other support roles.

A broader effort to integrate hardening and concealment into the design of new construction projects is incorporated in Chinese civil defense and mobilization measures. For example, under the Chinese Civil Air Defense Law,

there is a mandate to incorporate air defense shelters into all major construction projects. Buildings with extensive foundations are expected to set aside portions of underground garages and basements to serve as bomb shelters. Additionally, the law requires that specific facilities be set aside for C2 and medical support uses.[82]

Physical hardening is complemented by physical defense. Key command posts, telecommunications nodes, data networks, and other such facilities include physical protection measures ranging from sensors and quick reaction security forces to air and naval defenses. PLA writings suggest that air attack and assault by the enemy's special operations forces are of particular concern.

Defensive information operations include preparing to operate under adverse natural conditions, as well as enemy threat. Thus, physical security measures are implemented when natural disasters occur. In the event of earthquakes, storms, floods, or other natural disruptions, networks and command posts must be able to resume operations promptly. This is especially the case as many physical components of networks require operating environments that are kept within certain temperature ranges, levels of cleanliness, and so on.

INFORMATION DETERRENCE

An essential mission of information operations is information deterrence. The PLA defines "information deterrence" (*xinxi weishe*; 信息威慑) as a type of "information operation activity" (*xinxi zuozhan xingdong*; 信息作战行动) that can either display one's information advantage or announce deterring information to compel an adversary to abandon its willingness to resist or to reduce the strength of its resistance.[83] It involves, at some level, threats against the enemy's information systems, such as to paralyze or disrupt them, to constrain enemy actions and thereby help achieve one's political goals.

Chinese writings on both information deterrence and deterrence writ large do not emphasize deterring activities *in* information space; that is, the Chinese are not focused on deterring activities against their information systems. Rather, Chinese writings on information deterrence discuss the use of information operations to *effect* deterrence. Information deterrence is about achieving deterrent goals *through* information operations.

The broad Chinese conception of deterrence, and the specific concept of information deterrence, incorporates both dissuasion and coercion. Chinese information deterrent actions are aimed at undermining the adversary's will by influencing their cost–benefit calculations, making it question whether its preferred course of action is worth likely damage incurred from attacks on its information networks and systems. Ideally, Chinese deterrent actions would persuade the target that the cost of noncompliance is too high, and it would be easier to accede to China's preferred course of action. Essentially, the Chinese

concept of information deterrence is the use of informational means, whether attacks on information systems and networks or certain types of information itself, to erode the adversary's willingness to resist.[84]

From the Chinese perspective, information's growing role in warfare means that threatening access to information can deter and coerce an informationally comparable adversary. The degree of Internet penetration in military, political, and economic affairs allows unprecedented access to foreign infrastructure. The potential ability to massively disrupt an adversary's entire society creates deterrence opportunities. Indeed, on a day-to-day basis, states

WEISHE: CHINESE CONCEPTS OF DETERRENCE

For most Western analysts, deterrence is dissuading an opponent from acting in a particular way or following a particular course of action. Thomas Schelling, in *Arms and Influence*, defines "deterrence" as "the threat intended to keep an adversary from doing something."[85] Schelling specifically differentiates deterrence from "compellence," defined as "the threat intended to make an adversary do something."[86] Glenn Snyder makes the same point by noting that deterrence "is the power to dissuade *as opposed to the power to coerce or compel*."[87]

This is in sharp contrast with the Chinese term *weishe* (威慑), which embodies *both* deterrence *and* compellence. The PLA volume on terminology, for example, defines a "strategy of deterrence" (*weishe zhanlue;* 威慑战略), as "the display of military power, or the threat of use of military power, in order to compel an opponent to submit."[88] Generals Peng Guangqian and Yao Youzhi, in the 2005 edition of the PLA textbook *The Science of Military Strategy*, note that

> deterrence [*weishe*] plays two basic roles: one is to dissuade the opponent from doing something through deterrence, the other is to persuade the opponent what ought to be done through deterrence, and *both* demand the opponent *to submit to the deterrer's volition*.[89]

Thus Peng and Yao combine Schelling's definitions of deterrence and compellence within the Chinese term *weishe*.

A different Chinese volume attests that either the purpose of deterrence is to prevent the other side from starting a conflict, or "it is to shake the other side's will to resist (*dikang yizhi*; 抵抗意志), and thus seize those interests or benefits that originally would have required conflict in order to obtain them."[90] Another Chinese analysis notes that strategic deterrence psychologically constrains an opponent's actions or causes it to submit.[91] This same volume goes on to state specifically that not only can a defending side utilize deterrence to compel an aggressor to abandon offensive intentions, but an offensive side can also implement strategic deterrence, causing a defender to conclude that the cost of resistance is too high.[92]

It is important to note that the Chinese concept of deterrence does not obviate the possibility of the *deterred* party nonetheless achieving some of their goals. It is simply that any such achievement will not be at the expense of the deterring party's goals.[93]

already engage in information deterrence, precisely because the scale of disruption that would otherwise erupt would be enormous. Few states are confident that their defenses could prevent such disruptions.[94]

However, where there is a distinct imbalance in information capabilities, it is harder for the weaker side to effect information deterrence. Conversely, the side with less conventional military power but significant network warfare capabilities can nonetheless paralyze and disrupt the more conventionally capable side. The weaker side can inflict high costs, and may even defeat the conventionally stronger one.[95]

In the Chinese view, conducting offensive information operations is key to implementing information deterrence. A demonstrated capability of exploiting information, especially waging computer network attacks, even if not employed in a given crisis, will nonetheless make the adversary wary.

Network offensive operations are the foundation of information deterrence.[96] They can be used to attack a variety of targets, threatening much of an adversary's society, economy, and military. They are hard to defend against, in some ways harder than conventional, nuclear, or space attacks. In the event of a crisis, threats of information attacks (e.g., computer viruses) will affect an adversary's will and may persuade it to cease resistance.

The lack of experience with large-scale network offensive operations also enhances deterrence. In the Chinese view, the uncertainty about the ultimate effects of network attacks is a factor forestalling large-scale network conflict.[97]

On the other hand, Chinese analysts believe the defense and safeguarding of one's information resources and systems can deter an adversary, by limiting its ability to establish information dominance. Without information dominance, the enemy cannot easily establish dominance over other domains (e.g., air, space, maritime), raising the costs to achieve their broader strategic objectives. They are therefore likely to be deterred from initiating aggression, or may be coerced into submitting.

A Possible Information Deterrence Ladder

Chinese writings about deterrence activities in the space and nuclear domains, suggest a possible analogous "deterrence ladder" for information operations. If this exists, it may comprise the following "rungs":

- *Demonstrated capability in a peacetime context.* Chinese conduct of peacetime information operations would seek to remind potential adversaries of Chinese capabilities. These might include penetrations of potential adversaries' networks, electronic interference (including jamming or dazzling of various sensors), and efforts to psychologically intimidate or influence public figures. These measures may not be destructive or overt but would demonstrate that the PRC possesses

significant capabilities which could be employed in event of conflict. This would begin to influence all potential adversaries' calculations and decision-making frameworks.

- *Wargames and exercises*. Periodically, the PLA and other Chinese information operations forces would engage in wargames and exercises, demonstrating not only technical capabilities for offensive information operations but a doctrine governing its employment. Such events would also allow the PLA to demonstrate that it has integrated information operations into larger military activities, such as amphibious assaults and unified joint operations. It would also provide PLA forces training opportunities.
- *Heightened operations*. In both space and nuclear contexts, Chinese writings suggest an increase in operational tempo in time of crisis to coerce or dissuade the adversary. A higher level of activity allows Chinese leaders to signal their concerns, while also shifting the balance of forces in China's favor (e.g., by increasing deployed forces or altering their locations). In the context of information deterrence, this might entail a range of increased information activities. Some may be more defensively oriented. For example, traffic across the GFWC may become highly restricted, to demonstrate that China's population is not vulnerable to enemy influence. Alternatively, it might entail increased information reconnaissance, both to obtain the most current information possible and to signal one's penetration of adversary networks.
- *Limited actual offensive information operations*. In both the space and nuclear contexts, the highest rung of the deterrence ladder involves *use* of weapons, as the ultimate demonstration of resolve. The same may be true in the information context, through execution of offensive information operations. The initial goal, however, would not be to disarm or devastate the adversary but to coerce or dissuade it into acceding to Chinese demands. Possible activities at this level, for example, might involve expanded DDOS attacks through redirection of Internet traffic, perhaps via the Great Cannon; redirection of Internet traffic (as part of a de facto "information blockade"); or interference with the adversary's space information systems, whether against satellites, space situational awareness systems, or mission control facilities. These activities would also serve to improve the balance of forces, should the adversary fail to be deterred.

It is important to keep in mind that such information deterrent activities would not occur in isolation but would be coordinated with a host of comparable activities in other domains. These would include not only military forces (e.g., naval exercises, space exercises) but also diplomatic and political

pronouncements, economic measures, and legal warfare measures. This is especially likely at higher rungs on the ladder.

For Chinese decision makers, this situation is further complicated, because the PRC confronts a number of potential adversaries. Therefore, they must constantly engage in multilateral deterrence. China cannot only focus on deterrent activities against, the United States or Japan, even in the midst of a crisis involving those states. It must factor in how Russia, India, and other states may react, both immediately and in the longer term. Heightened operations or limited offensive information operations, in the deterrent context, may be undertaken against third parties (e.g., the Philippines), perhaps to demonstrate capability against them, to signal resolve against the main target (e.g., the United States), or to signal still other parties (e.g., Russia, India) that China has sufficient capability to degrade them as well.

6 Chapter

Space and Information Warfare: A Key Battleground for Information Dominance

Throughout the 1990s, as the PLA views on information and future warfare were evolving, so were its assessments of space warfare. Analyzing other people's wars, the Chinese concluded that space warfare would be an integral part of future wartime operations. The information support necessary for the successful conduct of future local wars, whether under modern, high-technology conditions or informationized conditions, would have to include sources based in space.

Indeed, PLA assessments of American and Russian military operations concluded that space-based information played an outsize role in the conflicts of the 1990s. Therefore, the PLA must, at a minimum, deny an adversary the ability to use space freely. Space warfare and information warfare have long been intimately linked in the Chinese mind.

EVOLUTION OF CHINESE THINKING ABOUT MILITARY SPACE

While China's space program dates from the 1956 founding of the Fifth Academy of the Ministry of Defense, its ability to exploit space for military purposes is much more recent. China launched its first satellite only in 1970 and for two more decades orbited only a handful of communications and reconnaissance satellites. Space activities were more political gestures than a vital part of the economic or military arena and therefore were downgraded by Deng Xiaoping. After he succeeded Mao in 1978, Deng made it clear that the Chinese space program should focus less on gaining prestige and headlines and instead "concentrate on urgently needed and practical applied satellites."[1]

Support for China's overall space program did not improve until 1986, when Deng authorized Plan 863, formally termed the "National

High-Technology Research and Development Plan" (*guojia gao jishu yanjiu fazhan jihua;* 国家高技术研究发展计划).[2] Plan 863, which is still ongoing, supported scientific and technological research on topics essential for a modernizing economy. Aerospace, along with information technology, and later telecommunications were seen as key areas of high technology that would sustain economic growth, justifying substantial, sustained resource investment.

Space and Local Wars under Modern, High-Technology Conditions

For the PLA, the coalition performance against Iraq in 1990–1991 during Operation Desert Shield/Desert Storm served as a wake-up call about space. The war highlighted the importance of space as a key military technology that would influence future wars.

PLA analyses concluded that future joint operations would involve multiple services operating together across significant distances. The Gulf War, for example, involved forces ranging from armored units to aircraft carriers and long-range bombers, sprawled across 140 million square kilometers.[3] Coordinating such diverse forces operating in a variety of domains would therefore require not only extensive communications but also precise navigation and positioning information, for both units and the growing array of precision munitions. Joint operations would require command and control of operations across not only the traditional domains of land, sea, and air but increasingly outer space.

Waging "local war under modern, high-tech conditions" would therefore necessitate space capabilities. According to PLA estimates, the 70 satellites that were ultimately brought to bear against Iraq provided the United States with 90 percent of its strategic intelligence and carried 70 percent of all transmitted data for coalition forces.[4] These assets were the first to be employed, since they were essential for the success of all subsequent campaign activities. As one Chinese analysis observed, "Before the troops and horses move, the satellites are already moving."[5]

Nonetheless, there were still some doubts about the importance of space. In the 1997 *PLA Military Encyclopedia,* the discussion for "space warfare" (*tianzhan*; 天战) explicitly states that space is *not* a decisive battlefield—the key to wartime victory would remain in the traditional land, sea, and air realms. "It is impossible for it [space warfare] to be of decisive effect. The key determinant of victory and defeat in war remains the nature of the conflict and the human factor."[6] Space played a supporting, not leading, role.

In the 2002 supplement to the *PLA Encyclopedia,* a very different assessment is made of the importance of space. In a discussion of the "space battlefield" (*taikong zhanchang*; 太空战场), the entry concludes that its impact on land, sea, and air battlefields will become ever greater and the space battlefield

"will be a major component of future conflict."[7] Clearly, in the intervening five years the perception of space had changed and was now seen as a substantially more important arena for military operations.

This progression may have been due to the intervening NATO conflict in the Balkans. Belgrade's defeat through airpower, seemingly on its own, clearly caught Beijing's attention. Chinese analyses accorded great prominence to the role of space power. NATO forces are assessed to have employed some 86 satellites.[8] Another Chinese analysis concluded that NATO space systems provided 70 percent of battlefield communications, 80 percent of battlefield surveillance and reconnaissance, and 100 percent of meteorological data and did so through all weather conditions, 24 hours a day.[9] These space systems provided a dense, continuous flow of real-time data. NATO could strike Serbian forces because space provided precise locations for sustained, coordinated strikes, with 98 percent of the precision-guided munitions employing space-based information.[10] Airpower could achieve its goals only because substantial space power supported it.

Victory in future "local wars under modern, high-technology conditions" would therefore require not only unfettered access to space for one's own forces but also the denial of the same ability to the adversary. By preventing enemies from obtaining the amount of information they required, it would be far more difficult for them to coordinate their forces and operations. As important, by preventing them from operating in the manner to which they were accustomed (and had trained), they would be far less efficient and flexible and therefore more vulnerable to Chinese actions. In effect, by degrading the adversary's space capabilities, the enemy's OODA (observe–orient–decide–act) loop would be retarded. Offensive space operations were increasingly seen as complementing space information support activities.

Space and Local Wars under Informationized Conditions

This shift also reflected the ongoing development of Chinese concepts of future warfare. As part of the PLA's "new historic missions," Hu Jintao in 2004 made clear that the PLA must secure China's interests in outer space, as well as the electromagnetic spectrum.[11] The specific incorporation of the space domain into PLA responsibilities reflected the growing emphasis on space dominance, linked to securing information dominance.

Indeed, as the PLA shifted from preparing for "local wars under modern, high-technology conditions" to "local wars under informationized conditions," space was increasingly considered part of those "informationized conditions." As PLA writings noted, "informationized conditions" did not simply refer to computers and cyberwarfare. It involves the acquisition, transmission, and exploitation of all forms of information. Space plays a central role in all these

tasks. In the 2006 edition of *The Science of Campaigns,* it is specifically stated that "the space domain daily is becoming a vital battle-space. . . . Space has already become the new strategic high ground."[12]

This is exemplified in that volume's revised version of "campaign basic guiding concept." The new concept of "integrated operations, precision strikes to control the enemy" (*zhengti zuozhan, jingda zhidi*; 整体作战, 精打制敌) requires even more information support from space-based assets than the previous version of "integrated operations, key point strikes." One example is using precision munitions to attack vital targets. The goal is not only destroying key targets but also precisely controlling a conflict's course and intensity.[13] It also entails disrupting the normal function of enemy systems (and systems of systems). The focus is on disruption leading to paralysis, not just destruction of the adversary's weapons or forces.[14] Information from space systems facilitates such precision operations. "Establishing space dominance, establishing information dominance, and establishing air dominance in a conflict will have influential effects."[15]

Similarly, in the 2013 edition of *The Science of Military Strategy,* space is deemed the "high ground in wars under informationized conditions," tied to the struggles in networks space and the electromagnetic spectrum as key future battlegrounds.[16] In the Chinese conception, space is important for the advantage it confers with regard to the ability to collect, transmit, and exploit information, rather than for its own sake. As other Chinese analysts conclude, "space operations will be a core means of establishing information advantage."[17]

CHINESE SPACE CAPABILITIES: A BRIEF REVIEW

China's overall space capabilities have expanded significantly during the past two decades. In the wake of Plan 863, senior Chinese leaders renewed their support for space activities, in both political and resource terms. Under Jiang Zemin (1992–2002), China deployed both low-earth orbit and geosynchronous weather satellites (the *Fengyun* series), improved geosynchronous communications satellites (the *Dongfanghong*-3 series), as well as recoverable satellites with varying payloads (the *Fanhui Shi Weixing* series).

Chinese earth observation capabilities also improved during this period. In cooperation with Brazil, China in 1999 deployed the China Brazil Earth Resources Satellite (CBERS), its first electro-optical imaging satellite capable of beaming pictures directly to the earth. China subsequently launched several similar satellites with no Brazilian involvement; these are known as the *Ziyuan* series, to distinguish them from the CBERS satellites.

In 2000, China became only the third country to deploy a navigational satellite system, launching two *Beidou* regional navigation satellites into

geosynchronous orbit. This system also has a communications function, which was employed during the 2008 Sichuan earthquake.[18]

Jiang Zemin's successor, Hu Jintao, maintained support for China's space program. During his leadership term (2002–2012), China deployed a variety of new satellite systems, including remote sensing satellites (the *Yaogan* series), microsatellites such as the *Shijian* series, as well as improved versions of *Fengyun* and *Ziyuan* satellites. Under Hu, China also orbited several manned spacecraft (the *Shenzhou* program) and initiated a lunar exploration program, launching the *Chang'e*-1 and *Chang'e*-2 lunar probes.

Since Xi Jinping took power in 2012, he has not reduced high-level political support for China's space program. China inaugurated its *Gaofen* series of high-resolution earth observation satellites in 2013. The second Chinese space lab, *Tiangong*-2, is expected to be launched in 2016 and will be part of the next phase of Chinese manned space missions. China's robotic lunar rover, *Yutu* (Jade Rabbit), marked the first lunar landing since Apollo 17. China also announced the first landing on the far side of the Moon would be in 2018. Some of the current Chinese satellite constellations are listed in Table 6.1.

Table 6.1 Chinese Satellite Constellations

Constellation Name	Chinese Characters	Function
Beidou (Big Dipper)	北斗	Position, navigation, timing, communications
Fenghuo (Signal Fire)	烽火	Military communications
Fengyun (Wind and Clouds)	风云	Meteorology
Gaofen (High Resolution)	高分	High-resolution earth observation
Haiyang (Ocean)	海洋	Ocean monitoring and reconnaissance
Huanjing (Environment)	环境	Environmental monitoring
Shentong (Permeating)	神通	Military communications
Shijian (Practice, or Implementation)	实践	Technology testing, possible military applications
Shiyan (Experiment)	试验	Technology testing, possible military applications
Tianlian (Sky Link)	天链	Data relay
Yaogan (Remote Sensing)	遥感	Remote sensing
Ziyuan (Resource)	资源	Earth observation

In keeping with Deng Xiaoping's admonition that China's space program must serve broader national economic development goals, many Chinese satellites have dual purpose, supporting urban planners and agricultural programs as well as the military. For many of China's satellite programs, including earth observation, position and navigation, and weather satellites, the focus has been more on supporting Chinese economic development objectives than producing cutting-edge capability.

This has also been a two-way street. The Chinese space industrial complex has benefited from steady investment of resources. Much of China's space technology has been indigenously developed; Chinese satellites, launch vehicles, and ground support equipment are domestically produced. Two major aerospace conglomerates, the China Aerospace Science and Technology Corporation (CASC) and the China Aerospace Science and Industry Corporation (CASIC), manufacture the full range of space systems, including launch vehicles, satellites, and ground equipment, and associated subsystems and support items.

Similarly, a strong national space infrastructure is seen as benefiting the military as well. Military space systems, by their exquisite nature and extreme capabilities, are expensive and therefore limited in number. Civilian space assets are likely to be more numerous and often developed faster than their military counterparts. Consequently, Chinese analysts conclude that a comprehensive set of civilian space systems can usefully augment military space forces, at least for information support and space monitoring.[19]

CHINESE CONCEPTS OF MILITARY SPACE OPERATIONS

China's space program is not solely devoted to civilian use, however. It also provides the PLA with key pieces of information, deemed essential for both "local wars under high-tech conditions" and "local wars under informationized conditions." Moreover, the military plays an outsize role in Chinese space activities, as the PLA runs China's space facilities.[20]

Under Hu Jintao, the PLA began to publicly demonstrate space combat capabilities. The PLA tested its direct ascent, kinetic kill antisatellite (ASAT) system in January 2007. Launched from Xichang Satellite Launch Center, the Chinese ASAT destroyed a defunct *Fengyun*-1C weather satellite in low orbit. In the process, China also generated a massive amount of space debris.[21] Almost precisely three years later, in January 2010, China staged what was termed an antimissile test, involving "two geographically separated missile launch events with an exo-atmospheric collision also being observed by space-based sensors," according to the U.S. Department of Defense.[22] This test also helped Chinese scientists improve their ASAT systems. In August 2010, two Chinese

microsatellites were deliberately maneuvered into close proximity and apparently "bumped" each other.[23]

This antisatellite development effort has been sustained under Xi Jinping. In May 2013, the Chinese conducted another antisatellite test. This weapon, however, is assessed as threatening targets as far as the geosynchronous belt, over 26,000 miles away.[24] This is the first time that any nation has tested a weapon explicitly intended to hold satellites in that orbit at risk. Described by one senior U.S. military officer as the "most valuable orbit," the geosynchronous region is populated by not only large numbers of communications satellites but also strategic early warning satellites and weather satellites.[25] Destroying such systems would be a major step toward establishing information dominance.

As with other Chinese military activities, the PLA's approach to space operates within the context of "guiding thoughts"; those governing space is described as "active defense, all-aspects unified, key point is dominating space (*jiji fangyu, quanwei yiti, zhongdian zhitian*; 积极防御, 全维一体, 重点制天)."[26] Each phrase embodies a number of essential concepts.

The "Active Defense" concept is integral to all Chinese military strategy and, as noted earlier, is not limited to space-related operations. While assuming the strategic defensive, the PLA concept of "Active Defense" emphasizes seizing the initiative at the tactical and operational level. In the context of space operations, active defense again assumes a more strategically defensive stance, even while deterring aggression and maintaining national security and interests. Chinese military writings assume that in space, as terrestrially, the Chinese would not precipitate a war. At the same time, however, the concept of "Active Defense" expects the PLA to prepare for space combat, including seizing the initiative in space-related operations. In particular, it presumes "offensive actions at the campaign and tactical level to secure strategically defensive goals."[27]

The concept of "all-aspects unified" refers to unifying thinking about different aspects of space operations. In the first place, it entails viewing space as a holistic environment, encompassing not just satellites that are in orbit but also terrestrial mission control; launch; and tracking, telemetry, and control (TT&C) facilities that allow those satellites to operate and the data links binding the entire structure together. In striving for space dominance, the Chinese envision attacking and defending all three components. Destruction of mission control facilities, jamming of TT&C links, or entry of instructions that turn off satellites at key moments is as effective as launching an ASAT against a given satellite.

The concept of "all aspects unified" also requires viewing the various domains of military activity, including not only outer space but land, sea, air, and the electromagnetic spectrum (e.g., cyber and electronic warfare operations),

in a joint fashion, with operations in each domain contributing to, and receiving support from, the other domains. Since space operations are an integral part of joint operations, and especially information operations, adopting a joint perspective is essential. It is necessary to forge an organic, integrated whole, where each component supplements the others.[28] Space operations support terrestrial operations, while land, sea, air, and computer network operations can help achieve space superiority. All of these operations are ultimately aimed at predetermined political ends.

Similarly, the "all aspects unified" concept requires seeing various wartime activities, including offensive and defensive operations, provision of information support and fire support, and "hard-kill" and "soft-kill" methods, in an integrated or unified fashion, rather than as discrete phases, tasks, or methods. Proper conduct of space operations should involve the application of soft-kill methods such as dazzling or jamming, in coordination with hard-kill methods such as direct ascent, kinetic kill vehicles. Space operations should be coordinated with terrestrial operations, not only for the provision of meteorological, positioning and navigation, and communications information from space systems but also for air, land, and sea attacks on an enemy's space launch and mission support facilities.

To this end, command and control of space operations plays a central role. Not only must space activities, including offensive and defensive operations, be closely controlled, but competing demands for reconnaissance and early warning, communications, navigation, and various other space information support assets must also be managed. This encompasses not only military space assets but civilian and commercial systems as well. Space operations must therefore be integrated into overall joint campaign plans. Command and control of space operations must reconcile space-related requirements, timing, and structure with those of the overarching joint campaign.[29] This integrated C2 network, capable of drawing upon military, civilian, and commercial resources, is a vital means of unifying all aspects.

The concept of "key point is establishing space dominance" in part builds upon the PLA's emphasis on striking the enemy's "key points" (*zhongda yao hai*; 重打要害), especially nodes within the enemy's "combat system of systems" (*zuozhan tixi*; 作战体系). As a key point is to establish space dominance, the PLA commander will concentrate his or her best forces and capabilities to precisely strike key targets with a combination of hard- and soft-kill weapons, in order to paralyze the adversary.

Massive advances in information technology allow more networking of forces and weapons across the land, sea, air, space, and electromagnetic/cyber domains. While this networking has significantly advanced combat effectiveness by creating synergies across various forces, it has also introduced a new set of vulnerabilities. Chinese writings note that, given the importance of space

systems for positioning, navigation, and timing (PNT), disruption of associated networks will disrupt the OODA loop. Therefore, key point strikes in joint operations should seek to disrupt the enemy's PNT constellations, as well as information collection and transmission nodes and C2 networks. In the Chinese view, such attacks will cause the adversary's integrated systems of systems to decohere.

The concept of "key point is establishing space dominance" consequently emphasizes securing space dominance, comprehensively applying various tactics and forces, in different ways, including interference, obstruction, disruption, and destruction of enemy's space-related systems (including terrestrial facilities and data links). The objective is both to prevent the enemy from operating its space systems and to preserve one's own space operations. Establishing space dominance also encompasses space exploitation, whether by providing information support to terrestrial operations, undertaking space deterrence, or engaging in operations against remaining enemy space assets.[30]

The concept of "key point is establishing space dominance" has several implications. One is the need to prioritize the securing of space dominance. PLA commanders must allocate resources against enemy space systems (terrestrial facilities, orbiting platforms, data links) and cannot shortchange these operations. These attacks must be sustained throughout the course of the conflict, but special attention should be paid to the first battle, which is likely to influence the entire course of the conflict.

As important, one must also prioritize the defense of one's own space infrastructure, since the enemy is pursuing space dominance as well. This will entail incorporating both hard and soft defenses, including deceptive measures to mislead an opponent, as well as hard defenses to counter their attacks directly.

Even with the full range of national space assets at one's command, there remains only a limited resource base. Chinese analysts recognize that space systems are fragile; as important they are extremely expensive, so even wealthy nations are unlikely to have a substantial reserve of platforms. Nor do many nations have redundant terrestrial space launch and mission control networks. (China, with four launch facilities, is unique.) Therefore, a final aspect of the "key point is establishing space dominance" concept is that space operations need to be focused and not scattershot. Attacks against adversary space infrastructure need careful coordination with other operations. They should be undertaken at essential moments in the overall campaign, to maximize effect.

SPACE DOMINANCE AND INFORMATION DOMINANCE

In the decades since the first Gulf War, Chinese assessments of the relationship between space dominance and information dominance have evolved.

There has been growing emphasis in Chinese writings on establishing the former in support of the latter.

Several PLA analyses, for example, have observed that space is the "strategic high ground" (*zhanlue zhigao dian*; 战略制高点) in informationized warfare. They conclude that dominating the space domain will have greater impact on informationized warfare than controlling any other, because space assets provide:

- Real-time global monitoring and early warning, such that no major military activity can occur without being spotted;
- Secure, long-range, intercontinental communications; and
- Positional and navigational information that will support long-range, precision strikes, including against targets that are over the horizon.

All of these capabilities are unrestricted by political borders, physical geography, or weather conditions and time of day.[31]

With space dominance, the PLA can both obtain information support and deny such support to the adversary. The American reliance on space systems, in particular, has been remarked upon. One Chinese assessment notes substantial American investment in satellite support for military communications, navigation, reconnaissance and surveillance, ballistic missile early warning, and environmental monitoring.[32] Chinese space dominance would affect all these capabilities.

Nor is the United States unique in its space dependence, in the Chinese view. PLA writings indicate close observation of other nations' space developments. Russian space developments, in particular, garner heavy Chinese attention. The Chinese military textbook *Military Astronautics* discusses Russian as well as American aerospace forces.[33] The 2013 edition of *The Science of Military Strategy* observes that Russia has made space a major focus of its military refurbishment effort and that Moscow has increased its investments in the space sector as the Russian economy has improved.[34] The Chinese believe that Russia, too, is heavily dependent on space. One Chinese volume related the Russian observation that "If Russia did not have an advantage in space, then it would not have reliable communications and reconnaissance, in which case, it would lack modernized information systems," leaving Russia blind and deaf.[35]

The relationship between information and space dominance will make the struggle for the latter that much more pointed. Chinese authors believe that without space dominance, one cannot obtain information dominance and aerial dominance, and therefore one cannot achieve land or maritime dominance. Space will inevitably be a battleground, if only to deny an adversary free use.[36] Neither side can afford to neglect this theater, as it will be a central determinant of who will secure information dominance.[37]

MISSION AREAS ASSOCIATED WITH SPACE OPERATIONS

PLA analysts believe that military space operations are likely to entail five broad "styles" (*yangshi*; 样式) or mission areas: space deterrence, space blockades, space strike operations, space defense operations, and provision of space information support.[38] Chinese space operations will not be undertaken alone but as part of a larger, joint campaign, in support of information dominance.

Space Deterrence (*kongjian weishe;* 空间威慑)

Space deterrence is the use of space forces and capabilities to deter or coerce an opponent, preventing the outbreak of conflict or limiting its extent should conflict occur. Space deterrence is possible because space-derived information increasingly affects not only military but economic and social realms. By displaying strong space capabilities and demonstrating determination and will, the PLA seeks to induce doubt and fear in an opponent over the loss of access to information gained from and through space and resulting repercussions. The adversary would either abandon its goals or else limit the scale, intensity, and types of operations, benefiting the PLA and the PRC.[39]

The Chinese concept of space deterrence is "not" focused on deterring an adversary from conducting attacks against China's space infrastructure. Instead, it is focused on employing space systems as a means of influencing the adversary's overall perceptions, in order to dissuade or compel it into acceding to Chinese goals. Thus, it is not so much deterrence *in* space, as deterrence *through* space means.

Space capabilities are seen as contributing to overall deterrent effects in a number of ways. One is by enhancing other forces' capabilities. Conventional and nuclear forces are more effective when they are supported by space-based platforms, providing navigational, reconnaissance, and communications information. Nuclear and conventional deterrence become more effective and therefore more credible.

Space systems may also coerce or dissuade an opponent on their own. Space systems are very expensive and hard to replace. An adversary whose space systems are at risk must weigh costs and benefits. Is the focus of Chinese deterrence or coercive efforts (e.g., Taiwan, the South China Sea) worth the likely cost of repairing or replacing a badly damaged or even destroyed space infrastructure?

Moreover, because space systems affect not only military but economic, political, and diplomatic spheres, damage to space systems will have wide-ranging repercussions.[40] Would the loss of information from space-based systems on other military operations or on financial and other activities generate

even worse consequences than acceding to Chinese demands? The Chinese clearly hope that the adversary's calculations would conclude that it was better not to challenge Chinese aims. Even the threat of interference and disruption of space systems "will impose a certain level of psychological terror, and will generate an impact upon a nation's policy-makers and associated strategic decision-making."[41]

PLA teaching materials suggest that there is a perceived hierarchy of space deterrence actions, somewhat akin to an "escalation ladder." These involve displays of space forces and weapons; military space exercises; deployment or augmentation of space forces; and employment of space weapons.

"Displays of space forces and weapons" (*kongjian liliang xianshi;* 空间力量显示) occur in peacetime or at the onset of a crisis. These warn an opponent, in order to dissuade it from escalating a crisis or pursuing courses of action that will lead to conflict. Such displays include using various forms of media to highlight one's space forces and are ideally complemented by political and diplomatic gestures and actions, such as inviting foreign military attaches to attend weapons tests and demonstrations.

"Military space exercises" (*kongjian junshi yanxi;* 空间军事演习) can occur in peacetime or as a crisis escalates, if displays of space forces and weapons are insufficient to compel an opponent to alter course. They can involve actual forces or computer simulations. They demonstrate one's capabilities but also display ongoing preparations. Such exercises will also improve military space force readiness. Examples include ballistic missile defense tests, antisatellite unit tests, exercises demonstrating "space strike" (*kongjian tuji*; 空间突击) capabilities, and displays of real-time and near-real-time information support from space systems.

"Space force deployments" (*kongjian liliang bushu;* 空间力量部署) are considered a significant escalation of space deterrent efforts. These involve rapid adjustments of space force deployments and are undertaken when one concludes that an opponent is preparing for war. As with military space exercises, this measure not only seeks to deter an opponent but, should deterrence fail, will improve one's own preparations for combat. Undertaking this step, which may involve moving on-orbit assets and/or deploying additional platforms and systems, should lead to local superiority of forces over the adversary. It may also involve the recall of certain space assets (e.g., space shuttles), either to preserve them or to allow them to prepare for new missions. This may be comparable to the evacuation of dependents from a region in crisis, as a signal of imminent conflict.

The Chinese term the final level of space deterrence as "space shock and awe strikes" (*kongjian zhenshe daji;* 空间震慑打击). If the three previous, less violent deterrent measures are insufficient, then the PLA may conduct punitive strikes to warn an opponent that China is prepared for full-blown,

comprehensive conflict in defense of the nation. Such strikes are seen as "the highest, and final technique" (*zuigao xingshi he zui hou shouduan*; 最高形式和最后手段) in deterring and dissuading an adversary. These can involve hard-kill methods, soft-kill methods, or a combination. If successful, opposing decision makers will be psychologically shaken and cease their activities. If it fails, an opponent's forces will nonetheless have suffered some damage and losses.

Space Blockade (*kongjian fengsuo zuozhan;* 空间封锁作战)

Space blockades use space and terrestrial forces to prevent an opponent from entering space and from gathering or transmitting information through space. There are several different varieties of space blockade activities. One is blockading terrestrial space facilities, including launch sites; TT&C sites; and mission control centers. They can be disrupted through kinetic means (e.g., special forces, missiles) or through electronic and network warfare efforts.

Another means is to obstruct orbits. This includes destroying orbiting satellites or else obstructing orbits, such as by creating clouds of space debris or deploying space mines. Just threatening satellites might limit their function (e.g., by forcing them to engage filters or maneuver to a new orbit). The risk, however, is that either such step might damage third-party space systems, which in turn could generate strategic consequences. Therefore, Chinese writings emphasize that space blockades impose very high requirements for precise control; extremely detailed space situational awareness; and highly focused, limited deployment of weapons.

Another alternative is the obstruction of launch windows. If one can delay a launch, whether by interfering with onboard systems or otherwise disrupting the schedule, then a satellite may not reach its proper orbit at the right time. In the past, some American space launches have been delayed because fishing and pleasure boats were present downrange.[42] Another obstructive technique is boost-phase intercept of a space launch vehicle.

Finally, one can impose an information blockade. One approach is interfering with and disrupting data links between terrestrial control stations and satellites. By hijacking the satellite's control systems or preventing ground control from issuing instructions, it is effectively neutralized. Alternatively, one can interfere with the data that the satellite is collecting or transmitting. Rather than tampering with the satellite's controls, one can contaminate or block the data that is passing through it. A third form of information blockade involves "dazzling" a satellite, using low-powered directed-energy weapons against sensors or other systems. In each case, the intent is to effect a "mission kill," whereby the satellite cannot perform its functions but is not necessarily destroyed.

Space Strike Operations (*kongjian tuji zuozhan;* 空间突击作战)

The ability to conduct space strike operations is essential for space deterrence and space blockades. These operations involve space and terrestrial forces pursuing offensive operations against the range of enemy space-related targets, including those in orbit, on land, sea, and air. In general, space strike operations attack vital strategic and operational space-related targets, that is, "key points."[43]

Space strike operations, in the Chinese view, are marked by "integrated operations; stealth and surprise; key point strikes; rapid, decisive action." "Integrated operations" reflect the need to coordinate space strike operations with land, sea, and air operations, to forge "integrated combat power" (*zhengti weili*; 整体威力). They should be undertaken at key moments when the enemy least expects it, exploiting stealth. They should also incorporate unexpected methods and tactics, not only to maximize material damage but also to undermine enemy morale. By employing a mixture of hard- and soft-kill methods, one can maximize stealth and generate additional surprise by confusing an opponent, making it harder to defend against.

"Key point strikes" refers here to tightly focused space operations, concentrating space forces along the main direction, at key times, against key targets in the enemy's combat systems of systems. The goal is to disrupt, attrit, and paralyze the enemy's combat systems of systems, to prevent the enemy from generating integrated capabilities.[44] This also requires carefully assessing the enemy's space architectures and identifying key systems and vulnerabilities.

"Rapid, decisive action" denotes using space strikes to seize the overall initiative in a campaign. With an overwhelming initial volley followed by sustained strikes, one can not only retain the initiative but achieve operational goals and rapidly conclude the conflict. At the same time, due to limited numbers of available space platforms and weapons, their fragility, and their expense (which limits numbers acquired), space strike operations are likely to be of relatively limited duration.

In the Chinese conception, space strike operations involve attacks against the full range of enemy space-related systems. One key target is the enemy's various satellite constellations. These can be attacked by a variety of hard-kill methods, such as directed-energy weapons, kinetic kill vehicles (such as the one used in the 2007 antisatellite test), and space mines and coorbital antisatellite systems.[45]

Equally useful are such information warfare methods as "space electronic warfare and space network warfare" (*taikong dianzi zhan he taikong wangluo zhan;* 太空电子战和太空网络战). Integrated network electronic warfare (INEW) methods applied in space can interfere and disrupt various enemy satellite systems, including onboard computers and other electronic

components. Such methods can achieve a "mission kill," effectively neutralizing the platform, without generating debris associated with collisions by kinetic kill vehicles and other physical attacks. Such soft-kill methods are a vital means of conducting space information combat.

In addition, just as terrestrial information operations include integrated information–firepower attacks, the same is true for space. Attacking an opponent's terrestrial space support functions is an essential means, in the Chinese view, of securing an advantage, comparable to traditional attacks against enemy command nodes or military bases.[46] Such attacks also retard an opponent's ability to reinforce or replace damaged or destroyed orbiting systems. As one analysis notes, striking at both space and terrestrial targets is necessary to establish local space superiority.[47]

Therefore, Chinese analyses indicate that they will target the ground component of the enemy's space architecture, including launch sites and attendant data and communications systems linking them together. Air, naval, ground, and special operations forces are therefore part of the arsenal of offensive space weapons, alongside ASATs and laser dazzling systems.[48]

Chinese authors, however, also recognize that attacks against terrestrial targets, especially those based in the enemy's home territory, will generate significant strategic implications and potential repercussions. Therefore, attacks against strategic space targets require the approval of highest-level political authorities.[49]

Chinese analysts also believe that space strike operations will eventually include space-to-ground offensive operations; that is, space-based weapons will bombard terrestrial targets. Some Chinese commentators, for example, have posited that the X-37B unmanned space vehicle might serve as a basis for prompt global strike capability.[50] They clearly see parallels between the development of space power and air power, that is, a steady move from providing information support (aerial artillery observation, space-based reconnaissance and surveillance) to attacks against the enemy's information support systems (fighters, ASATs), to the provision of fire support.

Defensive Space Operations (*kongjian fangyu zuozhan;* 空间防御作战)

While conducting space information operations and space offensive operations, the PLA will also undertake space defensive operations. These defend one's space systems (including orbiting satellites, terrestrial facilities, and associated data links) from enemy space or terrestrial attacks and also protect national strategic targets from attacks from space systems or ballistic missiles.[51]

Defensive space operations involve a combination of passive and active defensive measures. Passive measures make Chinese satellites harder to

track or determine their function. Chinese writings suggest that space systems should incorporate camouflage and stealthing measures, concealing spacecraft nature and functions from enemy observation and probes.[52] Other passive measures include deploying satellites into orbits designed to avoid enemy detection; employing political, diplomatic, and other channels to mislead opponents of real operational intentions or otherwise influence the enemy's decision making; and deploying false targets and decoys, to overload opponents' tracking capacities.

Because it is difficult to hide objects in space for very long, the Chinese have also shown an interest in resiliency, that is, extending survivability of space systems even after they are discovered. Some Chinese writings have discussed deploying small- and microsatellites in networks and constellations, rather than single large systems. According to one Chinese analysis, larger numbers of much smaller satellites may be as or more capable yet less vulnerable than a smaller number of larger, individually more capable systems.[53] Larger satellites should be capable of functioning autonomously, so that they continue operations even if their ground links are severed.[54] In addition, ground controllers should be prepared to move satellites, if there are indications of attack. Sufficient autonomy may be incorporated into future Chinese satellites that they can alter their orbits on their own to evade perceived attacks.

Another set of survivability measures is hardening. This can only go so far, however, since spacecraft are very fragile by nature. This is an inherent function of concentrating a number of subsystems into a small volume and the extremely hostile environment of outer space, so that any damage to the spacecraft is likely to have substantial cascading effects.[55] Similarly, while some ground facilities, including mission control facilities, might be physically hardened, the requirement for large antennae to handle telemetry imposes limits on how much physical hardening is possible.

Defensive space operations, however, do not mean solely reactive measures in the Chinese view. As one PLA article notes, one can, and should, also employ offensive means and seek the initiative in the course of space defensive operations.

More active defenses might include targeting enemy antisatellite weapons, such as previously identified coorbital ASATs. Both offensive and defensive means, moreover, should be undertaken by not only space forces but also land, sea, and air forces.[56] In the PLA's view, a combination of electronic and physical measures, including firepower strikes, may disrupt and suppress the enemy's space systems. Attacking terrestrial support components such as TT&C facilities disrupts the enemy's ability to conduct any kind of space operations, including offensive space operations, thereby helping defensive space operations.

It should be noted that the Chinese concept of "space defensive operations" does not necessarily parallel "defensive space control," as laid out in U.S.

Joint Publication 3–14 *Space Operations*. Indeed, some aspects would seem to overlap "offensive space control" in the American sense.[57]

Space Information Support Operations (*kongjian xinxi zhiyuan zuozhan*; 空间信息支援作战)

In the 2005 edition of *Military Aerospace,* a PLA textbook on military space activities, provision of information support by space systems was listed as the second task, after space deterrence.[58] In PLA teaching materials published in 2013, provision of information support by space systems was now the fifth of five tasks. This suggests that space information support operations, while still important, are being eclipsed by more active space offensive and defensive measures. Indeed, as one Chinese assessment observes, space resources are increasingly important, and military aerospace technology, especially those related to offensive space operations, is steadily improving. Consequently, space force development is shifting focus from providing information support toward securing space dominance.[59]

Nonetheless, in the context of informationized warfare, space dominance most benefits provision of space information support. As the 2013 edition of *The Science of Military Strategy* notes, "space information support is now and for a long time into the future the main form (*zhuyao fangshi*; 主要方式) by which various nations apply space strength."[60] As PLA joint operations mature, they will increasingly depend on space-based systems for information support, especially as Chinese forces move farther and farther away from Chinese territory (and, therefore, land-based information support infrastructure).

Key tasks within "space information support" (*kongjian xinxi zhiyuan*; 空间信息支援) to the ground, air, and naval forces include:

- Space reconnaissance and surveillance;
- Early warning of missile launches;
- Communications and data relay;
- Navigation and positioning; and
- Earth observation, including geodesy, hydrographics, and meteorology.

*Reconnaissance and Surveillance (*kongjian zhencha jianshi; 空间侦察监视*)*

Space reconnaissance is one of the oldest tasks for space-based systems and also one of the most heavily utilized. The ability to survey vast areas rapidly and continuously, as well as multiplicity of the types of surveillance possible (including not only electro-optical surveillance in the visible light spectrum but also electronic signatures and radar imaging), makes satellite reconnaissance invaluable. Reconnaissance satellites provide not only strategic intelligence but increasingly support operational and tactical activities.[61]

Space-based reconnaissance and surveillance systems are essential for battlefield surveillance in support of information warfare efforts. Because they can undertake electronic as well as electro-optical reconnaissance, they help detect and locate enemy electronic systems, communications, and radar networks.[62] This, in turn, provides the basis for not only cataloging enemy electronic networks but also targeting. Thus, space-based reconnaissance systems play a central role in INEW and integrated firepower–information operations.

Chinese reconnaissance satellites include the *Ziyuan* series of electro-optical satellites; the *Gaofen* electro-optical satellites; and the *Yaogan* series of satellites, which include both electro-optical and synthetic aperture radar satellites. It is believed that some of the *Shijian* and *Yaogan* satellites may have electronic intelligence (ELINT) functions.[63]

*Space Missile Early Warning (*kongjian daodan yujing; 空间导弹预警*)*

Space systems provide early detection and tracking of ballistic missiles throughout their flight. As several PLA analyses note, satellites allow the prompt issuance of missile attack warnings and can help predict both flight paths and impact locations. They are described as an essential part of ballistic missile early warning systems and have advantages over terrestrially based early warning radars or airborne early warning aircraft. Moreover, a networked series of satellites can maintain a constant watch of any spot on the earth for missile launches. In one Chinese analyst's view, this will become an increasingly important capacity, as the threat from ballistic missiles increases.[64]

Given the growing number of PLA ballistic missile defense tests, tracking adversary ballistic missiles is apparently a growing Chinese concern. Insofar as the PRC appears interested in deploying its own ballistic missile defense systems, early warning satellites are likely to be incorporated into them.

Unlike the United States and the Soviet Union, both of whom developed missile early warning satellites as priority projects, the PRC has not deployed such a constellation. As of 2016, there is still debate about whether China has yet deployed missile early warning satellites, although unconfirmed reports suggest a 2015 Chinese launch may have been of such a system.[65]

*Space Communications and Data Relay (*kongjian tongxin shuju zhongji; 空间通信数据中继*)*

The importance of integrated joint operations in future "local wars under informationized condition" gives space-based communications and data relay systems a more central role. This includes fixed and mobile earth stations, communications terminals, and communications and data relay satellites.[66]

Such systems provide global connectivity for a large number of users simultaneously and can provide wide bandwidth. Like reconnaissance satellites, they can also provide coverage around the clock, through a variety of weather conditions. Moreover, the Chinese see satellite communications as more secure.[67]

In light of the benefits of space communications and data relay systems, it is noteworthy that the PRC has been deploying data relay satellites since 2008.[68] The Tianlian-1 satellite was launched on April 26, 2008, augmenting the PRC's satellite reconnaissance capabilities. As Chinese authors have noted, only with such relay systems can intelligence information be smoothly and rapidly transmitted.[69] Combining communications and data relay satellites allows commanders and subordinate units to communicate with each other rapidly, reliably, and securely, across vast distances, improving shared situational awareness. Since joint operations, in the Chinese assessment, require forces to operate as "an organic, integrated whole" (*yige youji de zhengti*; 一个有机的整体), communications satellites are an essential means of forging such "an integrated set of combat capabilities" (*zhengti zuozhan xiaoneng*; 整体作战效能).[70]

China fields a number of communications satellites, which have a variety of names, including *Zhongxing* (China Star) and ChinaSat. Many of these are managed by commercial companies, as part of global telecommunications networks. However, some are believed to be part of two military satellite communications networks: *Shentong* (roughly, Permeating) and *Fenghuo* (Signal Fire). The PRC has generally not discussed whether any given satellite is a military satellite or has military functions.

*Space Navigation and Positioning (*kongjian daohang dingwei; 空间导航定位*)*

Chinese space and military planners have recognized the importance of space-based positioning, navigation, and timing capabilities since the first Gulf War. China became only the third nation to deploy a satellite-based navigation system when it placed the first Beidou satellites into geosynchronous orbit in 2000.

Space navigation and positioning systems provide users with continuous, real-time, highly precise information regarding three-dimensional position and speed, under all weather conditions, day and night. They also provide global timing functions, which improve the accuracy of various automated systems. For example, frequency hopping radios use this for timing the changes of frequency. PLA analysts also view these satellites as the prerequisite for long-range, precision-strike capability, reducing friendly casualties while inflicting more damage. These benefits help create decisive advantage at times and places of one's own choosing when attacking an opponent.[71]

Space-Based Weather Observation (*kongjian qixiang guance; 空间气象观测*) and Space-Based Earth Surveying (*kongjian dadi cehui; 空间大地测绘*)

By closely observing the earth and its atmosphere, space systems provide essential information about the operating environment. Weather satellites, for example, provide continuous observation of the earth's weather, including over key enemy targets. As important, those located in geosynchronous orbit can provide broad coverage, while those in polar orbits provide more detailed information about local conditions. The two together provide a comprehensive set of data. As the PLA textbook *Military Astronautics* notes, this is essential in determining appropriate weapons selections.[72]

Similarly, earth-surveying systems measure the earth's gravitational and magnetic fields, which can affect weapons guidance systems. They are also central in creating accurate military maps (still important even with satellite navigation systems) and can help locate enemy targets as well.

Interestingly, despite China's substantial investments in space systems, PLA analysts assess their space information support capacity as weak. One Chinese analysis concludes that China must expand its information-gathering capacity, with a top priority being more specialized reconnaissance satellites suitable for military use. These systems must be able to operate and respond in the initial period of any conflict, providing PLA forces with reconnaissance and early warning information.[73]

THE CHINESE VIEW OF SPACE AND INFORMATION DOMINANCE

For the PLA and Chinese security decision makers, the Information Age and the Space Age are inextricably linked. The growth in computing power and the role of telecommunications has heavily influenced both. Indeed, China's first series of satellites, the Dongfanghong-2, were communications satellites.

Chinese analyses of recent wars underscore the intimate relationship between these two realms in warfighting. Modern wars have demonstrated the linkage between information and space, where space systems play a central role in collecting, transmitting, and exploiting information. Consequently, "seizing the space information advantage as a high ground is the first decisive condition for seizing information dominance, space dominance, air dominance, naval dominance, land dominance, and therefore the initiative in wartime."[74]

By dominating space, one gains an enormous advantage in accessing information and managing information flow.

- *The battlefield is much more transparent*. Combat forces can therefore be much more effective, since enemy and friendly dispositions will be known.
- *Command and control is much more precise and capable*. Because the battlefield is more transparent, commanders can respond in real-time

or near-real-time to enemy actions, and widely separated units from a variety of services can act in a highly integrated manner.

- *It makes noncontact, nonlinear warfare possible.* By dominating outer space, one secures the most important portion of the battlefield, that of information space. The more transparent battlefield and facilitated command and control enables long-range, precision strikes, which the adversary is hard-pressed to counter. Friendly casualties are reduced, while one's actions are much more effective.

For Chinese military planners, these advantages are further enhanced by certain geographic and strategic realities. China, even now, remains focused on such nearby flashpoints as Taiwan, the Korean Peninsula, the South China Sea, and the Sino-Indian border.

Consequently, the PLA can bring to bear substantial resources, drawn from across the country if necessary, to establish information dominance. PLA forces can be supplemented by mobilized civilian assets, ranging from fishing boats for maritime surveillance to the militia for camouflage and deception operations. Shorter-range assets from fast attack craft to older fighter aircraft can similarly be employed to counter adversary information collection platforms. Communications can be sustained through fiber-optic cables, cell phones, line-of-sight radios, as well as satellite communications, enhancing communications security and providing redundancy. In many ways, China does not need space for the PLA to operate in accordance with its doctrine.

By contrast, the United States is an expeditionary military, operating far from American shores. In time of conflict, it relies upon space-based systems even for operational communications, especially to coordinate disparate, separated forces, as well as for intelligence collection against targets halfway around the globe. As important, American military planners have chosen to rely on space-based assets for positioning, navigation, and timing, whether it is aircraft routing, shipborne navigation, or weapons guidance. The combination of geostrategic conditions and weapons acquisition policies makes American forces much more dependent upon space.

In short, in the struggle for information dominance, because of the asymmetric strategies and starting conditions, there is a resulting asymmetric dependence on space. Chinese ability to dominate space would deny its use to an adversary—strategically benefiting China even more.

At the same time, it is important to recognize that the various space architectures are microcosms of the larger information battlefields. Space networks, encompassing satellites, terrestrial support structures such as mission control, and data links connecting them, are themselves systems of systems bound together via information networks. Satellites require communications and data links, not only to carry information about various targets or to provide navigation and other updates but also to allow mission control to monitor the

satellites' status, adjust their orbits, update their software, and otherwise manage and control their operations. It is this tracking, telemetry, and control (TT&C) network, and the information flow governing satellite constellations and linking them back to the earth, that allows space systems to operate. Damaging or affecting that flow can effectively neutralize the constellation or even allow an adversary to take control of one or more satellites. Its preservation is vital for securing information dominance. Denying the adversary satellite monitoring and control, that is, denying it information about its space assets, can devastate its larger ability to establish information dominance.

It is for this reason that the Chinese emphasize that space dominance entails not only targeting satellites but ground facilities such as mission control sites and the data links connecting them. The struggle for space dominance is, in fact, a part of the larger struggle for information dominance. It is the facet that occurs within the confines of the two sides' space architectures.

7 Chapter

Organizing to Secure Information Dominance

Given the emphasis placed in Chinese writings on securing information dominance, it is essential to understand how the People's Liberation Army (PLA) is organized, especially for conducting information warfare. The PLA, as an organization, is organized differently from many other militaries, especially those of the United States and other Western powers.

In the first place, it is not a national military per se. Instead, the PLA is, first and foremost, a party army; that is, it is the armed wing of the Chinese Communist Party (CCP). As such, the PLA's first loyalty, as noted in an earlier chapter, is to the CCP, and its paramount "new historic mission" is to ensure the CCP's continued rule. Furthermore, because it is a party army, a substantial element of the PLA is dedicated to political warfare, which in turn also provides the basis for conducting psychological and other forms of information warfare.

In addition, the PLA has historically been neither organized primarily along service lines nor answering to the Ministry of National Defense (MND). Instead, it has been primarily managed by the party's Central Military Commission (CMC) and its constituent four general departments, which are superior to the various services and to the MND. The PLA reorganizations that began on December 31, 2015, have not altered these fundamental aspects.

OVERALL PLA ORGANIZATIONAL STRUCTURE

The Chinese armed forces, which include the PLA, the People's Armed Police (PAP), and the militia, are headed by the CMC. The head of the CMC is its chairman, who is usually also the head of the CCP (the General Secretary of the party) and the head of the Chinese government (the Premier). This overlapping set of responsibilities is a reminder that not only is the party in charge

of the nation but "the party controls the gun." The head of the CCP simultaneously controls the levers of governmental power as well as holds ultimate control of the military, which is a part of the party.

Under the chairman of the CMC are two vice-chairmen, the most senior uniformed officers in the Chinese armed forces. The 2012 CMC was the first to have a vice-chairman drawn from the navy. Up until then, no PLA Navy (PLAN), PLA Air Force (PLAAF), or PLA Second Artillery officer had ever been appointed a CMC vice-chairman.

Through 2016, the CMC leadership exercised command of the armed forces through four general departments, as well as the headquarters of the PLAN, PLAAF, and Second Artillery and the People's Armed Police.[1] The four general departments are as follows:

General Staff Department (GSD). The GSD is responsible for many of the central functions of military operations, including formulating war plans, overseeing training, developing and promulgating doctrine, as well as collecting intelligence (including about adversary forces, signals, radars and electronics, and surveying and cartography). It assists national mobilization planning. One of its main subsidiary departments is responsible for maintaining strategic communications links. Because the four general departments also manage the ground forces, there is a Service Arms Department that oversees the branches of the PLA (e.g., armor, artillery, army aviation including helicopters, combat engineers).[2]

General Political Department (GPD). The GPD ensures that the PLA remains firmly under the CCP's control. The GPD controls the political officer system, with a political officer at every level of command, party committees at battalion level and above, and party branches at company level and below. Under this system, every department aboard warships, for example, may have a separate political officer, in addition to the political officer for the entire ship (whose authority is equivalent to that of the ship's commanding officer). In addition to ensuring party discipline and individual loyalty, the GPD is responsible for much of the "people" work in the PLA. Cultural work, civil–military relations, morale issues, and personnel management are all part of the GPD portfolio. The GPD is also responsible for military legal and judicial issues, criminal investigation, and the conduct of political warfare.[3]

General Logistics Department (GLD). The GLD is responsible for maintaining the PLA's supplies, including provision of food, fuel, spare parts, munitions, clothing, and infrastructure construction. The GLD maintains a transportation department, to ensure that items can be moved where needed. The GLD also undertakes certain aspects of

military budgeting and finance, provides health services, and audits various accounts. As the PLA increasingly operates farther afield from Chinese shores (e.g., the ongoing antipiracy operations in the Gulf of Aden), the GLD's responsibilities have become correspondingly more complex. GLD training and preparations must now incorporate aspects of expeditionary logistics, obtaining support either from foreigners or from Chinese suppliers at a greatly extended distance.[4]

General Armaments Department (GAD). The GAD was created in 1998, when the Chinese leadership reorganized the defense industrial base, including key weapons development, space, and other infrastructure sites and their oversight. The GAD assumed responsibility for the nuclear test site at Lop Nor, Xinjiang; China's various space launch, tracking, telemetry, and control (TT&C), and mission control facilities; as well as other test ranges and facilities. The GAD is also apparently responsible for some aspects of equipment budgeting and auditing of some accounts. It may be that it has responsibility for equipment acquisition decisions, whereas the GLD is responsible for operations and maintenance (O&M) costs. The GAD also includes a Science and Technology Commission, which appears responsible for advising GAD about advances in various aspects of science and technology related to military and defense applications.[5]

Bureaucratically half a step below the four general departments are the heads of the various services (PLA Navy and PLA Air Force) and the Second Artillery, which was more of a "superbranch" than a full-fledged service. Like other militaries, the PLA has created services to foster expertise and provide specialized training for forces to operate in specific domains (e.g., sea, air). Until December 31, 2015, there was no separate ground forces command. Instead, the general departments not only administered the overall Chinese military but also served as the headquarters staff for the ground forces. Not surprisingly, this gave the ground forces distinct bureaucratic and political power, since it was the "default setting" for the larger PLA. Indeed, several heads of the PLAN had been ground forces commanders, given authority over the navy when they were promoted.

While the CMC administers the overall PLA, military planning is undertaken by the staffs of seven military regions, who coordinate with the CMC. These military regions somewhat resemble the "Combatant Commands" of the U.S. military, focusing on specific geographic areas. Military regions are in turn comprised of military districts, which are usually coterminous with provincial boundaries (Table 7.1).

Supplementing the regular armed forces is a substantial militia force, as well as the broader Chinese population and industrial base once mobilized.

Table 7.1 Chinese Military Regions as of 2015

Military Region Name	Provinces, Autonomous Regions, and Municipalities Encompassed	Area of Responsibility
Beijing	Beijing City, Tianjin City, Hebei, Shanxi, Inner Mongolia Autonomous Region	Russia, Mongolia
Chengdu	Chongqing City, Sichuan, Yunnan, Guizhou, Tibet Autonomous Region	India, Bhutan, Nepal, Vietnam, Burma, Laos
Guangzhou	Guangdong, Hunan, Hubei, Hainan Island, Guangxi Autonomous Region, Hong Kong Special Administrative Region, Macau	South China Sea, Vietnam
Jinan	Shandong, Henan	Strategic reserve
Lanzhou	Qinghai, Gansu, Ningxi, Shaanxi, Xinjiang Autonomous Region, Ali region of the Tibet Autonomous Region	Russia, Kazakhstan, Tajikistan, Kyrgyzstan, Afghanistan, Pakistan, India
Nanjing	Anhui, Jiangsu, Jiangshi, Fujian, Zhejiang, Shanghai City	Taiwan, East China Sea
Shenyang	Jilin, Heilongjiang, Liaoning	Korean Peninsula, Japan

The Chinese envision "national defense mobilization" as converting all aspects of potential national power to augment their actual wartime capacity. For the PLA, mobilization converts several broad categories of resources, including human talent, financial power, industrial capacity, and scientific and technical capacity, into military capability. It allows the exploitation of civilian and commercial equipment and facilities, as well as personnel, to meet wartime needs. Coupled with long-standing Chinese interest in civil–military integration of infrastructure and resources, and an emphasis on dual-use capacity, especially in high-technology areas as space and telecommunications, Chinese decision makers can call upon substantial reserve capacity to augment the regular armed forces.

Mobilization applies not only to national-level resources but also to local assets. This is typically coordinated between the command staff of the military regions and subordinate military districts on one side and provincial, county, and township authorities within the relevant military region on the other. This is managed by the nationwide structure of National Defense Mobilization Commissions.

PLA ORGANIZATIONS RESPONSIBLE FOR SECURING INFORMATION DOMINANCE

In order to conduct "local wars under informationized conditions," the PLA will especially rely on certain organizations within the PLA. In particular, certain parts of the GSD, GPD, and GAD are responsible for key information warfare and information operations portfolios. While the reporting chains have likely changed in the wake of the major reorganization unveiled in late 2015 and early 2016, the associated functions are unlikely to change for some time, wherever they reside organizationally.

General Staff Department

Given its portfolio of responsibilities, the GSD includes a number of subordinate second-level departments and third-level bureaus responsible for collecting military intelligence, signals intelligence, and radar and electronic intelligence. These departments appear to have outsize responsibilities in preparing for the conduct of informationized warfare and information warfare.

GSD Second Department

The GSD Second Department, also known as the GSD Intelligence Department and 2PLA, collects strategic-level military and political intelligence for the CMC and China's political leadership. It also collects operational-level intelligence in support of military operations. It employs a variety of sources including human intelligence (spies), space systems, and unmanned aerial vehicles. It has subordinate bureaus that are responsible for specialized analytical skills such as imagery analysis or have specific regional focus (e.g., Europe, Russia and Eastern Europe, other Asian states). The GSD Second Department apparently also helps manage China's military attachés. It encompasses many of the responsibilities that in the United States are the purview of the Central Intelligence Agency, the Defense Intelligence Agency, and the National Reconnaissance Office.

Each of the military region headquarters (MRHQ) has a subordinate GSD Second Department cell. This military intelligence section provides focused intelligence support to the MRHQ staff supporting potential military operations within their area of responsibility.

GSD Third Department

The GSD Third Department is also known as the GSD Technical Department and 3PLA. It is responsible for signals intelligence (SIGINT). This includes undertaking computer network operations, encompassing computer network espionage, computer network attack, and computer network defense. It is often compared to the National Security Agency (NSA) in the United States.[6]

The GSD Third Department has both a research and an operational side. The former includes a Science and Technology Intelligence Bureau and a Science and Technology Equipment Bureau. The latter controls three research institutes, dedicated to computer science, sensor technology, and cryptography.[7]

The operational arm of the GSD Third Department resides in 12 operational bureaus, as well as Technical Reconnaissance Bureaus (TRB) attached to the military regions and the PLAN, PLAAF, and Second Artillery.[8] The Third Department also oversees the Beijing North Computing Center, which is a key part of Chinese efforts to develop computer network attack and defense systems.

THE 12 BUREAUS OF THE GSD THIRD DEPARTMENT[9]

First Bureau (Unit 61786). This bureau appears to be responsible for preserving information security of the PLA. It is believed to have 12 subordinate offices.

Second Bureau (Unit 61398). This bureau appears to have a regional focus, aimed mainly at the United States and Canada, but it may target all Anglophone countries. It engages in computer network espionage against political and economic as well as military targets.

Third Bureau (Unit 61785). This bureau appears to engage in communications intelligence, collecting information on radio networks that operate near China's frontiers, including Taiwan, Central Asia, and Korea. It also appears to be responsible for monitoring wireless networks in Hong Kong and Macau.

Fourth Bureau (Unit 61419). This bureau is apparently focused on Japanese and Korean targets.

Fifth Bureau (Unit 61565). This bureau is apparently focused on Russia.

Sixth Bureau (Unit 61726). This bureau is apparently focused on Southeast and South Asian targets and may also cover Taiwan.

Seventh Bureau (Unit 61580). This bureau is believed to have at least 10 subordinate offices. Like the First Bureau, it may have a more functional than regional focus, perhaps focusing on various aspects of information technology.

Eighth Bureau (Unit 61046). This bureau appears to cover Europe, Africa, the Middle East, and South America.

Ninth Bureau (Unit 61221). This bureau may be responsible for strategic intelligence analysis. It may also review computer equipment for the entire armed forces, perhaps like the U.S. Defense Information Services Agency.

Tenth Bureau (Unit 61886). This bureau may be regionally oriented, especially toward Russia and Central Asia, or be focused on missile tracking and telemetry.

Eleventh Bureau (Unit 61672). This bureau may be focused on Russian-related targets.

Twelfth Bureau (Unit 61486). This bureau appears to be oriented toward space-related remote sensing and satellite information, especially from European companies, as well as aerospace and telecommunications information from European and Japanese companies.

Recent media reporting have focused on several of the operational bureaus. Cyber security firm Mandiant has highlighted the activities of Unit 61398. This is believed to be the Second Bureau of the Third Department and reportedly engages in various types of computer espionage, including collecting economic and political as well as military-related information.[10] Crowdstrike, another American cybersecurity firm, has identified extensive cyber espionage activities by the Twelfth Bureau of the Third Department, also known as Unit 61486. This bureau, also apparently named "Putter Panda," appears to be focused on satellite- and space-related information.[11]

Another computer espionage force is Unit 78020, also referred to as "Naikon." This unit is different from the other two attackers, as it is apparently a TRB associated with the Chengdu Military Region (MR), rather than one of the GSD's own operational bureaus. In addition, although the Chengdu MR is mainly oriented toward continental Southeast and South Asia, Unit 78020's activities seem to be much more wide ranging. According to cybersecurity firm ThreatConnect, working in conjunction with Defense Group International, Unit 78020

> conducts cyber espionage against Southeast Asian military, diplomatic, and economic targets. The targets include government entities in Cambodia, Indonesia, Laos, Malaysia, Myanmar, Nepal, the Philippines, Singapore, Thailand, and Vietnam, as well as . . . United Nations Development Programme (UNDP) and the Association of Southeast Asian Nations (ASEAN).[12]

WHAT ARE THOSE NUMBERS?[13]

Press reports have often referred to Unit 61398 of the Chinese People's Liberation Army. Other reports have mentioned Unit 61486 and Unit 78020. These five-digit numbers are known as "military unit cover designators" (MUCDs). These numbers are used instead of unit names (e.g., 2nd Battalion, 5th Marine Regiment, 1st Marine Division), which are apparently the "true unit identifier" and are often classified. The use of MUCD provides a means of referring to specific units in public discussions while obscuring the identity.

MUCDs are assigned in blocks to the general departments and to the services, who then apply them to units down to the regiment/brigade level. This allows for a certain degree of organizational determination. However, this capacity is limited, as units are transferred to or from various headquarters, while retaining their MUCD.

There have also been several revisions of the MUCD system, including in 2000 and apparently in 2002. In the wake of this last revision, it would appear that MUCD assignment may now be more randomized.

It is unclear as to whether the major reorganization of the PLA will also see an attendant change in the MUCD system.

Both types of bureaus are the equivalent of an army division in China's military hierarchy; thus, their commanders have the authority typically vested in a divisional commander (American O-7/brigadier general equivalent). The bureaus' actions are unlikely to be undertaken on a whim or indiscretions of junior officers and enlisted personnel.

As important, such groups' behavior has earned them the title of "advanced persistent threat (APT)." APTs are entities that undertake protracted, stealthy cybercrime and cyberespionage activities. Their goal is not simply to make money but to penetrate various information networks and systems for long periods, gathering information for various potential uses and consumers. APTs engage in targeted attacks, that is, they are not exploiting targets of opportunity but focus on specific networks and specific information.

APTs have the following qualities:

- *Advanced*. They employ many means to access targeted computer networks and systems, including malware, spyware, infected media, identity theft, human engineering to identify specific user vulnerabilities, and exploitation of backdoors and other entry methods. They often combine various measures to ensure access. Moreover, APTs will usually tailor their attack methods, modifying phishing emails, attachments, and so on, to enhance the chances of being opened.
- *Persistent*. Unlike most criminal entities, APTs are not focused on rapid financial gain or just information that can be immediately accessed. Instead, they will typically engage in continuous monitoring, installing programs that will constantly report back to the APT, or facilitate future access. The objective is to preserve access to the network and its information content over an extended period. As of 2011, the average length of APT penetration was 145 days.[14]
- *Threatening*. The APT is not a worm or virus, although such programs may be employed. Rather, it is one or more people, acting in pursuit of larger goals. APTs often involve extensive reconnaissance of the targeted networks and research about operators and users, as well as the networks.[15]

Although the GSD Third Department is part of the PLA, it typically operates in conjunction with other parts of the Chinese government, especially those responsible for aspects of information security. These include the State Council's Ministry of Science and Technology, the State Secrecy Bureau, the Ministries of Public Security and State Security, and the National Cryptologic Management Center.[16]

This apparent integration of civilian and military efforts, at least in computer network operations, supports the observation in the 2013 edition of

The Science of Military Strategy that there are three broad categories of Chinese computer network warfare forces. These are:

- Specialized network warfare forces, which are dedicated military units that specifically implement network offensive and defensive operations;
- Authorized forces, which are specialist nonmilitary units organized with military permission, drawn from local capabilities (e.g., from within a military region or war zone), including the Ministry of State Security and the Ministry of Public Security, and other relevant government departments;
- Civilian forces, comprised of voluntary civilian participants who conduct network operations after being mobilized and organized.[17]

Consequently, although individual attackers may not be identified as part of 3PLA, there is nonetheless reason to believe that GSD Third Department coordinates or even directs their efforts.

GSD Informationization Department

Known as the GSD Communications Department until 2011, the GSD Informationization Department manages strategic-level communications for the top CCP leadership, as well as strategic and tactical military communications channels. Its responsibilities are comparable to such American organizations as the Defense Information Systems Agency, the National Security Agency, and the J-6 (responsible for command, control, communications, and computers) on the Joint Staff, as well as Army signals and communications (given the GSD's role as part of the ground forces' command structure). These include overseeing national-level military command-and-control system, supporting both operational and strategic missions; coordinating communications policies among military regions; coordinating national telecommunications projects and policies with the Ministry of Industry and Information Technology (MIIT); and developing communications doctrine, including training metrics, for the PLA.[18]

When Jiang Zemin ordered the PLA to divest its business enterprises by 1999, a key exception was the information and telecommunications industries. The Communications Department has played a major role in developing China's national telecommunications infrastructure, including laying extensive fiber-optic cable networks to provide secure landline communications. The Communications Department's purview may also extend to satellite communications.

The change in name to Informationization Department suggests that this department is now coordinating the employment of various forms of information technology. This probably not only includes computer networks but may extend to software.

GSD Fourth Department

The GSD Fourth Department is also known as the Electronic Countermeasures and Radar Department. Founded in 1990 as the Counter-Electronic Warfare Department, it seems to share some SIGINT responsibilities with the Third Department.[19] It also collects electronic intelligence (ELINT), primarily at the operational and tactical levels of war. The lines separating GSD Second, Third, and Fourth Department responsibilities are blurred and perhaps serve more as guidelines.

The Fourth Department has a subordinate bureau that focuses on radar issues and another on electronic countermeasures (ECM). The Radar Bureau both improves radars and detection programs and develops systems to counter stealth and low-observable technologies. It may also research space surveillance systems, to support space situational awareness. The ECM Bureau not only develops counters to adversary electronic systems but also electronic counter-countermeasures (ECCM), allowing Chinese systems to operate in the face of adversary ECM. It is believed that the Fourth Department may operate its own ELINT satellite ground stations, as well as satellite jamming regiments.[20]

General Political Department

Waging information warfare alongside the GSD will be the General Political Department (GPD). While typically envisioned as political officers in the Soviet mode, the GPD actually has responsibilities beyond ensuring PLA political loyalty. One essential role is the conduct of various aspects of information warfare. This will occupy various departments and bureaus within the GPD. Unfortunately, literature regarding the roles and functions of the GPD is much scarcer than that for the GSD or the GAD.

General Office

The General Office manages the entire GPD, overseeing the General Department's workflow, managing paperwork, setting the agenda for various conferences and meetings by its leadership, and serving as the main interface with other general departments as well as other parts of the PLA. It is the nerve center of the GPD and arguably for the entire PLA.

In wartime, the General Office would help plan and coordinate GPD activities, both within its own bureaucratic chain (i.e., among unit political departments and political officers) and with line combat forces. Of particular importance is the Legal Bureau. Some Western analyses believe that almost all PLA lawyers are part of this bureau.[21] If that is the case, then Chinese legal warfare efforts will be coordinated through, and often undertaken by, this office.

Organization Department

The Organization Department of the GPD is responsible for the various party committees that manage PLA units. As such it also manages the political

commissars and political officers who are part of the command structure of every PLA unit. It is also one of the key points of interaction between the PLA leadership and the civilian leadership of the CCP (given the PLA's role as a party army).[22] It is likely that, if the GPD maintains a separate set of command, control, and communications links, independent of the GSD's system, it runs through the Organization Department. Therefore, the Organization Department would provide a separate means of promulgating orders and obtaining feedback and situational updates.

Propaganda Department

Given the importance of public opinion warfare, the GPD Propaganda Department will be a key player in Chinese political warfare efforts. Responsible for preparing and disseminating indoctrination materials, ideological training, and political education, the Propaganda Department controls a vast public outreach empire, including television stations and programs, film studios, publishing houses, the main military newspaper *Liberation Army Daily* (*jiefangjun bao;* 解放军报), and various artistic troupes (although many are likely to be disbanded as part of Xi Jinping's 300,000 troop cut).[23]

The Propaganda Department targets several audiences. One is the PLA itself. Ensuring that the PLA, both rank and file and officers, understands why it is fighting is a central task for the GPD. In future conflicts, bolstering military morale in the face of losses (its first in perhaps two generations) will be vital.

The successful undertaking of propaganda requires a thorough psychological understanding of target audiences. The Propaganda Department will therefore provide extensive support for both public opinion warfare and psychological warfare operations. It may also implement such operations, drawing upon combat force assets.

Given the power of the GPD, coupled with the relative importance of the Propaganda Department within the GPD hierarchy, both psychological and public opinion warfare operations will probably be high bureaucratic priorities. Moreover, the PLA has historically emphasized such operations in fragmenting and distracting adversaries. It is therefore likely that GSD and units staffs will provide staff and logistical support to such operations and be fully cooperative.

General Armaments Department

Because GAD administers most of China's space capabilities, it will also play a key role in Chinese efforts to establish information dominance. The GAD controls a range of space-related facilities. These include the following:

- *Launch facilities*. These generally include one or more launch pads, as well as facilities where satellites are mated with the launch vehicles.

There are also usually tracking facilities onsite or nearby. Available information indicates that some, and possibly all, of China's launch facilities were designed and constructed by predecessor organizations that are now part of the GAD.[24]

- *Mission control and TT&C facilities*. Once the satellite is in orbit, the satellite must still be observed and tracked. Some types of satellites, such as photoreconnaissance and earth-imaging satellites, may also need to maneuver once they are placed in orbit. These tasks are done by mission control centers and TT&C facilities. China has supplemented its ground-based TT&C facilities (largely located on Chinese soil) with a fleet of space-tracking ships.
- *Educational institution*. The key training facility for Chinese aerospace personnel is the Equipment Academy, formerly the Academy of Equipment Command and Technology.

Jiuquan Satellite Launch Center

The Jiuquan Satellite Launch Center (*jiuquan weixing fashe zhongxin*; 酒泉卫星发射中心) (JSLC) is located in the Gobi desert, near Jiuquan City in western Gansu Province. It is also known as No. 20 Testing and Training Base. Opened in 1958, it is the oldest Chinese launch facility and one of the largest, covering an area of 2,800 sq. km.[25] The facility has two launch zones: a northern one with three launch pads and a southern one with two launch pads. The southern pads support China's manned space effort. The southern launch zone also reportedly has its own launch control center.[26]

The JSLC is one of the most versatile Chinese launch centers, having handled Long March-2C (LM-2C), Long March-2D (LM-2D), and LM-2F boosters as well as the LM-4. The LM-2C provides the basic first and second stages for a number of other Chinese launchers.[27] The LM-4, with more powerful motors, has been used primarily to launch polar-orbiting satellites.[28] JSLC has placed satellites mainly into low- and middle-earth orbit. It has also been the main launch facility for China's manned systems, handling all Shenzhou spacecraft launches as of 2015.

Taiyuan Satellite Launch Center

The Taiyuan Satellite Launch Center (*taiyuan weixing fashe zhongxin*; 太原卫星发射中心) (TSLC) is located near Taiyuan City, Shanxi Province. It is also known as the No. 25 Testing and Training Base. The TSLC was constructed in 1968 as part of the missile development effort for the DF-5 ICBM. It was reportedly not incorporated into the space program until the mid-1980s.[29]

TSLC is mainly responsible for placing satellites in polar orbit. These have included the *Fengyun* weather and *Ziyuan* earth-resourcing satellites, as well as

American Iridium communications satellites.[30] TSLC was responsible for the first Chinese launch of two satellites atop a single booster.

Xichang Satellite Launch Center

The Xichang Satellite Launch Center (*xichang weixing fashe zhongxin*; 西昌卫星发射中心) (XSLC), also known as the No. 27 Testing and Training Base, is located in Xichang, Sichuan Province. Construction of the facility began in 1970 and was completed in 1983.[31] The facility has two launch pads and can handle a wide variety of boosters, including the LM-2C, LM-2E, Long March-3 (LM-3), LM-3A, and LM-3B. The LM-3 series is China's most powerful current booster, until the LM-5 is placed into service (currently estimated to be in the 2016–2017 time frame). It is comparable to the French/European Space Agency Ariane or the U.S. Delta-type launchers.[32]

The XSLC was the southernmost Chinese launch facility, until the satellite launch center on Hainan opened. Consequently, it was where China launched its geosynchronous-orbit satellites, although the facility has also launched satellites into polar and low-earth orbits.[33]

In support of China's first launch of a geostationary communications satellite, the *Dongfanghong*-2, in 1984, XSLC apparently had its mission control facilities upgraded. Booster ignition, lift-off, and initial flight status could all be observed from the mission command-and-control center, and images could be transmitted to Beijing. Improved timing equipment was also installed.[34]

Xi'an Satellite Telemetry and Control Center

The Xi'an Satellite Telemetry and Control Center (*xi'an weixing cekong zhongxin*; 西安卫星测控中心) (XST&CC) is the hub of China's space-tracking system.[35] Also known as the No. 26 Testing and Training Base, the XST&CC is responsible for tracking satellite orbits, transmitting digital data, and managing satellite information. It is also responsible for actually controlling many of China's satellites.[36] It was built near Xian in the mid-1980s, beginning operations in December 1987.[37] It also helps track China's manned space missions.[38]

China's TT&C Network

The Chinese TT&C assets controlled by XST&CC form a triangle in China, with the points at:

- Kashi (喀什), Xinjiang autonomous region;
- Sanya (三亚) on Hainan Island; and
- Jiamusi (佳木斯) in Heilongjiang Province.[39]

These are supplemented by China's fleet of space support vessels, which operate from the Aerospace Oceanic Telemetry Ship Base (*hangtian yuanyang celiang-chuan jidi*; 航天远洋测量船基地), also known as Base 23, on the Liaoning Peninsula. The current fleet is comprised of three space support vessels, *Yuan Wang-3, Yuan Wang-5*, and *Yuan Wang-6*. As with Chinese launch and TT&C facilities, these ships are part of GAD (not the PLA Navy).[40]

The GAD Equipment Academy[41]

Chinese writings indicate that the GAD trains all the personnel manning China's various space facilities. This is conducted at the GAD's Equipment Academy (*zhuangbei xueyuan*; 装备学院), formerly known as the Academy of Equipment Command and Technology (*zhuangbei zhihui jishu xueyuan*; 装备指挥技术学院). This academy trains mid-level officers to serve as managers and commanders and also trains high-level engineering and technical officers. The graduates staff China's various satellite launch centers; satellite TT&C centers; and aerospace command centers; as well as high-technology weapons equipment management, research, and testing centers.

The academy was first established in 1978 and was subordinated to the GAD when the latter was established in 1999. Its focus is on familiarizing officers in both command and technology. Chinese writings describe the school as the main academy for training in weapons and equipment program management, as well as aerospace engineering and information technology. The academy offers basic courses in a number of fields, including equipment command systems, control systems, and electronic engineering, as well as master's degrees in seven fields: computer applications, communications and information systems, signals and information management, weapons firing theory and technology, operational/combat command, military communications, and military operations research. Beginning in 1999, it also began to offer doctoral degrees in combat command.

COMMAND AND CONTROL AT THE OPERATIONAL LEVEL

For the PLA, successfully waging "local wars under informationized conditions," and to secure "information dominance," requires properly organizing and coordinating the actions of these various national-level elements, as well as the forces in the relevant military regions. Building a joint campaign command structure is therefore essential. Smooth information flows depend on fielding a properly organized command structure, allowing all the participating forces to coordinate their operations.

This command structure will be headed by a "joint campaign command headquarters" (*lianhe zhanyi zhihui jigou*; 联合战役指挥机构), hereafter

referred to as JCCH. This JCCH will be formed from the command elements of participating military region(s), services, local command elements, and senior officers seconded from the CMC. It will be divided into a primary command post, a forward command post (which may also serve as an alternate or reserve command post), and a rear-area command post.[42]

The JCCH creates and implements operational plans for the participating forces, reconciles various resource demands, coordinates various actions and activities, and reacts to developments.

Until 2016, JCCHs were not permanent entities vested with standing authority over subordinate forces. Instead, they appear to have been experimental, testing various organizational templates, while the military regions remained the main peacetime planning and organizational structure, along with service-based lines of authority. Thus, assorted types of JCCH structures have been proposed in various Chinese military writings.

One possible organization proposed in the 2006 edition of the *Science of Campaigns* is comprised of four command centers:

- *Operations center* (*zuozhan zhongxin*; 作战中心). This will include the commander of the headquarters section (*siling bu shouzhang*; 司令部首长) and command staff from relevant operations departments. This center would organize and plan the joint campaign, help coordinate commanders' decision making, and exercise C2 responsibilities.
- *Intelligence center* (*qingbao zhongxin*; 情报中心). This would contain the headquarters section commander and intelligence department personnel.
- *Communications center* (*tongxin zhongxin*; 通信中心).
- *Safeguarding center* (*baozhang zhongxin*; 保障中心). It would be organized from command-level safeguarding personnel and would undertake all operations command safeguarding missions (*zuozhan zhihui de baozhang renwu*; 作战指挥的保障任务). These missions include providing logistical and maintenance support, as well as ensuring physical security (and possibly data and information technology security).

These centers could then be supplemented as necessary, such as with a firepower coordination center or an information operations center (*xinxi zuozhan zhongxin*; 信息作战中心), depending on campaign requirements.[43]

A variation on this structure would have six centers, including a C2 center, intelligence center, communications center, an information operations center, as well as an air defense center (*fangkong zhongxin*; 防空中心) and a special operations center (*tezhong zuozhan zhongxin*; 特种作战中心). The special operations center would control all special operations forces' activities, specifying targets and coordinating special operations.

Other Chinese volumes suggest that a "basic joint operations command post" (*lianhe zuozhan jiben zhihui suo*; 联合作战基本指挥所) should be organized, comprised of a command-and-control center, with intelligence, communications, military mobilization, political work, logistics safeguarding, and equipment safeguarding departments subordinated or subsumed within it.[44]

- *Command-and-control center* (*zhihui kongzhi zhongxin*; 指挥控制中心). This center is the main support for the joint operation commander, assisting in the planning and C2 efforts for the overall force. It would provide coordination and guidance to other departments. It would also engage in information operations, as well as coordinating firepower strikes and special operations. It would be the center of command-and-control warfare efforts.
- *Intelligence department* (*qingbao bumen*; 情报部门). This department provides joint operations intelligence support. It coordinates intelligence activities, oversees intelligence collection and data management, and distributes any findings. In conjunction with the command-and-control center, it also organizes counter-recon activities and battle damage assessments. It would be a central part of intelligence warfare operations.
- *Communications department* (*tongxin bumen*; 通信部门). This department safeguards all communications associated with the joint operation and helps formulate the plans and directives associated with communications safeguarding. It would also help guide and coordinate other communications activities of subordinate forces, including frequency and spectrum management. It would also coordinate interactions with civilian communications assets.
- *Military affairs mobilization department* (*junwu dongyuan bumen*; 军务动员部门). This department organizes military affairs, mobilization, and ground warfare management work. It is also responsible for coordinating with local governments for supplementing military transportation, obtaining material support, undertaking mobilization of various scientific and technical resources, and other interactions with local assets.
- *Political work department* (*zhengzhi gongzuo bumen*; 政治工作部门). This department undertakes propaganda, legal affairs, mass work, and other political work matters. This includes planning, directing, and managing political work for the campaign and overseeing political work in subordinate units. It also includes undertaking political warfare tasks, including the "three warfares," as well as managing media outreach generally, and political mobilization.
- *Logistics safeguarding department* (*houqing baozhang bumen*; 后请保障部门). This department coordinates operational logistics and

safeguarding. It apprises the command-and-control center of logistical status, manages information flow between the main command post and rear-area command posts, and provides logistical planning for the campaign.

- *Equipment safeguarding department* (*zhuangbei baozhang bumen*; 装备保障部门). This department ensures equipment maintenance and security, coordinating such efforts across all participating forces.

All these proposed structures include a command or command-and-control center responsible for operational planning, coordination, and oversight of participating forces; a communications center or department; and an intelligence center or department. Several also have one or two departments responsible for aspects of safeguarding (*baozhang*; 保障), such as equipment safeguarding (ensuring physical security and maintenance support for physical assets) and data safeguarding (data integrity and IT support).

THE REFORMS OF 2016

While the PLA has undertaken several modernization efforts since the 1980s, it largely adhered to a structure that it had inherited from the Mao and Deng era. It recognized, however, that this structure did not meet the demands of fighting and winning "local wars under informationized conditions." There was no permanent joint operational command. Instead, the ground forces remained politically and bureaucratically dominant, as reflected in the military region command structures—none were headed by naval or air officers.

This changed at the end of 2015, when Xi Jinping announced the first of at least three major PLA reorganization efforts (as of April 2016). The overall thrust of these major reorganizations is encapsulated in the aphorism that Xi issued in November 2015: "The Central Military Commission manages the overall military, the war zones are in charge of conflict, the services are in charge of construction (*junwei guanzong, zhanqu zhu zhan, junzhong zhu jian*; 军委管总，战区主战，军种主建)."[45] That is, the CMC would be restructured to better manage the entire military; the war zones would be responsible for planning and coordinating wartime functions; the services would be responsible for equipping, training, and providing suitable forces (Table 7.2).

Creating New Services

The first component was the announcement of the creation of three new service commands, made on the last day of 2015.[46] Joining the PLAN and PLAAF would be:

The PLA Ground Forces Command. The ground forces are now a distinct, separate service. This means that ground forces have been downgraded

in political influence, as they are no longer the default source of senior commanders and the heads of the various general departments. It also suggests that various institutions, from the Academy of Military Sciences to weapons development centers, will address other service concerns more consistently.

The PLA Rocket Force (PLARF). The Second Artillery, which controlled both China's land-based nuclear deterrent and much of its conventional missile forces, was not a service, but a "superbranch." It was an offshoot of the ground forces' artillery branch. Xi, however, has formally made the "PLA Rocket Force" a service, making it eligible for a strategic mission but also to head one of the new war zone/theater commands.

The PLA Strategic Support Force (PLASSF). Perhaps the most important of the new services for establishing information dominance, is the "PLA Strategic Support Force." The PLASSF gathers together not only China's space forces from the GAD but reportedly Chinese electronic warfare and network warfare capabilities.[47] If accurate, then the PLA is presumably shifting elements from the GSD Third and Fourth Departments (SIGINT and radar/electronic warfare) to this new service as well. It might also receive elements of the GSD Communications/Informationization Department and the GSD Second Department. This new service will therefore bring under a single bureaucratic umbrella all the key combat elements that PLA analyses conclude are needed for waging information warfare.

Reorganizing the Central Military Commission

In January 2016, the PLA announced a second set of reforms aimed at the CMC. Where the CMC had previously been organized around the four general departments, only joined by the services and Second Artillery branch in 2004, the future CMC will be organized around *15* subordinate functional organizations.[48]

This new CMC will be managed by the CMC General Office. Although such an entity has likely always existed, by specifically enumerating it, this suggests that the new General Office will be a bureaucratic power center in its own right.

Six departments (*bu*; 部) will manage key aspects of military planning:

- *CMC Joint Staff Department* (*junwei lianhe canmou bu*; 军委联合参谋部). This would appear to be the new iteration of the previous General Staff Department. Incorporating "joint" in its name, though, emphasizes that the new department is not an offshoot of the ground forces but responsible for promoting joint thinking.

- *CMC Political Work Department* (*junwei zhengzhi gongzuo bu*; 军委政治工作部). The PLA remains a party army, an aspect that has not changed in this reorganization. Political work remains an essential part of PLA thinking. As important, the political officers and party committee structure remain a central element of the PLA's administration.
- *CMC Logistics Safeguarding Department* (*junwei houqin baozhang bu*; 军委后勤保障部). No changes are currently evident in the logistics structure and organization.
- *CMC Equipment Development Department* (*junwei zhuangbei fazhan bu*; 军委装备发展部). This entity will probably be responsible for developing Chinese weapons, in conjunction with the Ministry of Industry and Information Technology (MIIT) and its subordinate State Administration for Science, Technology, and Industry for National Defense (SASTIND), which oversee the Chinese military industrial complex. However, with the shift of space assets to the new PLA Strategic Support Force, this department is unlikely to have as many operational units.
- *CMC Training Management Department* (*junwei xunlian guanli bu*; 军委训练管理部). This is a new entity with no counterpart in the previous CMC structure. It suggests that the PLA will prioritize training and that the same training metrics are applied across the entire force. It is likely to emphasize joint training tasks.
- *CMC National Defense Mobilization Department* (*junwei guofang dongyuan bu*; 军委国防动员部). While there has been a National Defense Mobilization Commission since the 1990s, that entity straddled governmental, party, and military lines. The creation of a CMC department specifically focused on defense mobilization indicates the PLA will devote more effort to specific military mobilization concerns. This department will probably expand training and planning for incorporating civilian assets and facilities as well as personnel. High priorities for such mobilization planning efforts will probably include telecommunications, computing, and space assets and facilities, as well as civilian experts in these fields.

These departments will be supplemented by three commissions (*weiyuan hui*; 委员会), overseeing discipline (including countering corruption); politics and law; and science and technology. This last is likely to include some of the duties of the former GAD's Science and Technology Commission, which resembled the Defense Advanced Research Projects Agency (DARPA) and specialized expert groups like the "Jasons" in the U.S. Department of Defense. This commission will probably try to identify key new areas of militarily useful technology.

Finally, five offices (*bangong shi*; 办公室) will have administrative responsibilities. These will include offices for strategic planning, reform and organization, international cooperation, financial audits, and a general administrative office. The precise responsibilities have not been publicly discussed nor how

Table 7.2 The New Central Military Commission Organization

English Name	Chinese	Pinyin
CMC General Office	军委办公厅	Junwei bangong ting
Departments		
CMC Joint Staff Department	军委联合参谋部	Junwei lianhe canmo bu
CMC Political Work Department	军委政治工作部	Junwei zhengzhi gongzuo bu
CMC Logistics Safeguarding Department	军委后勤保障部	Junwei houqin baozhang bu
CMC Equipment Development Department	军委装备发展部	Junwei zhuangbei fazhan bu
CMC Training Management Department	军委训练管理部	Junwei xunlian guanli bu
CMC National Defense Mobilization Department	军委国防动员部	Junwei guofang dongyuan bu
Commissions		
CMC Discipline Inspection Commission	军委记律检查委员会	Junwei jilu jiancha weiyuanhui
CMC Politics and Law Commission	军委政法委员会	Junwei zhengfa weiyuan hui
CMC Science and Technology Commission	军委科学技术委员会	Junwei kexue jishu weiyuan hui
Offices		
CMC Strategic Planning Office	军委战略规划办公室	Junwei zhanlue guihua bangongshi
CMC Reform and Organization Office	军委改革和编制办公室	Junwei gaige he bianzhi bangongshi
CMC International Military Cooperation Office	军委国际军事合作办公室	Junwei guoji junshi hezuo bangongshi
CMC Audit Office	军委审计署	Junwei shenji shu
CMC General Office for Administrative Affairs	军委机关事务管理总局	Junwei jiguan shiwu guanli zongju

they might differ from some of the departments. For example, what is the line separating the CMC Strategic Planning Office from the CMC Joint Staff Department, which also must engage in strategic planning?

Replacing the Military Districts

The third announcement, in February 2016, was the replacement of the seven military regions (*da junqu*; 大军区) with five "war zones" or "theater commands" (*zhan qu*; 战区): North, East, South, West, and Central.[49] The precise areas of responsibility for the new war zones have not been announced. It is believed that, where the military regions had largely followed the outlines of the provinces, the new war zone boundaries will be determined by likely areas of operations, beyond China's shores. It is not clear, though, as to whether the South China Sea will be part of the East or South war zone or whether the Korean Peninsula will be part of the East or North war zone.

The Central war zone's responsibilities are even less clear. It may be intended primarily as a reserve to support the other four war zone commands. However, it is also possible that it may be responsible for a differently oriented set of tasks. For example, it may be responsible for a broad range of deterrent missions, in which case it would have control over not only the PLARF but also the PLASSF.

What also remains unclear is the bureaucratic standing of certain key organizations that had been the equivalent of military regions. The commanders and political officers of the Academy of Military Sciences (AMS), the PLA's National Defense University (NDU), and the National University of Defense Technology (NUDT) have each been historically treated as the equivalent of a military region commander, reflecting their institutional importance.

The AMS, for example, is not only a top-level think tank and brain trust for the senior military leadership, but it also embodies aspects of the U.S. Army's Training and Doctrine Command (TRADOC), developing new doctrine for the entire PLA and corresponding training plans. It has also undertaken some roles comparable to the inspector general, assessing training activities. Whether it will cede these roles to the new CMC Training Management Department is unknown. More generally, it is unclear as to whether these institutions will be treated as the equivalent of a war zone—or if they, too, will be reorganized, perhaps into an entirely new format.

Chinese commentary makes clear that the command structure of the new war zone commands will be permanent, rather than ad hoc. In essence, the JCCH will now be a formal, regular part of the PLA's warfighting organizational structure. These JCCHs will likely be similarly organized across all the war zones. The final step of making joint operations the true, conceptual capstone of future Chinese military operations is effectively codified in this move.

Implications for the PLA's Ability to Secure Information Dominance

Any one of these groups of reforms would constitute a tectonic change in a military. The combination, however, constitutes nothing short of a fundamental reconsideration of how the PLA will operate. The overhaul disrupts traditional bureaucratic power lines (especially the ground forces' foremost role); challenges long-standing organizational precepts (the addition of GAD was the last previous change, in 1999); and, above all, reorients the PLA for "local wars under informationized conditions."

The restructuring of the PLA as outlined here, however, does not alter the PLA's missions and tasks. The "new historic missions" that have animated PLA planning since at least 2004, including the ability to secure dominance of the outer space, electromagnetic space, and maritime domains, remain in effect. Similarly, the imperative to conduct "political warfare," including the "three warfares" of public opinion warfare, legal warfare, and psychological warfare has not been rescinded, even as the General Political Department is renamed the CMC Political Work Department. Fighting and winning "local wars under informationized conditions," and securing information dominance as the means to that end, remains the foremost tasks for the PLA.

A primary motivation for this reorganization is arguably to upset the PLA's fundamental organization and procedures, which affect bureaucratic power and resource allocation, *in order to* better wage "local wars under informationized conditions." It is likely that the previous organization of the PLA had been assessed and found wanting in its ability to establish information dominance.

For example, assigning network and electronic warfare to first-level subordinate departments of the old GSD did not necessarily generate forces capable of conducting integrated operations on future battlefields. GSD units were organized apart from warfighting forces, making them harder to integrate in the field or incorporate into military region war plans. Concentrating them within the newly created PLASSF alongside space forces creates a service much more focused on waging information warfare. PLASSF units (especially INEW forces) will now more regularly operate alongside land, sea, air, and PLARF forces, improving coordination and joint training.

In this regard, the Chinese are pursuing a different path than the Russian military (which established the Russian Aerospace Force, combining the Russian air force, air defense troops, and space forces) or the United States (which has the service-oriented Air Force Space Command, the subunified command Cyber Command, and service-centered electronic warfare forces). In pursuit of information dominance, the PLA appears to have taken a much more far-reaching and radical step, concentrating its most elite information warfare forces.

Indeed, given the Chinese expectation that services will equip and train suitable forces (much like the American conception of service responsibilities), creating a single service with this range of capabilities is clearly intended to foster a holistic view of information warfare, cutting across domains (electromagnetic, computer network, outer space). This will affect future PLASSF doctrinal development, as it contemplates the interplay among these various forces, now sister branches. This, in turn, will also foster changes in training and eventually affect unit structures and numbers.

The major PLA reorganization also affects the warfighting organization of the new war zones. Although the previous military region system had emphasized joint operations, there was no permanent joint structure. The JCCH was a temporary entity, established in the event of crisis or war. Command relationships, both between units and personnel, were unmoored, formed on an ad hoc basis. This would inevitably affect information flow, which has a human as well as a technological element.

In the new structure formed in 2016, however, the new war zone commands are explicitly made joint and permanent. The renaming of the General Staff Department to the CMC Joint Staff Department further emphasizes how joint operations are now the norm for PLA planning and operations. Making the joint command structure permanent will foster relationships between various units of all services, as well as among various commanders. This will, in turn, facilitate information flow among all the various forces.

All of this hones the ability of the PLA to challenge future adversaries for information dominance. Once these reorganizations and changes have been fully implemented, the PLA will have a service specifically oriented toward information warfare, including electronic warfare, network warfare, space warfare, and command-and-control warfare. It will have a warfighting structure whose components are accustomed to operating in a joint manner. It will also have a C2 organization that will have developed standard operating procedures; tactics, techniques, and procedures; and more advanced doctrine and associated training standards.

8 Chapter

Chinese Views of Future Warfare and Implications for the United States

As of 2016, much like 2015 and 2014, much of the public's attention has been focused on China's activities in cyberspace. Hacking of U.S. government databases, such as the Office of Personnel Management (OPM), as well as various corporations has tended to dominate the American public's discourse on Chinese information activities. But understanding the reasons and strategy underlying China's actions is essential. One cannot formulate policy responses to counter activities without understanding the motivations that cause the activities in the first place.

HOW CHINA SEES INFORMATION AND FUTURE WARFARE

The most important element, as reflected in Chinese writings regarding informationized warfare, information warfare, and information operations, is that *the Chinese leadership sees information as inextricably linked to both the broader national interest and regime (or at least CCP) survival.* It is important to note here that this does not simply apply to the role of information in wartime. The Chinese leadership is not solely focused how information might be applied in a military conflict; rather, the leadership sees it as being a determinative factor in the ongoing competition among states writ large.

This, as Chinese writings emphasize, is because of the ascendant role of information in the 21st century's economic and political realities. This is the Information Age, and the ability to gather accurate information in a timely manner, transmit and analyze it, and then rapidly exploit it, is the key to success. These abilities are the centerpiece of any effort to achieve "information dominance"—the ability to gather, transmit, analyze, and exploit information

more rapidly and accurately in support of one's own ends, while denying an adversary the ability to do the same.

At the same time, however, the free flow of information constitutes a dire potential threat to CCP rule. While the Chinese Communist Party may no longer emphasize ideological arguments of "from each according to their ability, to each according to their needs," it remains firmly committed to its role as the "vanguard party" and, therefore, the sole legitimate political authority in the PRC. It also likely sees the collapse of the Soviet Union as a consequence of the failure to retain the "vanguard party" role and, as important, the liberalization of informational controls. The policies of *glasnost* and *perestroika*, of opening and reform, led to the downfall of the other major Communist Party. Just as information is the currency of economic and military power, it is also the basis for political power.

This "conundrum" (*maodun;* 矛盾), sets the stage for the second key conclusion. As an authoritarian party and with the fate of the Communist Party of the Soviet Union as an object lesson, the CCP cannot afford to allow the free flow of information. This would allow too many challenges to its rule. *The Chinese leadership therefore will seek to control the flow of information*.

To some extent, efforts at exerting this control are merely sustaining long-standing policies. The CCP has long demonstrated a willingness to employ extravagant lengths, such as the massive organizational infrastructure to support censorship, to limit that flow. However, because of the nature of the Information Age, including extensive interconnections and linkages across various information networks, the CCP cannot control the flow of information only *within* China. Instead, it must also control the flow of information *to* China.

This effort to control the external flow of information constitutes a fundamental, qualitative change in how nations approach information as a resource. Of course, states have long sought to shape and influence how they are portrayed. Nor is limiting access to outside information a new phenomenon. However, the Chinese efforts, in light of their views of the qualitative changes wrought by the rise of the Information Age, are different in scale and scope. Controlling information now means limiting not just newspapers and television programs, but the functioning of the Internet, on a global scale.

This elemental shift is replicated in how the PRC looks upon the international system, including the governance of the international common spaces. *If the Chinese are going to control and influence information flow to China, then it will have to shape and mold the international structures that manage that information flow*. This is not to suggest that China is about to overthrow the current system. Chinese writings regularly note that the PRC is still in the period of "strategic opportunity," which China needs to exploit, if it is to improve itself

and elevate itself to the ranks of middle-developed powers.[1] Thus, China must continue to pursue policies of peaceful development and interaction.

As China has grown steadily more powerful, though, it has increasingly questioned the underlying international structures that more and more often constrain its behavior. These structures, as Chinese writings note, were often formulated without input from the PRC. A reviving China, as well as a CCP intent on staying in power, increasingly chafes at these externally imposed limitations.

Nonetheless, challenging the current structure assumes greater urgency as *the PRC, and especially the CCP, also sees itself as increasingly in competition with the other major powers, especially the United States*. It is the United States that champions Internet freedom and, more broadly, the free flow of information. Moreover, as many Chinese officials have argued, it is American policies that encourage China's neighbors to challenge Chinese hegemony over its littoral waters or help sustain the Dalai Lama and other sources of internal instability.

This does not mean that the PRC believes that war or armed conflict is inevitable. Indeed, there is no reason to think that, in the short term (the next decade or so), that the PRC would actively engage in an armed attack on its neighbors. Unlike the Cold War, there is no "Fulda Gap" scenario to concentrate upon.

At the same time, the Chinese leadership is well aware of the utility of pursuing its ends through a variety of means, including "hybrid warfare." China has demonstrated an ability to employ fishing boats and civilian law enforcement vessels to pursue its territorial agenda. If Chinese warships are not shooting at foreign craft, Chinese fishing boats have had fewer compunctions about physically interfering with foreign vessels' operations. The world's information networks, where attributing actions are much harder, would seem to be the ideal environment for waging the kind of gray conflict typical of hybrid warfare.

Therefore, at the strategic level, the PRC will be constantly striving to shape both domestic and foreign views of itself through the information that it transmits and projects. Meanwhile, it will be trying to determine and dictate how others view China, as well as identifying their strengths and weaknesses. These efforts are no different than how every state behaves, in terms of collecting intelligence about potential allies and adversaries.

Where the PRC has begun to diverge from other states' practices, however, is their growing focus on dominating the information space in both peacetime and wartime. In particular, Chinese efforts to establish information dominance, while somewhat constrained in peacetime by the international system, are likely to be more comprehensive as well as much more pronounced in event of war.

This is reflected in Chinese military developments of the past several years, which are themselves *the culmination of nearly a quarter century of thought regarding the shape and requirements of future warfare*. The Chinese concept of "local wars under informationized conditions" reflects this ongoing evolution, with its focus on the role of information in all aspects of future warfare. This concept grows out of the lessons initially derived from observing the allied coalition in the first Gulf War of 1990–1991, leavened with observations from the Balkan wars of the 1990s and the American invasions of Afghanistan and Iraq. Thus, the PLA initially conceived of future wars as "local wars under modern, high-technology conditions," but then concluded that not all high technology was equally important.

With the conclusion that information technology is the foremost element of high technology, reflecting the larger strategic shift from the Industrial Age to the Information Age, the PLA has subsequently developed new doctrine, to link its concept of future wars to the kinds of forces it will field and the kinds of operations they will conduct. In the process, the PLA appears to again be refining its views.

From an initial focus on network warfare, electronic warfare, and psychological warfare, it is not apparently emphasizing command-and-control warfare and intelligence warfare. The implication would seem to be that not all networks, electronic systems, or leaders are equally important; instead, those in key decision-making roles, and the people and systems that inform their decisions, should be higher-priority targets. It is important to note here that this does not mean that the PLA will neglect other networks, systems, or personnel (e.g., logistics, combat units) in its pursuit of winning future informationized wars. Rather, it reflects priorities for allocating resources and developing capabilities.

This may be seen in the efforts of the last several years in fielding various types of new equipment and improved joint training. Alongside new fighters, warships, and self-propelled artillery are an array of new unmanned aerial vehicles, electronic warfare platforms, and sensors. The massive reorganization of late 2015 and early 2016 marks a major waypoint in this steady effort to prepare the PLA "to fight and win future local wars under informationized conditions."

HOW CHINESE CONCLUSIONS WILL SHAPE CHINESE ACTIONS

Given these Chinese conclusions, there are certain implications that arise, which are reflected in Chinese behavior.

Chinese actions must be holistic and will be comprehensive. The PRC still sees itself as a developing country. Despite being the second-largest GDP in

the world, this must be spread over a population of 1.3 billion. As important, China is not necessarily wealthy; while it has enormous untapped human and physical potential, until that is converted into actual capacity and capability, much of China will remain poor. In this light, the Chinese are likely to pursue more of a whole-of-government approach, if only to leverage its available resources. Thus, whereas the United States has both a military and a civilian space program (the latter divided into three substantial segments), China is unlikely to pursue such a strategy that demands extensive redundancy and overlap.

This will likely be reinforced by the high priority accorded to informationization in general. While various senior-level efforts have been halting at times, Xi Jinping has clearly made informationizing China a major policy focus. Insofar as the Chinese see their future inextricably embedded in the Information Age, these efforts will enjoy highest-level support, with efforts to reduce stove-piping and enhance cross-bureaucracy cooperation. This, in turn, will mean greater cooperation not only within the military but also between the military and the other national security bureaucracies, as well as with the larger range of Chinese ministries, and both public and private enterprises.

Chinese actions are determined by Chinese priorities and are unlikely to be heavily influenced by external pressure or blandishments. If the Chinese leadership sees information as integral to national survival and views economic espionage as part of the process of obtaining necessary information, then it will not be easily dissuaded. Similarly, insofar as the Chinese leadership links information flow with regime survival, Beijing will also restrict and channel information flow in ways that meet internal security requirements. To this end, the targets of Chinese actions will have to impose very high costs on Beijing, so that the gains are not worthwhile to the PRC, if they seek to alter the Chinese approach.

The difficulty of influencing Beijing is exacerbated by the Chinese leadership's sense that it is already in a strategic competition with various other states. The CCP perceives challenges to its security stemming not only from the United States but also from Russia, India, and Japan, as well as certain nonstate actors such as Uighur and Tibetan separatists. Indeed, it is essential to recognize that the Chinese leadership sees itself as already engaging in multilateral deterrence—a position it has adopted since at least the 1960s, when it believed it was facing threats from both the Soviet Union and the United States.

Chinese views about the extent of threats are further reinforced by the reality that the information space is both virtual and global; it is therefore not currently restricted by any national borders. For the Chinese leadership, controlling information flow and content therefore entails operating

not just within the Chinese portion of information space but globally. It requires accessing foreign information sources and influencing foreign decision makers, while preventing outside powers from being able to do the same in China.

As a result, *the PRC is undertaking an increasing array of actions beyond its own borders, striving to dominate what had previously been part of shared spaces*. This applies to not only information space, such as the Internet, but also physical domains such as the seas and outer space. Indeed, one can see parallels among Chinese efforts to dominate the South China Sea, its growing array of counterspace capabilities, and its efforts to control and dominate information space. In each case, the PRC is intent upon extending Chinese sovereignty, including its rules and its administrative prerogatives, over what had previously been open domains.

In this regard, Chinese actions are justified by a very different perspective on the functioning of national and international law. Indeed, Chinese views of legal warfare occur in the context of a historical and cultural view of the role of law that is very different from that in the West. At base, the Chinese subscribe to the concept of "rule-*by*-law," rather than the "rule-*of*-law." That is, the law serves as an instrument by which authority is exercised but does not constrain the exercise of authority.

In the broadest sense, pre-1911 Chinese society saw the law from an instrumental perspective, that is, a means by which authority could control the population but not a control extended over authority. Laws were secondary to the network of obligations enunciated under the Confucian ethic. The Legalist "school" of ancient China placed more emphasis on the creation of legal codes (versus the ethical codes preferred by the Confucians) but ultimately also saw the law as a means of enforcing societal and state control of the population. No strong tradition ever developed in China that saw the law as applying to the ruler as much as to the ruled.

During the early years of the PRC, Chinese legal development was influenced by the Marxist perspective that the "law should serve as an ideological instrument of politics."[2] Consequently, the CCP during the formative years of the PRC saw the law in the same terms as imperial China. The law served as essentially an instrument of governance but not a constraint upon the party, much less the Great Helmsman, Mao Zedong. In any case, the party exercised rule by decree, rather than through the provision of legal mechanisms. Mao himself, during the Cultural Revolution, effectively abolished both the judiciary and the legal structure.[3] Since Mao's passing, while there have been efforts at developing a body of laws, most have been in the area of commercial and contract law. Moreover, the law remains an instrument that applies primarily to the masses as opposed to the party, that is, the law exists to serve authority, not to constrain it.

This has meant that the Chinese government employs laws, treaties, and other legal instruments to achieve their ends, even when it flies in the face of traditional legal understanding or original intentions. Thus, the Chinese do not see their efforts to extend Chinese authority over shared spaces as inconsistent with international law but as part of political warfare; opposition to their efforts is similarly seen as an effort to contain China and to threaten CCP rule.

Consequently, Chinese efforts to dominate information space strive not only to control the flow of information but to delegitimize the idea of the information realm as a shared space, accessible to a variety of groups. Chinese authorities have striven to limit the role of nonstate players in setting the rules for the Internet. At the same time, it has also sought to limit the access of dissidents, Taiwan political authorities, Tibetan activists, and others who have tried to oppose China's position to not only Chinese audiences but global ones. Given the Chinese leadership's view of the existential threat posed by information (whether inside or outside China), such efforts are perceived as defensive efforts aimed at preserving the regime.

China is likely to pursue a form of informational isolationism. The Chinese solution to the challenge of information vulnerability is to restrict the flow of information. This is not intended to replicate the extreme North Korean form of isolation but to align information flows ideally "with Chinese characteristics." Indeed, Beijing strives to make itself informationally autarkic, wholly self-dependent in terms of information access, information generation, and information transmission. Thus, the PRC has created Chinese versions of information companies, is pursuing a homegrown semiconductor industry to substitute for imported computer components and otherwise tries to limit informational access to and from China.

This is an ironic rejection of the very macroeconomic policies of the past four decades that have allowed China to succeed and advance. But, just as the CCP accepts performance costs in the speed of the Chinese Internet (imposed by the nature of the Great Firewall of China), it accepts the economic and innovative opportunity costs that are imposed by the broader restrictions imposed on information flow. This is a dangerous bargain, however, as CCP leaders appear to be trading longer-term economic growth for short-term stability and curbing immediate challenges to their authority. If the Chinese leaders are correct that future development of "comprehensive national power" (CNP) is directly tied to the ability to exploit information, then their actions are likely, in the long run, to actually limit future CNP growth.

IMPLICATIONS FOR AMERICAN POLICY MAKERS

Given the Chinese conclusions regarding the impact of information on Chinese strategy and policy, American decision makers need to recognize

the extent to which the United States is already in competition with the PRC. This, in turn, has implications for a variety of American policies. Similarly, all those involved in the national security enterprise, not simply decision makers, need to recognize the range of efforts that the PRC is undertaking, and begin to move to counter them.

The United States and China Are Competing

The foremost consideration must be the recognition that the Chinese leadership sees itself in competition with the United States, and indeed with the rest of the world writ large, and arguably in a state of conflict. It is important to note that *competition* does not imply *war*. The PRC clearly does not operate as though it is in a state of armed conflict with the United States, nor with its neighbors. But it does see its relations with many of these states, including the United States and Japan, as fundamentally adversarial in nature. Restrictions on access to advanced technology, imposed in the wake of the Tiananmen Massacre in 1989, subsequent additional restrictions on transfers of space and other technology, limitations on Chinese ability to acquire various Western corporations, all are seen as denoting an unfriendly stance toward China.

There is a recognition among various key American decision makers that China is one of the foremost security competitors of the United States. The 1999 Cox Commission Report, the annual Worldwide Threat Assessment provided by the Office of the Director of National Intelligence, the annual DOD report to Congress on China, all make clear that China is increasingly challenging American security constructs in the western Pacific and globally. This involves Chinese development of an array of new capabilities not only in its armed forces but in the realm of information warfare capabilities.

Ironically, many of the concepts underlying these new capabilities appear to parallel American ones. Chinese descriptions of the need to establish information dominance correspond to American writings regarding the need to understand and exploit the information environment, especially as embodied in Joint Pub 3–13 "Information Operations."[4] In terms of military doctrinal writings, the two sides' uniformed services clearly share some common ground.

The United States and China Are Competing Orthogonally

The difference between the Chinese and American approaches to information warfare, despite certain similarities in doctrinal writings, typifies the larger, more fundamental chasm separating the two nations. In many ways, American leaders do not recognize how the two states are competing.

What is essential is understanding the extent to which Chinese and American concepts approach *informationized warfare* (rather than *information warfare*) from very different angles and starting points. The two sides are not so much *asymmetric* (implying a different approach to a problem from a common starting point), as *orthogonal* (implying a completely different set of starting points for the two parties). For example, publications from the Joint Chiefs of Staff, such as doctrinal statements regarding information operations or space operations, only apply to American military forces, operating under the restrictions imposed by American laws (e.g., the separation of military, Title 10, functions from intelligence, Title 50, functions). Chinese writings, by contrast, clearly encompass all national information resources, whether military, civilian, or nongovernmental.

Part of this difference is rooted in the fundamentally different historic circumstances that frame the contexts for Chinese and American decision makers. As noted earlier, East and West have radically different perspectives on the role and nature of law, whether it constrains authority or not. Similarly, the United States, for example, ultimately believes in the free flow of information. The Constitution and the rights enshrined therein essentially guarantee a minimum of governmental interference in the transmission of information, such as through freedom of the press, freedom of expression, and freedom of assembly. As important, there has long been a role for a robust civil society in the West's more liberal conception of the interplay between state and society. The very recognition that the two are discrete elements, distinct from each other, reflects this core concept.

By contrast, the CCP has clearly demonstrated that it is not prepared to countenance free and open expression of information. And the pervasive presence of party committees ensures that civil society develops in China only under party guidance and supervision. This view is not simply the product of the CCP's positions but is more deeply rooted in various aspects of Chinese culture and history, including the very different views regarding the role of the law.

For this reason, the Chinese should not be seen as pursuing an *asymmetric* approach, because "asymmetric" implies a different approach from a comparable starting point for roughly similar ends. Beijing's starting point is one that is fundamentally dissimilar, shaped by wholly different circumstances. It should not be surprising that this radically alternative contextual framework leads to constraints and objectives that are wildly divergent from our own—in short, *orthogonal*.

In this regard, it is not that the United States and China are necessarily pursuing *antagonistic* goals. Indeed, the two sides may at times find themselves in agreement on ends, means, or both. At other times, they will find themselves pursuing mutually unrelated objectives. But more and more often, the two

states will find themselves at odds, as the two states' interests intersect, albeit for different reasons.

Most fundamentally, the American interest in maintaining a free flow of information on a global scale, for philosophical, political, commercial, and military reasons, will constitute a challenge to the Chinese, and specifically the CCP's, vision of its interests. So long as the CCP sees regime survival as tantamount to national survival ("l'etat, c'est nous"), then such efforts will also be seen as jeopardizing the party's grip on power, even if that is not the motivation underlying American efforts.

The Competition Is All-Encompassing

For the same reason, the Chinese leadership sees the competition with the United States, and the larger liberal Western order, as all-encompassing. In the first place, the Chinese concern about raising their CNP requires that the PRC improve itself, not simply in military or economic terms but across the board. This will include elevating the level of sophistication of the economy, expanding its scientific and technological prowess, obtaining greater political unity, and securing more diplomatic respect. All of these aspects entail some degree of information operations, whether it is engaging in espionage, gathering intelligence, exerting influence, or preparing for military operations. Because of the emphasis on improving China's position during this period of "strategic opportunity," there is little likelihood of any abatement in various Chinese information activities, including economic and technological espionage or efforts at extending global influence.

Moreover, from Beijing's perspective, determining who controls the flow of information across the globe and who has access to that information is not only a fundamental national security issue but one touching on regime survival. The United States subscribes to the view that there are multiple legitimate stakeholders in determining who should have access. This is reflected in the American support for ICANN and its inclusive stance on who gets to participate in the rules-setting regime. The free flow of information does not affect the fundamental stability of the United States or its institutions.

For the Chinese leadership, allowing such a wide variety of groups to have unfettered access to the dissemination of information necessarily poses a fundamental threat. Information not only can affect China's future security but, more important, *will* affect the CCP's ability to retain power. In the first place, if this divergence is left unchecked, then there will be a proliferation of potential sources of information. This would make it virtually impossible for the PRC to limit its flow. As important, the greater the variety of players providing information, the more likely that it will include sources such as religious groups, separatists, and dissidents. That, in turn,

would begin to make such groups, and their messaging, appear legitimate to Chinese audiences and therefore pose a greater challenge to the CCP.

Therefore, the PRC wants to restrict access, ideally, to state-level players. Hence, its support for transferring administration of the Internet to entities such as the United Nations International Telecommunications Union (ITU). If successful, this would minimize the range of players while affording Beijing maximum leverage over each of them. China is more likely to successfully pressure states into denying groups Internet addresses and the like, by employing its economic strength. (This would be a case of asymmetric pressures.) By contrast, the greater the role for civil society organizations (NGOs, press entities, religious organizations), the harder it will be to suppress the introduction of unfriendly information.

This same persistence will mark Chinese military activities. There will, on the one hand, be a growing effort on the part of the Chinese military to obtain information about potential adversaries, including not only the United States but Taiwan, Japan, Vietnam, India, and also Russia. This will include not only technical information about weapons systems but information about organization and processes—how decisions are made, who staffs those decisions, what procedures are followed. All of this provides insights about both whom to target and when and with what types of capabilities. It might be determined that it would be more advantageous to defer attacking a target until it has become a single point of failure (e.g., attacking satellites after first damaging undersea cables which carry far more bandwidth). Or there may be circumstances where it is determined that it would be more useful to employ trusted agents to alter information, rather than employ hard-kill methods to destroy physical infrastructure. Much of this will depend upon peacetime gathering of information.

At the same time, there will likely be a growing effort to deny adversaries the ability to collect comparable information about their Chinese counterparts. American and other states' intelligence gathering operations are likely to be major targets for physical, technical, and political interference. The Chinese island-building activities in the South China Sea, for example, are likely to lead to the creation of an air defense identification zone that, in turn, will serve to exclude American reconnaissance aircraft from patrolling easily off China's shores. Similarly, the ability to engage in a variety of jamming and dazzling behavior against space systems will compel adversaries to consider carefully when (and whether) they will employ their satellites to observe the PRC. If gaps emerge in coverage, that, in turn, will afford Chinese military forces opportunities to engage in more effective denial and deception operations.

Given the Chinese leadership's efforts at integrating civilian and military capabilities and assets, these enhanced efforts at information reconnaissance and denial are likely to involve greater participation of various Chinese entities

that are not necessarily formally part of the military but that have been assigned supporting tasks and roles. This will likely make attribution even more difficult than it has been in the past. At the same time, the massive reorganization of the PLA is likely to similarly complicate attribution efforts, as past patterns (and therefore certain indicators) are disrupted as well.

The Competition Will Be Intensifying—and Militarizing

None of this means that Chinese efforts at establishing strategic information dominance in peacetime will be abating. Indeed, if the Chinese economy slows down, and if this leads to greater internal unrest, then the Chinese are likely to *intensify* their efforts to control the global information space. This will be in order to minimize the ability of outsiders to influence, exacerbate, or exploit the domestic discord. At the same time, they will also be even more restrictive on the Chinese domestic information scene, for the same reason—to limit the potential for more widespread dissent and disruption.

Unfortunately, this is also likely to mean an intensification of Chinese efforts to exclude foreign, and especially American, forces from the western Pacific littoral. Insofar as Chinese leaders believe that it is the American military that heartens local states in rejecting Chinese sovereignty claims (or even that the U.S. foments such efforts outright), limiting American freedom of action in the region will reduce that appeal. Moreover, denying American forces the ability to establish information dominance is an essential means of deterring, or coercing, Washington into acceding more to China's vision of the regional order.

The reorganization of the PLA will also likely lead to an intensification of Chinese military information gathering efforts, as various organizations determine their respective purviews. With an entire service (the PLASSF) oriented toward establishing information dominance through actions in the electromagnetic domain, network space, and outer space, that new organization will probably be as intensively engaged as its previous constituent elements (e.g., the various GSD Third Department entities). Similarly, the newly created permanent joint commands in charge of the various new war zones will undoubtedly also be trying to obtain information about their respective areas of responsibility.

POLICY OPTIONS FOR THE UNITED STATES: SOME DON'TS

For the United States, the PRC will constitute a major challenge but one that fundamentally differs from the Soviet Union. The PRC is not necessarily intent upon displacing the United States; indeed, Chinese leaders are insistent

that they are only interested in raising China to the level of middle-developed nation by the time the PRC celebrates its centennial in 2049. As important, given the orthogonal nature of the Chinese challenge, the Chinese challenge is likely to appear episodic, since what China wants not only is different from what we want but often does not overlap with (or interfere with) American interests.

This means that there will be as many opportunities for Sino-American cooperation as there will be confrontational situations. The vital interests of the two states will not necessarily only be in conflict; this will not be a zero-sum relationship. Indeed, insofar as the Chinese choose to remain committed to the global trading regime, which has helped facilitate the Chinese economic miracle of the past three decades, they should be welcomed.

Don't Make Concessions on the Principle of Free Information Flow

Unfortunately, the issue of information dominance, including the ability to establish the rules for information management, will be one of the fundamental areas where the two sides will be *unlikely* to reach agreement. The basic philosophical differences between the two systems, and the Chinese view of information as essential to regime survival, will likely represent fundamental contradictions between the two states that will increasingly animate conflicts of interest. Worse, because the CCP sees this as a matter of regime survival, it is likely to act assertively in this regard and offer little room for negotiations.

For the same reasons, however, this is not an area that the United States can afford to make major concessions. Not only is it central to the American fabric and ethos to allow and facilitate the free flow of information, but it is also vital to its economic and national security interests. Just as the fledgling American republic could not afford to cede freedom of the seas to foreign dictates as this would have strangled the nascent American economy, the modern American economy, and the associated global trading system, cannot survive if the PRC insists upon preventing the free flow of information that undergirds it. China can certainly strive to control the flow of information within China—what happens behind the Great Firewall of China can stay behind the GFWC. But once Chinese actions impinge upon other players, whether through cyber economic espionage, political and economic pressure to muzzle various parties, or efforts to rewrite the rules on Internet governance to extend sovereignty to shared informational spaces, then it becomes a matter of vital interest to the United States as well.

It is also important to recognize that, while China is one of the most important players, it is not the only one. Unlike the Cold War, American actions and decisions farther afield will impinge upon Chinese actions, in ways that

were not true when the global situation was largely determined by the bipolar United States–Soviet relationship. As with factors influencing the evolution of the PLA's views on future warfare, joint operations, and the rise of informationized warfare, it is inevitable that the Chinese will draw lessons from other people's efforts at information dominance, including computer network operations. These efforts are not limited to American wars (although they are likely to be foremost) but also Russian and other states' wartime experiences. Indeed, computer network attacks in Estonia, Georgia, and Ukraine are likely to have made Russian efforts a premier case study for Chinese thinking about how to conduct such attacks themselves, including how to mask attribution and exploit them for political leverage.

If Russian operations in Syria or Ukraine or the Caucasus are seen as effective, then the Chinese will strive to emulate the factors that led to those successes in their own activities in East Asia, the Indian Ocean, and Central Asia. Conversely, if the Russians are seen as failing, then China will likely draw lessons from that as well. Therefore, the United States needs a consistently robust response to all efforts to dominate or reduce the shared information spaces, not just those from the PRC. Any and all such attempts will be firmly opposed.

For all these reasons, the United States must reacclimate itself to the ideological, as well as power politics, element of the Sino-American competition. What Beijing ultimately is promoting is a balkanized global information environment, one where its rules (which will find support from other authoritarian governments such as Russia's) will be extended to more and more of the shared information spaces and where free flows of information will be increasingly constrained and constricted. The economic benefits that the more inclusive, more expansive American approach entails must be paired with an emphasis upon the political considerations—the dignity of the individual (as a source as well as a consumer of information).

Don't Underestimate the Difficulties of Keeping Information Secure

Although the United States invented the Internet, it has no monopoly on information creation or transmission or exploitation. Indeed, the United States is not an information *superpower*; instead, it is one among many information *major powers*. While it has enormous informational resources, whether in terms of information technology companies, software developers, or Internet users, it does not dominate all of the information domain the way the U.S. Navy still outweighs any single other naval force.

The Internet is a prime example of the difficulties involved. The computer network attacks in Ukraine and Estonia are a reminder that the global

information threat environment is increasing in intensity and complexity. The reality is that it is likely to be impossible to create a secure global information space.

As many of the earlier Internet pioneers have observed, the system they created was never designed to be secure, any more than it had been designed to handle the scale of use. The nature of software vulnerabilities only further exacerbate this. Closing vulnerabilities is not something that can be done overnight, even after they are detected.

> The sad reality is that the average zero day threat goes undetected for almost a year. Only once captured by anti-malware researchers and decompiled can this new vector of cyber attack be examined and the true nature of the cyber threat analyzed and evaluated. Then the company needs to write a fix or a "patch" for the security vulnerability, issue it, or distribute updated software. This could take weeks, or even months, just to issue the software upgrade.
>
> Then there is the patch problem. It takes around 21 days to upgrade and patch 50 per cent of corporate *servers* but it takes 62 days to patch 50 per cent of corporate desktop *computers*. Of course, some are never patched at all. Home computer users are even worse: it is estimated that over 40 per cent of the current computers attached to the Internet are at risk—simply because users never download and install current computer upgrades.[5]

Similar problems exist in trying to secure hardware. Although some have suggested inspecting at least samples of chips and computers that enter the United States from China, not only would this be a challenge in terms of scale (in 2014 the United States imported some $22 billion in semiconductors and other computer components from China alone), but it is not even clear that we would know what the inspections were supposed to find.[6] It's one thing to test a chip to see if it contains a known virus or piece of malware. However, as the comment about software vulnerability notes, it can take a year to find a zero-day exploit in a program. If there was deliberately concealed malware on a chip, finding it would be even more difficult and time consuming. What happens in the meantime?

Don't Ignore Inherent Chinese Advantages in Establishing Information Dominance

The Chinese effort to become informationally isolationist complements other Chinese advantages, especially in the military sense. The PLA enjoys certain asymmetric geographic advantages, simply because of physical realities. To

begin with, for the foreseeable future, the PLA will remain focused primarily on defending the PRC. While it is extending its reach, the focus through the first half of the 2020s is likely to be on the area within the first island chain, stretching from Japan in the north, through Okinawa, Taiwan, and the Philippines, to the Straits of Malacca.

This, in turn, leads to asymmetric informational advantages. In the area between the first island chain and the Chinese mainland, the PLA will have sufficient overlapping networks of sensors, communications, and so on, to establish and maintain situational awareness, even in the face of concentrated attacks.

Many of these networks, moreover, will be relatively more secure. The Chinese, for example, can rely upon line-of-sight radio (difficult to intercept) and fiber-optic landlines (difficult to tap), in addition to microwave, satellite, and other communications systems. They can mobilize their substantial fishing fleet and merchant fleet to provide additional eyes and radars to supplement their naval and coast guard forces for maritime domain awareness. They can, and are, building new islands on which they can build radars, sonar stations, and airfields from which they can deploy aircraft and helicopters.

By contrast, American forces that seek to deploy to the region will, in essence, have to bring their communications and sensors with them. Whereas China has an array of redundant sensors and communications, the United States is far more dependent upon satellites for finding and identifying targets, coordinating forces, and battle damage assessment. If China were to cut key undersea cables, which carry a vast proportion of global bandwidth, the impact would be disproportionately greater on American military forces than the PLA. This also applies more broadly. Insofar as the Chinese military is able to monitor and control the flow of information across various networks, it will be in a better position to establish information dominance, because its internal networks are more robust, redundant, and protected.

This has both strategic and operational impact. If the PLA can achieve information dominance, it will allow the Chinese leadership, both military and civilian, to better create a psychological advantage, not only against the United States but also against local states. This, in turn, will help them effect deterrent and coercive strategies which will allow them to achieve their political ends—the main focus of their policies.

Don't Ignore Inherent Chinese Weaknesses in Establishing Information Dominance

But while the PLA enjoys certain advantages in terms of the struggle for information dominance, the PRC, writ large, suffers from major weaknesses. Some are ironically due to Chinese misbehavior and lack of respect

for international norms. It is estimated that over 200 million Chinese computers still run the old Windows XP operating system.[7] Three-quarters of Windows users in China, meanwhile, are believed to be running pirated editions of that software.[8] It is likely that many, perhaps most, never receive security updates, since they are unregistered. This means that many zero-day exploits that were closed elsewhere potentially remain open (and therefore exploitable) in China.

Nor are China's weaknesses solely in terms of information technology. The Beijing leadership must divide its attention between internal and external threats, to a far greater extent than does Washington. The CCP's focus on constricting the flow of information suggests that, from a national security perspective, the Chinese perceive their greatest weakness as involving internal unrest. This is also reflected in the prompt crackdowns on any social media messaging calling for action outside party channels, even if the action nominally supports the CCP. This situation is likely to be exacerbated, if the economic slowdown already apparent in 2016 lasts for any period of time. A Chinese population that is suffering from increased unemployment, and whose rising expectations are not met, is one that is also likely to be more restive. Increased repression, and further constraints on internal information flows, will only complicate the maintenance of control.

The potential for internal instability is likely to stoke demand for more resources. For several years, until 2014 when the Chinese stopped reporting data, the internal security budget (combining national- and provincial-level spending) was rising faster than the external security budget (primarily money spent on the PLA). Indeed, official figures indicated that spending on internal security (including the People's Armed Police and the Ministry of Public Security) actually exceeded that on the armed forces.[9] Since then, only the central government figures have been provided. Even those figures, however, suggest that internal security spending continues to rise rapidly. In 2015, the Chinese raised their public security spending by 7.2 percent and by a further 5.3 percent in 2016.[10] Further expanding China's already extensive array of internal security forces, including censors, would entail further increases in internal security spending.

This, in turn, may intensify one of China's most pervasive problems, that of organizational stovepipes. The history of the Chinese bureaucratic state is one that spans millennia. Overcoming bureaucratic interests and encouraging information flow is implicitly encouraged in many Chinese writings; indeed, improved information flow is seen as both a cause and effect of reducing barriers between military services and branches, as well as those within the government among various ministries. It is unclear whether there is competition for resources between the internal and external security services, or between the security and nonsecurity ministries. However, if China's economy continues

to slow down, the Chinese leadership will eventually have to confront the issue of resource allocation, that is, guns versus butter.

Indeed, the massive military reorganization is clearly intended, in part, to break down the barriers among the Chinese services, between the various departments comprising the Central Military Commission and among the various commands within the former military regions (now reorganized into war zone commands with permanent, standing joint headquarters). This suggests that there is a clear awareness of the need to overcome these internal obstacles to information flow, at least within the uniformed military.

This effort will likely take many years, perhaps as much as a decade, if only because of the constantly evolving nature of technology and global society. Indeed, the steady metamorphosis of the PLA, in terms of doctrine as well as organization, as well as the myriad Chinese organizations that have arisen to handle informationization, suggests that the Chinese authorities are not necessarily hidebound or rigid in their approach but recognize the need to accommodate that evolution. In the interim, however, the PLA is going to be even more vulnerable, as it adjusts its organizations and further modifies its doctrine. This suggests that, if military concerns are paramount, the next decade may see the CCP leadership proceed more carefully, relying more on pressure and threats while refraining from overt use of the still evolving military.

POLICY OPTIONS FOR THE UNITED STATES: SOME DO'S

For American decision makers, because of the fundamentally different, orthogonal views that animate Washington and Beijing, the least viable option is to emulate the PRC. An approach that involves restricting the flow of information to the broader population, the muzzling of civil society, and efforts to restrict shared information space would only weaken the United States and other Western democracies. Therefore, rather than restricting the flow of information, the United States needs an alternative paradigm (which also is consistent with the orthogonal nature of the competition).

Arguably, for the United States, the focus should be on preventing the PRC from being able to establish information dominance. This entails, on the one hand, assuring that the United States will be able to effectively collect, transmit, and exploit information in a timely fashion, whatever Chinese actions are undertaken. At the same time, holding at risk certain Chinese information systems, networks, and decision-making processes, such that the Chinese leadership cannot expect to achieve their larger political goals, is essential. Here, it is vital to note that the center of gravity is on the political issues that might precipitate a conflict (e.g., South China Sea, Senkaku

Islands, Taiwan). The American focus should therefore not be on engaging in information warfare but on denying China political success. Denying the Chinese the ability to achieve information dominance matters, only insofar as it frustrates their ability to achieve their political goals.

Do Give Greater Consideration to the Demands of Deterrence

Too often, there is an assumption that an equivalent Western ability to hold Chinese systems at risk will serve to deter. For example, it is sometimes presumed that, if China is creating a robust counterspace capability, then the United States needs to develop a comparable set of capabilities. Even more problematically, it is sometimes assumed that such a symmetric capability would serve to deter Chinese activities.

Deterrence, however, only works where one holds what the other side values at risk. This requires, first, identifying what the other side values. It is not at all clear that the ability, for example, to counter Chinese satellite communications would necessarily affect Beijing greatly, especially given the asymmetric geographic conditions and likely political objectives. This also begs the question of whether one can actually hold the adversary's overall set of systems and capabilities at risk. It may be that being able to threaten Chinese communications networks would deter Chinese action; given the proliferation and redundancy of such systems, however, it is not clear that this objective can be achieved at reasonable cost.

In the case of the CCP, it would seem that the Chinese clearly value the ability to gather information about adversary networks, about decision makers, about decision-making processes, in both peacetime and wartime. The ability to disrupt Chinese peacetime information gathering, denying them information about adversary capabilities and procedures, would therefore likely hold at risk Chinese assumptions of the ability to establish information dominance.

Such efforts would prove especially disruptive, due to the nature of many offensive information operations. As with solving zero-day exploits, the ability to implement information warfare on any given X-Day (the initiation of hostilities) requires an extensive array of steps that must be undertaken days, weeks, months, and even years prior to X-Day. Not only is extensive prior intelligence gathering in peacetime is necessary but for many types of information warfare activities (including network and electronic warfare), weapons and capabilities must also be created and implanted far in advance. This makes information warfare much less flexible and responsive than often suggested in popular entertainment, even as it makes it also potentially more devastating (since it might be employed against systems long thought secure). Denying

China intelligence about key electronic systems, networks, decision-making processes, or altering them on a regular basis would raise the likelihood that weapons and tactics would not be ready in time of conflict. Worse, they may be inappropriate to the actual capabilities that are fielded.

At the same time, the CCP clearly is worried about the ability to maintain internal stability. This concern is true even in peacetime; in event of conflict, these worries are likely to be heightened. Therefore, if the American Achilles' Heel is its dependence upon a comprehensive information network to allow expeditionary operations, China's weakness lies in its leadership's concern about facing internal opposition even as it is fighting foreign adversaries. If the United States is to successfully deter the PRC, it is this fear of loss of internal control that it must be prepared to exploit.

For the CCP, then, the loss of the ability to monitor China's population, damage to the various information networks that support censorship of traditional media, monitor social media, and limit access to the outside world, would be as devastating as the American inability to detect missile launches or guide JDAMs. Indeed, degradation of such systems might be more devastating, because unlike their American counterparts, China's leadership sees the PRC as surrounded by enemies. Even a successful Chinese conflict with the United States over, for example, Taiwan, would not affect the threat potentially posed by Russia or India, or Uighur or Tibetan separatists. A victory over the United States that left internal and external security information systems crippled or even badly damaged might well be viewed as Pyrrhic, since the available resources to sustain deterrence against remaining external threats, and internal challenges, would be severely weakened.

Do Promote Broader "Whole-of-Society" Participation

One element of the American efforts needs to be enhancing the inclusive nature of our approaches. It is essential that American leaders bridge both the civil–military divide and the government–private sector divide. The Chinese approach is one of "whole of government," under the direction of the CCP. In a system where the role of civil society and the private sector is minimized and tightly channeled, that is sufficient.

For the United States, there must be not only a "whole-of-government" approach but also a "whole-of-society" approach. The entire government, both military and civilian portions, represents only a fraction of the larger information capacity and potential of the United States. Much of the most important information, including not only patents and formulas but often even military and intelligence information, resides within the private sector (e.g., government contractors). Vulnerabilities in the private sector affect the public sector and vice versa. But no corporation is likely to be able to defend

itself against concerted, state-backed information attack efforts. Greater collaboration will be necessary, not only in order to successfully defend information frontiers but in order to leverage the vast pool of American, and global, expertise.

Some measures are already under way. The Obama administration, for example, opened the door to greater commercial roles in space operations. The result has been a variety of new players, some of whom made their fortunes in the information technology sector. Elon Musk's SpaceX, Jeff Bezos' Blue Origin, Sir Richard Branson's Virgin Galactic, and Robert Bigelow's Bigelow Aerospace are merely some of the best-known examples of the effort to go beyond the traditional aerospace suppliers.

Just as important has been the growth of various competitions, such as the Ansari X-Prize, which offer both financial incentives and prominence. Tapping into the broader range of public interest, including such measures, is a more bottom-up approach that arguably is more capable of promoting innovation and finding solutions than the more centrally directed, top-down approach that Beijing envisions. It is also an approach that is arguably better suited to the American and Western perspective.

Do Promote Resiliency and Diversification

Such approaches aimed at defeating active attacks would be complemented by shifting the focus to being able to ensure the continued flow of information, what some might term "resiliency." By denying the PRC the ability to achieve information dominance, through the continued ability to operate even in the face of information denial and interference efforts, the United States would be demonstrating that even successful attacks would not be decisive. If Chinese leaders cannot reasonably assume the ability to establish information dominance for a reasonable length of time, then they equally cannot reasonably assume a chance of victory in event of conflict.

This is not to suggest that antimalware, patches, or other current security measures should be abandoned; rather, it is to recognize that they are insufficient. If it is impossible to defend against attacks, then palliative and ameliorating measures must be incorporated into planning. The more that information systems lack redundancy and alternatives, the more lucrative they are as a target set; conversely, the more diverse the information networks, the fewer single points of failure, the more potential adversaries will look for other target sets.

Unfortunately, governmental budgetary considerations tend to downplay the importance of resilience, which is often associated with redundancy and therefore inefficiency. Such considerations have been rife in the aerospace realm. With the widespread utility of GPS, for example, emphasis

on alternative means of navigation have fallen by the wayside. The decision to cease support for the LORAN navigation system, a series of fixed, ground-based radio beacons that for decades provided navigational information, was driven in no small part by the feeling that it was unnecessary in the era of GPS.[11] Similarly, the Navy's decision to cease teaching the use of sextant in 2006 (reversed in 2015) was based on the idea that it was an obsolete skill, given the availability of satellite navigation systems.[12] In both cases, little consideration was given to what might happen if GPS systems were to fail, be jammed, or otherwise made unavailable.

Do Keep Calm and Carry On

Finally, American defense planners need to better assess just what damage might occur in the event of an all-out information warfare effort. On the one hand, this would entail attacks employing far more than just computer network operations. It could include strikes against space systems, crippling of infrastructure networks (e.g., transportation, energy, communications), elimination of key databases and computer records. These would, in turn, generate second- and third-order effects. But such a massive attack would also generate repercussions in third-party economies, infrastructure, and information networks. Chinese writings caution that use of kinetic antisatellite systems must include assessments of the impact of debris on third parties. This does not eliminate the chance of their use but suggests a careful application of such systems, rather than a "shoot-out at the OK Space Corral." Similarly, shutting down the American stock exchange systems and deleting the records would generate global financial effects, which would, in turn, have diplomatic and political impact on the PRC.

If there is no way to defend the entirety of information systems and operations, there are nonetheless ways to ameliorate the impact of adversary attacks. If there is no way to economically create a secure Internet, undertaking some steps to ensure that at least basic information services can continue to operate or that they can be restored in relatively short order (days or weeks) would remove much of the sting, while enhancing deterrence. Prioritizing key networks, and taking steps to improve their security, would help impose intellectual discipline. By expanding the range of consulted parties, tapping additional expertise, and creating more resilient systems, the scale of threat cannot be eliminated but can be made more manageable.

This page intentionally left blank

Notes

In order to limit confusion, Chinese authors have been listed with their surname in all-capital letters (e.g., CHANG Xianqi).

CHAPTER 1

1. TAN Wenfang, "The Impact of Information Technology on Modern Psychological Warfare," *National Defense Science and Technology* (#5, 2009), p. 72.

2. State Council Information Office, Tenth Five Year Plan for National Economic and Social Development, Informationization Key Point Special Plans (October 18, 2002), http://www.cia.org.cn/information/information_01_xxhgh_3.htm.

3. ZHENG Weiping and LIU Minfu, *Discussions on the Military's New Historic Missions* (Beijing, PRC: People's Armed Police Publishing House, 2005), p. 138.

4. For further discussion of the creation of Plan 863, see Evan Feigenbaum, *China's Techno-Warriors* (Stanford: Stanford University Press, 2003), pp. 141–143.

5. Ibid., pp. 175, 181.

6. Greg Austin, *Cyber Policy in China* (Malden, MA: Polity, 2014), p. 33.

7. Alice Miller, "More Already on the Central Committee's Leading Small Groups," *China Leadership Monitor* (#44, Summer 2014), http://www.hoover.org/sites/default/files/research/docs/clm44am.pdf.

8. ZHOU Wang, *Research on China's "Leading Small Groups"* (Tianjin, PRC: Tianjin People's Publishing House, 2010), pp. 44–51.

9. Christine Zhen-wei QIANG, *China's Information Revolution* (Washington, DC: World Bank, 2007), p. 93; and GUO Liang, *Under the Golden "Shine": China's Effort to Bridge Government and Citizens* (Beijing, PRC: Chinese Academy of Social Sciences, January 2006), pp. 4–6, http://unpan1.un.org/intradoc/groups/public/documents/undpadm/unpan042815.pdf.

10. WANG Yukai, "Wang Yukai: Central Network Security and Informationization Leading Small Group's Origins and Impact," *Renminwang* (March 3, 2014), http://theory.people.com.cn/n/2014/0303/c40531-24510897.html.

11. Ibid.

12. Ibid.

13. JIANG Zemin, Work Report to the 16th Party Congress, *Xinhua* (November 17, 2002), http://www.china.org.cn/english/features/49007.htm.

14. Austin, *Cyber Policy in China*, p. 91.

15. Ibid., p. 68.

16. Internet World Stats, "China: Internet Usage Stats and Population Report," 2010 www.internetworldstats.com/asia/cn.htm.

17. China Internet Network Information Center, *Statistical Report on Internet Development in China* (January 2014).

18. Ibid.

19. Reporters without Borders, *2015 World Press Freedom Index*, http://index.rsf.org/#!/.

20. Qiang GANG and David Bandurski, "China's Emerging Public Sphere: The Impact of Media Commercialization, Professionalism, and the Internet in an Era of Transition," in *Changing Media, Changing China*, ed. by Susan L. Shirk (New York: Oxford University Press, 2011), p. 41.

21. Susan Shirk, "Changing Media, Changing China," in *Changing Media, Changing China*, ed. by Susan L. Shirk (New York: Oxford University Press, 2011), p. 9.

22. Daniela Stockmann, "What Kind of Information Does the Public Demand? Getting the News During the 2005 Anti-Japanese Protests," in *Changing Media, Changing China*, ed. by Susan L. Shirk (New York: Oxford University Press, 2011), p. 180.

23. Ibid.

24. Miao DI, "Between Propaganda and Commercials: Chinese Television Today," in *Changing Media, Changing China*, ed. by Susan L. Shirk (New York: Oxford University Press, 2011), p. 98. For further discussion of the key organs for Chinese censorship, see "Agencies Responsible for Censorship in China," Congressional-Executive Commission on China, http://www.cecc.gov/agencies-responsible-for-censorship-in-china.

25. Richard McGregor, *The Party: The Secret World of China's Communist Rulers* (New York: Harper Collins Publishing, 2010), pp. 248–249. Examples of some of these directives may be found at *China Digital Times,* http://chinadigitaltimes.net/china/directives-from-the-ministry-of-truth/.

26. Chris Buckley, "China Train Crash Censorship Scorned on Internet," *Reuters* (August 1, 2011), http://www.reuters.com/article/2011/08/01/us-china-train-censorship-idUSTRE7700ET20110801; and "A Letter to Yiyi: Chinese Newspaper's Defiant Commentary on Train Collision," *Wall Street Journal* (July 31, 2011), http://blogs.wsj.com/chinarealtime/2011/07/31/a-letter-to-yiyi-chinese-newspapers-defiant-commentary-on-train-collision/.

27. Ben Blanchard, "China's Effort to Muzzle News of Train Crash Sparks Outcry," *Reuters* (July 25, 2011), http://www.reuters.com/article/2011/07/25/us-china-train-censorship-idUSTRE76O1IG20110725.

28. Zoe Murphy, "China Struggles to Censor Train Crash Coverage," BBC News (July 28, 2011), http://www.bbc.com/news/world-asia-pacific-14321787.

29. For a fuller discussion and examples of the level of censorship in the Wenzhou case, see David Bandurski, "Chinese Media Muzzled after Day of Glory," China Media Project (July 31, 2011), http://cmp.hku.hk/2011/07/31/14332/.

30. http://chinadigitaltimes.net/2013/01/ministry-of-truth-southern-weekend-new-year-piece/.

31. http://chinadigitaltimes.net/2013/01/ministry-of-truth-southern-weekly-tempest/.

32. http://chinadigitaltimes.net/2013/01/ministry-of-truth-urgent-notice-on-southern-weekly/.

33. Joseph Kahn, "China Shuts down Influential Weekly Newspaper in Crackdown on Media," *New York Times* (January 25, 2006), http://www.nytimes.com/2006/01/25/international/asia/25china.html.

34. Beina XU, "Media Censorship in China," Council on Foreign Relations (September 25, 2014), http://www.cfr.org/china/media-censorship-china/p11515.

35. Foreign Correspondents Club of China, *Position Paper on Working Conditions for Foreign Correspondents in China*, September 12, 2014, http://www.fccchina.org/2014/09/12/fccc-position-paper-2014/.

36. Angela Kockritz, "They Have Miao," *Die Zeit* (January 14, 2015), http://www.zeit.de/feature/freedom-of-press-china-zhang-miao-imprisonment.

37. Foreign Correspondents Club of China, *Position Paper on Working Conditions*.

38. Erik Wemple, "Chinese Leader Xi Jinping Blames Western News Outlets for Visa Problems in China," *Washington Post* (November 12, 2014), https://www.washingtonpost.com/blogs/erik-wemple/wp/2014/11/12/chinese-president-xi-jinping-blames-news-outlets-for-visa-problems-in-china/.

39. Andrew Jacobs, "For Foreign Journalists in Beijing, It's All about Asking the Right Question," *New York Times* (March 13, 2014), http://sinosphere.blogs.nytimes.com/2014/03/13/for-foreign-journalists-in-beijing-its-all-about-asking-the-right-question/.

40. Nicole Perlroth, "Hackers in China Attacked the Times for Last Four Months," *New York Times* (January 30, 2013), http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html; and Nicole Perlroth, "*Wall Street Journal* Announces That It, Too, Was Hacked by the Chinese," *New York Times* (January 31, 2013), http://www.nytimes.com/2013/02/01/technology/wall-street-journal-reports-attack-by-china-hackers.html.

CHAPTER 2

1. International Institute for Strategic Studies, *The Military Balance 2016* (London, UK: Routledge, 2016), pp. 240–249.

2. Edward O'Dowd, *Chinese Military Strategy in the Third Indochina War: The Last Maoist War* (New York: Routledge, 2007), pp. 153–154.

3. DENG Xiaoping, "Peace and Development Are the Two Outstanding Issues in the World Today," Remarks to a visiting delegation of the Japanese Chamber of Commerce and Industry (March 4, 1985), http://en.people.cn/dengxp/vol3/text/c1330.html.

4. State Council Information Office, *China's National Defense in 2006* (Beijing, PRC: State Council Information Office, 2006), http://fas.org/nuke/guide/china/doctrine/wp2006.html; and John F. Burns, "China Plans More Manpower Cuts in the Military," *New York Times* (January 4, 1985), http://www.nytimes.com/1985/01/04/world/china-plans-more-manpower-cuts-in-the-military.html.

5. James C. Mulvenon, *Soldiers of Fortune* (Armonk, NY: M.E. Sharpe Publishers, 2001), p. 53.

6. Testimony of Andrew D. Marble to the U.S. China Economic and Security Review Commission, Washington, DC, December 7, 2001.

7. Taylor Frayvel, *Strong Borders, Secure Nation* (Princeton: Princeton University Press, 2008).

8. Major General WANG Baocun, "China and the Revolution in Military Affairs, Part 1" *China Military Science* (#4, 2001), p. 151.

9. Ibid.

10. Colonel ZHOU Xiaopeng, "On the Development of Joint Operations Theory," *China Military Science* (May 1996), in FBIS-CHI (May 1996).

11. Lieutenant Colonel WU Jianchu, "Joint Operations—the Basic Form of Combat on High-Tech Terms," *China Military Science* (#4, 1995), in FBIS-CHI (April 1996).

12. SHI Yukun, "Lt. Gen. Li Jijun Answers Questions on Nuclear Deterrence, Nation-State; and Information Age," *China Military Science* (#3, 1995), in FBIS-CHI (August 1995).

13. Patrick J. Garrity, *Why the Gulf War Still Matters*, Report #16 (Los Alamos, NM: Center for National Security Studies, Los Alamos National Laboratory, 1993), p. 77, http://www.osti.gov/scitech/servlets/purl/10178236; and Defense Intelligence Agency, Intelligence Information Report, *PLA Modernizes Its Military Training Program* (June 23, 1995), http://nsarchive.gwu.edu/NSAEBB/NSAEBB39/document13.pdf.

14. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide* (Beijing, PRC: Military Science Publishing House, November 2005), p. 399.

15. Ibid., p. 400; and DONG Chongmin, *Research on Non-Linear Operations* (Beijing, PRC: Liberation Army Publishing House, 2005), pp. 50–57.

16. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, pp. 400–401.

17. David Finkelstein, "China's National Military Strategy," in *The People's Liberation Army in the Information Age*, ed. by James Mulvenon and Andrew Yang (Santa Monica, CA: RAND Corporation, 1999), p. 136.

18. Chinese Military Encyclopedia Committee, *Chinese Military Encyclopedia*, Vol. II (Beijing, PRC: Military Science Publishing House, July 1997), pp. 126–127.

19. Chinese writings invoke the Yijiangshan campaign of 1955, which involved the seizure of some islands from nationalist forces, as China's experience with joint operations. For a brief history of the campaign, see Xiaobing LI, "PLA Attacks and Amphibious Operations during the Taiwan Strait Crises of 1954–55 and 1958," in *Chinese Warfighting: The PLA Experience Since 1949,* ed. by Mark A. Ryan, David M. Finkelstein and Michael A. McDevitt (Armonk, NY: M.E. Sharpe, 2003), pp. 154–156; and Chinese Military Encyclopedia Committee, *Chinese Military Encyclopedia, Military History* Vol. IX (Beijing, PRC: Military Science Publishing House, July 1997), pp. 1370–1371.

20. GAO Yubiao, Chief Editor, *Joint Campaign Course Materials* (Beijing, PRC: Military Science Publishing House, August 2001), p. 8.

21. LI Yinnian, DONG Aiguo, and HU Haijun, "The Status and Future of Joint Tactics," *China Military Science* (#3, 2001), p. 98; and ZHOU Xiaoyu, PENG Xiwen,

and AN Weiping, *New Discussions on Joint Campaigns* (Beijing: National Defense University Publishing House, January 2000), pp. 21–22.

22. Lieutenant Colonel WU Jianchu, "Joint Operations—The Basic Form of Combat on High-Tech Terms," *China Military Science* (#4, 1995), in FBIS-CHI (April 1996).

23. Zhou et al., *New Discussions on Joint Campaigns*, p. 222.

24. Gao, *Joint Campaign Course Materials*, p. 49.

25. KE Jinjun and CHEN Bojiang, *Air-Land Coordinated Combat Concepts* (Beijing: People's Liberation Army Publishing House, 1996), p. 1.

26. Gao, *Joint Campaign Course Materials*, p. 51.

27. Ibid., p. 44.

28. James Mulvenon, *Soldiers of Fortune* (Armonk, NY: M.E. Sharpe Publishers, 2001), pp. 176–179.

29. Ibid., p. 186.

30. AMS Strategies and Campaigns Department, "New Developments in Campaign Theory," *Military Art* (#4, 1999), p. 17.

31. Kenneth Allen and Maryanne Kivlehan-Wise, "Implementing the Second Artillery's Doctrinal Reforms," in *China's Revolution in Doctrinal Affairs*, ed. by James Mulvenon and David Finkelstein (Alexandria, VA: Center for Naval Analysis, 2005), pp. 171, 175.

32. WANG Houqing and ZHANG Xingye, Chief Editors, *The Science of Campaigns* (Beijing: National Defense University Publishing House, May 2000), p. 124.

33. It should be noted that, in some cases, an exception is made for special cases where the participating forces are less than *juntuan* level. However, the overall strength must still total a *juntuan*-level force. Chinese People's Liberation Army Academy of Military Science, *Military Terminology* (Beijing, PRC: Military Science Publishing House, 1997), pp. 75–76; Wang and Zhang, *Science of Campaigns*, p. 385; and Gao, *Joint Campaign Course Materials*, p. 27.

34. ZHANG Xingye, "The Important Aspects of the Conduct of Joint Campaigns," *China Military Science* (#2, 2001), p. 92.

35. Major General DAI Qingmin, "Innovating and Developing Views on Information Operations," *China Military Science* (#8, 2000), pp. 72–77, in FBIS-CHI.

36. YING Desong, "Information Warfare: A Main Pillar of Joint Combat," *People's Liberation Army Daily* (September 11, 2001).

37. ZHANG Ming, "Discussing 'Air Dominance' and 'Network and Electromagnetic Spectrum' Dominance," *People's Liberation Army Daily* (October 29, 2002).

38. Major General DAI Qingmin, "On Integrating Network Warfare and Electronic Warfare," *China Military Science* (#2, 2002), pp. 112–117, in FBIS-CHI.

39. Zhang, "The Important Aspects of the Conduct of Joint Campaigns," p. 89.

40. Finkelstein, "China's National Military Strategy," p. 96.

41. HU Jintao, "See Clearly Our Military's Historic Missions in the New Period of the New Century" (December 24, 2004), http://gfjy.jxnews.com.cn/system/2010/04/16/011353408.shtml. For further discussion of the "new historic missions," see Daniel Hartnett, *Towards a Globally Focused Chinese Military: The Historic Missions of the Chinese Armed Forces* (Alexandria, VA: CNA Corporation, 2008).

42. HU Jintao, "Understanding Our Military's New Historic Missions in the New Phase of the New Century" (December 24, 2004), http//gfjy.jxnews.com.cn/system/2010/04/16/011353408.shtml.

CHAPTER 3

1. CHANG Long, "Tightly Grasping the Tends of the New Military Transformation—Reflections and Outlook from the Gulf War to the Iraq War," *PLA Daily* (October 28, 2003), http://www.xslx.com/htm/gjzl/jsgc/2003-10-38-15176.htm.

2. China Military Encyclopedia Editorial Committee, *China Military Encyclopedia*, *Military Art* Volume II (Beijing, PRC: Military Science Publishing House, 1997), pp. 764–766.

3. Chinese People's Liberation Army Academy of Military Science, *Chinese People's Liberation Army Military Terminology* (Entire Volume) (Beijing, PRC: AMS Publishing House, 1997), p. 17.

4. XU Xinzhao, "Examining How Information Has Become a Key Factor in Combat Power," *Jianghui Forum* (#2, 2001), pp. 65, 71.

5. Large Phrase Dictionary Editorial Committee, *Large Phrase Dictionary, Military Volume* (Shanghai, PRC: Shanghai Phrasebook Publishing Committee, 2003), p. 13.

6. State Council Information Office, *White Paper on China's National Defense in 2002* (Beijing, PRC: State Council Information Office, 2002), http://www.mod.gov.cn/affair/2011-01/06/content_4249946_2.htm.

7. Emphasis added. State Council Information Office, *China's National Defense in 2004* (Beijing, PRC: State Council Information Office, 2004), http://news.xinhuanet.com/mil/2004-12/27/content_2384964.htm.

8. Ibid.

9. All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume) (Beijing, PRC: Military Science Publishing House, 2011), p. 48.

10. Ibid., p. 79.

11. Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia,* 2nd Edition, *Military Strategy* (Beijing, PRC: China Encyclopedia Publishing House, 2007), p. 68.

12. FAN Gaoming, "Public Opinion Warfare, Psychological Warfare, and Legal Warfare, the Three Major Combat Methods to Rapidly Achieving Victory in War," *Global Times* (March 8, 2005), http://big5.xinhuanet.com/gate/big5/news.xinhuanet.com/mil/2005-03/08/content_2666475.htm.

13. CHANG Long, "Tightly Grasping the Trends of the New Military Transformation—Reflections and Outlook from the Gulf War to the Iraq War," *PLA Daily* (October 28, 2003), http://www.xslx.com/htm/gjzl/jsgc/2003-10-38-15176.htm.

14. YANG Chunchang and SHEN Hetai, Chief Editors, *Political Warfare/Operations under Informationized Conditions* (Beijing, PRC: Long March Press, 2005), p. 15.

15. "Public Opinion Warfare, Psychological Warfare, and Legal Warfare in Modern Conflict Are All Becoming More intense," *People's Liberation Army Daily* (April 1, 2004), http://mil.anhuinews.com/system/2004/04/01/000608647.shtml.

16. YUAN Wenxian, *The Science of Military Information* (Beijing, PRC: National Defense University Publishing House, 2008), pp. 77–79.

17. How the organizational reforms of 2015–2016 will affect the implementation of these regulations is unclear. However, there is a "Political Work Department" (*zhengzhi gongzuo bu*; 政治工作部) in the new structure, which will likely exercise comparable responsibilities.

18. WU Zhizhong, *Wartime Political Work Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), p. 153.

19. Ibid., p. 147.

20. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 403.

21. TAN Wenfang, "The Impact of Information Technology on Modern Psychological Warfare," *National Defense Science and Technology* (#5, 2009), p. 73.

22. Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia*, p. 143.

23. Tan, "The Impact of Information Technology on Modern Psychological Warfare," p. 76.

24. GUO Yanhua, *Psychological Warfare Knowledge* (Beijing, PRC: NDU Publishing House, 2005), p. 10.

25. Tan, "The Impact of Information Technology on Modern Psychological Warfare," p. 73.

26. Ibid., p. 74; and Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia*, pp. 76–77.

27. SUN Lihua, "Battlefield Deceit for Attacking and Disrupting Psychological Defenses—American Military Psychological Warfare Methods," *People's Net* (January 11, 2002), http://www.people.com.cn/GB/junshi/62/20020111/646108.html.

28. Ibid.

29. JI Zhenjie and LIU Wei, "A Brief Discussion of Network Opinion Warfare," *Military Correspondent* (#1, 2009), http://www.chinamil.com.cn/site1/jsjz/2009-01/14/content_1619064.htm.

30. WANG Yuping, "Strengthen Research into Psychological Warfare under Informationized Conditions," *PLA Daily* (May 18, 2004), http://news.xinhuanet.com/mil/2004-05/18/content_1475394.htm.

31. Ibid.

32. GUO Yanhua, *Psychological Warfare Knowledge* (Beijing, PRC: NDU Publishing House, 2005), p. 14.

33. Wang, "Strengthen Research into Psychological Warfare Under Informationized Conditions."

34. ZONG Wenshen, *Legal Warfare: Discussion of 100 Examples and Solutions* (Beijing, PRC: PLA Publishing House, 2004), p. 5.

35. Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia*, p. 143.

36. WANG Mei, "Research on Several Issues of Legal Warfare," *National Defense University Newspaper* (#7, 2004), p. 66. Cited in Song Yunxia, *Legal Warfare Under Informationized Conditions* (Beijing, PRC: Military Science Publishing, 2007).

37. HAN Yanrong, "Legal Warfare: Military Legal Work's High Ground: An Interview with Chinese Politics and Law University Military Legal Research Center Special Researcher Xun Dandong," *Legal Daily* (PRC) (February 12, 2006).

38. Fan, "Public Opinion Warfare, Psychological Warfare, and Legal Warfare."

39. Major General LIU Jiaxin, "General's Views: Legal Warfare—Modern Warfare's Second Battlefield," *Guangming Ribao* (November 3, 2004).

40. Charles J. Dunlap Jr., "Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts," Working Paper, Carr Center for Human Rights, Harvard University Kennedy School of Government (Cambridge, MA; November 29, 2001), p. 8.

41. U.S. Department of Defense, *The National Defense Strategy of the United States of America* (Washington, DC: Office of the Secretary of Defense, June 2008), p. 20.

42. Major General Liu, "General's Views." At the time, Major General Liu was the commandant of the Xian Political Academy of the PLA General Political Department.

43. Zong, *Legal Warfare*, p. 185.

44. ZHOU Jian and ZHU Manqiang, *Legal Warfare: An Overall Assessment of Wartime Military Affairs Law* (Haichao Publishing, 2004), p. 3. Cited in Song, *Legal Warfare under Informationized Conditions*.

45. Song, *Legal Warfare under Informationized Conditions*, pp. 150–153; and Yang and Shen, *Political Operations under Informationized Conditions*, p. 125.

46. Thomas E. Ricks, "Target Approval Delays Irks Air Force Officers," *Washington Post* (November 18, 2001), http://www.washingtonpost.com/wp-srv/nation/Airwar18.html.

47. Seymour Hersh, "King's Ransom: How Vulnerable Are the Saudi Royals" *New Yorker* (September 22, 2001), p. 36. For an alternative view, Gary Solis argues that the failure was in the commanding officer and the rules of engagement (ROE), not the JAG per se. Gary Solis, *The Law of Armed Conflict* (New York: Cambridge University Press, 2010), p. 499. But failure to adhere to ROE may itself become the grounds for legal action and would therefore seem nonetheless vulnerable to lawfare.

48. William M. Arkin, "The Cyberbomb in Yugoslavia," *Washington Post* (October 25, 1999), http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm; and Julian Borger, "Pentagon Kept the Lid on Cyberwar in Kosovo," *The Guardian* (UK) (November 8, 1999), http://www.guardian.co.uk/world/1999/nov/09/balkans.

49. LIU Gaoping, *Study Volume on Public Opinion Warfare* (Beijing, PRC: NDU Publishing House, 2005), p. 5.

50. Ibid., pp. 16–17; and Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 405.

51. The People's Armed Police are part of the Chinese armed forces, along with the PLA, and the reserve forces.

52. YAO Fei, "Some Thoughts Regarding Our Military's Anti-Secessionist Public Opinion and Propaganda Policies," *Military Correspondent* (PRC) (#5, 2009), http://www.chinamil.com.cn/site1/jsjz/node_22972.htm; and JI Chenjie and LIU Wei, "A Brief Discussion of Public Opinion Warfare on the Web," *Military Correspondent* (PRC) (#1, 2009), http://www.chinamil.com.cn/site1/jsjz/2009-01/14/content_1619064.htm.

53. Matthew Boswell, "Media Relations in China's Military: The Case of the Ministry of National Defense Information Office," *Asia Policy* (#8, July 2009), pp. 97–120; and Ben Blanchard, "China Takes Step at Openness, Allows Foreigners at Defense Briefing," *Reuters* (July 31, 2014), http://www.reuters.com/article/2014/07/31/us-china-defence-idUSKBN0G011K20140731.

54. WANG Zijun, CHEN Tao, and MO Jinshan, "Explaining People's Armed Police Public Opinion Warfare Thought," *Hebei Legal Newspaper* (April 6, 2010), http://jiuzhan.hbfzb.com/html/article/201004/201046104703823.html.

55. Yao, "Some Thoughts Regarding Our Military's Anti-Secessionist Public Opinion and Propaganda Policies," *Military Correspondent* (PRC) (#5, 2009), http://www.chinamil.com.cn/site1/jsjz/node_22972.htm.

56. JI Peilin and JI Kaiyun, "The Iran–Iraq War and Psychological Warfare," *Journal of Shangluo University* (XXVIII, #3, June 2014), p. 31.

57. Nanjing Political Academy Military News Department Study Group, "Study of the Journalistic Media Warfare in the Iraq War," *China Military Science* (#4, 2003), p. 28.

58. SHENG Peilin, WANG Lin, and LIU Ya, editors, *100 Examples of Public Opinion Warfare* (Beijing, PRC: PLA Publishing House, 2006), pp. 162–163, 208–209.

59. Rebecca MacKinnon, "China's Censorship 2.0: How companies Censor Bloggers," *First Monday* (XIV, #2, February 2, 2009), http://firstmonday.org/article/view/2378/2089.

60. Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review* (May 2013), p. 1.

61. Ibid., p. 13.

62. "Is China Fraying?" *Economist* (July 9, 2009), http://www.ecnomist.com/node/13988479.

63. Oiwan Lam, "China: When the Network Was Cut in Xinjiang," Global Voices Advocacy (October 13, 2010), https://advocacy.globalvoicesonline.org/2010/13/13/china-when-network-was-cut-in-xinjiang.

64. PU Duanhua, "On Wartime Public Opinion Mobilization," *Journal of the PLA Nanjing Institute of Politics* (#2, 2006), p. 110.

65. State Council Information Office, *China's Active Defense* (Beijing, PRC: State Council Information Office, 2015).

66. Andrew Jacobs and Chris Buckley, "Tales of Army Discord Show Tiananmen Square in a New Light," *New York Times* (June 2, 2014).

67. WANG Yueting, "The Power of Psychological Warfare in Modern Warfare," *Study Times* (March 27, 2005, #113), http://www.china.com.cn/xxsb/txt/2005-10/11/content_5994663.htm.

68. SHENG Peiling, WANG Ling, and LIU Ya, *100 Examples of Public Opinion Warfare* (Beijing, PRC: PLA Publishing House, 2005), pp. 162–180.

69. CHANG Long, "Tightly Grasping the Tends of the New Military Transformation—Reflections and Outlook from the Gulf War to the Iraq War," *People's Liberation Army Daily* (October 28, 2003), http://www.xslx.com/htm/gjzl/jsgc/2003-10-38-15176.htm.

70. "China's Cyber Security under Severe Threat: Report," *Xinhua* (March 19, 2013), http://news.xinhuanet.com/English/china/2013-03/19/c_132246098.htm.

71. Milton Mueller, "China and Global Internet Governance: A Tiger by the Tail," in *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*, ed. by Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2011), p. 190.

72. "Xi Jinping Leads Internet Security Group," *Xinhua* (February 27, 2014), http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm.

73. Ibid.

74. "Xi Jinping: Building Our Nation from a Big Internet State to a Major Internet Power," *Xinhuanet* (February 27, 2014), http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm.

75. For more on Lu Wei, see Paul Mozur and Jane Perlez, "Gregarious and Direct: China's Web Doorkeeper," *New York Times* (December 1, 2014), http://nyti.ms/1tuxRxl.

76. "China Sets Up Office for Internet Information Management," *Xinhuanet* (May 4, 2011), http://news.xinhuanet.com/english/2010/china/2011-05/04/c_138579.htm.

77. State Council, "Notification of the State Council on Authorizing the State Internet Information Office for Responsibility Regarding Internet Information and Content Management," State Council Information Office (August 26, 2014), http://politics.people.com.cn/n/2014/0828/c70731-25558093.html.

78. David Bandurski, "Lu Wei: The Internet Must Have Brakes," China Media Project (September 11, 2014), http;//cmp.hku.hk/2014/09/11/36011/.

79. ZHANG Weihua, "New Theories of Dominance: Issues Concerning Information Dominance," *Journal of Information* (#12, 2007), p. 59.

80. ICANN, *Beginner's Guide to ICANN* (Los Angeles: ICANN, 2013), pp. 1, 26, https://www.icann.org/en/system/files/files/participating-08nov13-en.pdf.

81. Severine Arsene, "The Impact of China on Global Internet Governance in an Era of Privatized Control," Paper presented at the 10th Annual Chinese Internet Research Conference (May 2012), https://hal.archives-ouvertes.fr/hal-00704196v2/document.

82. "Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary General" (September 14, 2011), https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.

83. Ibid.

84. Ibid.

85. "Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary General," https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

86. IPv6 addresses were developed to meet growing demand for Internet addresses, as the previous IPv4 pool was being exhausted. IPv6 addresses are also expected to be more secure. Penny Hermann-Seaton, "Security Features in IPv6," SANS Institute Reading Room (2002), https://www.sans.org/reading-room/whitepapers/protocols/security-features-ipv6-380; and Milton Mueller, "China and Global Internet Governance: A Tiger by the Tail," in *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*, ed. by Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2011), p. 185.

87. Monika Ermert, "ITU Secretary General Visits Old Arch-Rival IETF," Intellectual Property Watch (July 21, 2015), http://www.ip-watch.org/2015/07/21/itu-secretary-general-visits-old-arch-rival-ietf/.

88. Open Net Initiative, "Internet Filtering in China in 2004–2005: A Country Study," https://opennet.net/studies/china.

89. Ibid.

90. The Central People's Government of the People's Republic of China, "Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security" (December 28, 2000), http://english.gov.cn/laws/2005-09/22/content_68771.htm.

91. Ibid.

92. XIAO Li, "Emphasize the Building of Network and Information Security Management Standards, Improve Our Nation's Network Security Management Level," *Xinhuanet* (November 30, 2014), http://politics.people.com.cn/n/2014/1130/c70731-26120705.html.

93. The Chinese term is *xinxi anquan dengji baohu guanli banfa* (信息安全等级保护管理办法). Nathaniel Ahrens of CSIS has translated this as "Regulations on the Classified Protection of Information Security." Nathaniel Ahrens, "National Security and China's Information Security Standards" (Washington, DC: Center for Strategic and International Studies, 2012).

94. Dieter Ernst and Sheri Martin, "The Common Criteria for Information Technology Security Evaluation—Implications for China's Policy on Information Security Standards," Report #108 (Honolulu, Hawaii; East-West Center, 2010).

95. Robert McMillan, "China Policy Could Force Foreign Security Firms Out," *Network World* (August 26, 2010), http://www.networkworld.com/article/2217282/security/china-policy-could-force-foreign-security-firms-out.html; and United States Council for International Business, Statement on China's Compliance with Its World Trade Organization (WTO) Commitments, Statement Submitted to the U.S. Trade Representative (September 20, 2013), http://uscib.org/docs/USCIB_Submission_to_USTR_China_Compliance_with_WTO_Commitments.pdf.

96. Xiao, "Emphasize the Building of Network and Information Security Management Standards," and Hauke Johannes Gierow, "Cyber Security in China: New Political Leadership Focuses on Boosting National Security," Mercator Institute for China Studies (#20, December 9, 2014), p. 2.

97. Jim Finkle, "Beijing to Bar Kaspersky, Symantec Anti-Virus in Procurement: Report," *Reuters* (August 3, 2014), http://www.reuters.com/article/2014/08/03/us-china-software-ban-idUSKBN0G30QH20140803.

98. Arsene, "The Impact of China on Global Internet Governance in an Era of Privatized Control."

99. "People's Republic of China National Security Law," *China Daily* (July 1, 2015), http://www.chinadaily.com.cn/hqcj/zgjj/2015-07-01/content_13912103.html.

100. Bruce Einhorn, "A Cybersecurity Law in China Squeezes Foreign Tech Companies," *Bloomberg News* (January 21, 2016), http://www.bloomberg.com/news/articles/2016-01-21/a-cybersecurity-law-in-china-squeezes-foreign-tech-companies.

101. The Central People's Government of the People's Republic of China, "Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security."

102. Thomas Lum, Patricia Moloney Figliola, and Matthew Weed, *China, Internet Freedom, and US Policy*, R42601 (Washington, DC: Congressional Research Service, 2012), p. 1, https://www.fas.org/sgp/crs/row/R42601.pdf.

103. Bill Marczak, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ronald Deibert, Vern Paxson, "China's Great Cannon," The Citizen Lab Research Brief (April 2015), p. 3.

104. "Great Firewall 'Upgrade' Troubles VPN Users in China," AFP (December 21, 2012), http://www.securityweek.com/great-firewall-upgrade-troubles-vpn-users-china.

105. Sophia YAN, "China Crackdown Makes It Harder to Get around Great Firewall," *CNN* (January 28, 2015), http://money.cnn.com/2015/01/28/technology/china-censorship-vpn-great-firewall/.

106. Robert Faris, Hal Roberts, and Stephanie Wang, *China's Green Dam: The Implications of Government Control Encroaching on the Home PC*, Open Net Initiative Bulletin (June 2009), p. 2, http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc.

107. Andrew Jacobs, "China Faces Criticism over New Software Censor," *New York Times* (June 11, 2009), http://www.nytimes.com/2009/06/11/world/asia/11censor.html.

108. "Cat and Mouse," *Economist* (April 6, 2013), http://www.economist.com/news/special-report/21574629-how-china-makes-sure-its-internet-abides-rules-cat-and-mouse.

109. Arsene, "The Impact of China on Global Internet Governance in an Era of Privatized Control."

110. Open Net Initiative, "Internet Filtering in China in 2004–2005."

111. Anne S.Y. CHEUNG and ZHAO Yun, "An Overview of Internet Regulation in China," University of Hong Kong Faculty of Law Research Paper #2013/040 (November 21, 2013), p. 7, http://ssrn.com/abstract=2358247.

112. "Cat and Mouse," *Economist*; and "China Employs Two Million Microblog Monitors, State Media Say," *BBC News* (October 4, 2013), http://www.bbc.com/news/world-asia-china-24396957.

113. David Bamman, Bredan O'Connor, and Noah Smith, "Censorship and Deletion Practices in Chinese Social Media," *First Monday* (XVII, 3, March 5, 2012), http://firstmonday.org/article/view/3943/3169.

114. Beina XU, "Media Censorship in China," Council on Foreign Relations (September 25, 2014), http://www.cfr.org/china/media-censorship-china/p11515.

115. Jim Yardley, "A Hundred Million Cellphones Bloom, and Chinese Take to the Streets," *New York Times* (April 25, 2005), http://www.nytimes.com/2005/04/25/world/asia/a-hundred-cellphones-bloom-and-chinese-take-to-the-streets.html?_r=0.

116. Graham Earnshaw, *China Economic Review's China Business Guide 2005* (Shanghai, PRC: SinoMedia Holdings, 2005), p. 80, Joseph Kahn, "China Is Filtering Phone Text Messages to Regulate Criticism," *New York Times* (July 3, 2004), http://www.nytimes.com/2004/07/03/international/asia/03chin.html; and Li YUAN, "Text Messages Sent by Cellphone Finally Catch on in US," *Wall Street Journal* (August 11, 2005), http://www.wsj.com/articles/SB112372600885810565.

117. Yanzhong HUANG, "The SARS Epidemic and Its Aftermath in China: A Political Perspective" in *Learning from SARS: Preparing for the Next Disease Outbreak, a Workshop Summary*, ed. by Stacey Knobler and Adel Mahmoud (Washington, DC: National Academies Press, 2004), http://www.ncbi.nlm.nih.gov/books/NBK92479/.

118. Joseph Kahn, "China Is Filtering Phone Text Messages to Regulate Criticism," *New York Times* (July 3, 2004), http://www.nytimes.com/2004/07/03/international/asia/03chin.html.

119. Miguel Helft, "YouTube Blocked in China, Google Says," *New York Times* (March 25, 2009), https://www.nytimes.com/2009/03/25/technology/internet/25youtube.html.

120. Weibo Corporation, Form F-1 Registration Statement with US Securities and Exchange Commission (March 14, 2014), p. 36, http://www.sec.gov/Archives/edgar/data/1595761/000119312514100237/d652805df1.htm.

121. Edward Wong, "After Long Ban, Western China Is Back Online," *New York Times* (May 14, 2010), http://www.nytimes.com/2010/05/15/world/asia/15china.html.

122. Reporters without Borders, "Survey of Blocked Uyghur Websites Shows Xinjiang Still Cut off from the World" (October 29, 2009), https://www.rsf.org/china-survey-of-blocked-uyghur-websites-29-10-2009,34859.html.

123. Xu, "Media Censorship in China."

124. Simon Denyer and XU Yangjingjing, "Unable to Clean Air Completely for APEC, China Resorts to Blocking Data," *Washington Post* (November 10, 2014), https://www.washingtonpost.com/news/worldviews/wp/2014/11/10/unable-to-clean-air-completely-for-apec-china-resorts-to-blocking-data/.

125. Paul Carsten, "China Scrambles to Censor Social Media," *Reuters* (September 29, 2014), http://www.huffingtonpost.com/2014/09/29/china-social-media_n_5901362.html.

126. This section is drawn from Tao ZHU, David Phipps, Adam Pridgen, Jedidiah R. Crandall, Dan S. Wallach, "Tracking and Quantifying Censorship on a Chinese Microblogging Site" (November 26, 2012), arXiv:1211.6166[cs.IR]; and Tao ZHU, David Phipps, Adam Pridgen, "The Velocity of Censorship: High Fidelity Detection of microblog Post Deletions," Paper presented at the 22nd USENIX Security Symposium (August 2013).

127. Jed Crandall and Dan Wallach, "The Astonishing Speed of Chinese Censorship," *BBC News* (March 27, 2013), http://www.bbc.com/news/world-asia-china-21743499.

128. David Bamman, Brendan O'Connor, and Noah Smith, "Censorship and Deletion Practices in Chinese Social Media," *First Monday* (XVII, #3, March 5, 2012), http://firstmonday.org/article/view/3943/3169; and Cheung and Yun, "An Overview of Internet Regulation in China."

129. Zhu et al., "The Velocity of Censorship."

130. Nicholas Kristof, "Privately, More and More Chinese Say It's Past Time for Deng to Go," *New York Times* (April 17, 1989), http://www.nytimes.com/1989/04/17/world/privately-more-and-more-chinese-say-it-s-past-time-for-deng-to-go.html.

131. Zhu et al., "The Velocity of Censorship."

132. Zhu et al., "Tracking and Quantifying Censorship on a Chinese Microblogging Site."

CHAPTER 4

1. WANG Hui, *Foundational Knowledge, Considerations, and Explanations of Informationized Warfare* (Beijing, PRC: Military Science Publishing House, 2009), p. 108.

2. ZHANG Yuliang, Chief Editor, *The Science of Campaigns* (Beijing, PRC: National Defense University Publishing House, 2006), p. 155.

3. CUI Shizeng and WANG Junyi, "Advancing Military Transformation with Chinese Characteristics, Strengthening 'Integrated-Style Joint Operations,'" *People's Liberation Army Daily* (July 7, 2004), http://news.xinhua.net.com/mil/2004-07/07/content_1578870.htm.

4. Emphasis added. Zhang, *Science of Campaigns,* p. 273.

5. Cui and Wang, "Advancing Military Transformation with Chinese Characteristics."

6. LI Daguang, "Reconsideration of the Mechanisms for Winning Informationized Warfare," *China Military Science* (#6, 2014), pp. 80–81.

7. ZOU Zhenning and CHA Rui, *Command Information Capabilities Research, Based on Systems Combat between Information Systems* (Beijing, PRC: Oceans Publishing House, 2011), p. 57.

8. Li, "Reconsideration of the Mechanisms for Winning Informationized Warfare."

9. Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia,* 2nd Edition, *Campaigns* (Beijing, PRC: China Encyclopedia Publishing House, 2007), p. 126.

10. Ibid. The obvious parallel is to the Observe/Orient/Decide/Act (or OODA) loop identified by USAF Colonel John Boyd.

11. ZHANG Peigao, *Joint Campaign Command Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2012), p. 33.

12. XU Guoxing, *Research on Our Military's Information Operations Strength Construction* (Beijing, PRC: Military Science Publishing House, 2013), pp. 76–77.

13. Zou and Cha, *Command Information Capabilities Research*.

14. SUN Jinwei, *Research on Laws Governing Campaign Dilemmas and Activities* (Beijing, PRC: National Defense University Press, 2013), p. 74.

15. Zou and Cha, *Command Information Capabilities Research*, p. 61.

16. Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia*, p. 127.

17. HE Zhu, *Experts Assess the Iraq War* (Beijing, PRC: Military Science Publishing House, 2004), p. 146.

18. Zhang, *Science of Campaigns,* p. 155.

19. BAI Bangxi and JIANG Lijun, "Systems of Systems Conflict Is Not the Same as Systems Conflict," *National Defense Newspaper* (January 10, 2008), http://www.chinamil.com.cn/site1/xwpdxw/2008-01/10/content_1084469.htm.

20. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide* (Beijing, PRC: Military Science Publishing House, 2005), p. 114.

21. KOU Shiqiang, "A Clarification of Unified Joint Operations," *People's Liberation Army Daily* (August 11, 2004), http://www.china.com.cn/military/zhuanti/sjxjsbg/txt/2004-08/11/content_5632264.htm.

22. Bai and Jiang, "Systems of Systems Conflict Is Not the Same as Systems Conflict."

23. Ibid.

24. Li Yingming, Liu Xiaoli, et al., "An Analysis of Integrated Joint Operations," *PLA Daily* (April 12, 2005).

25. Wang, *Foundational Knowledge*, pp. 108–109.

26. LI Yousheng, *Science of Joint Campaign Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2012), p. 72.

27. WU Renhe, *Theory of Informationized Conflict* (Beijing, PRC: Military Science Publishing House, 2004), p. 21.

28. Zhang, *Science of Campaigns,* p. 155.

29. Wang, *Foundational Knowledge, Considerations, and Explanations of Informationized Warfare*, p. 4.

30. MAO Zedong, *Six Essays on Military Affairs* (Beijing, PRC: Foreign Languages Press, 1972), p. 50.

31. State Council Information Office, *China's Active Defense* (Beijing, PRC: State Council Information Office, 2015).

32. All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume) (Beijing, PRC: Military Science Publishing House, 2011), pp. 55, 79, 119.

33. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 13.

34. Wang, *Foundational Knowledge*, p. 113.

35. The following section is drawn mainly from Zhang, *Science of Campaigns,* pp. 86–90.

36. Ibid., p. 87.

37. All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology*, p. 67.

38. Zhang, *Science of Campaigns,* p. 89.

39. The following section is drawn mainly from Zhang, *Science of Campaigns,* pp. 90–93.

40. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 92.

41. Wu, *Theory of Informationized Conflict*, p. 173.

42. Zhang, *Science of Campaigns,* pp. 89–90.

43. Ibid., p. 164.

44. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 88.

45. Zhang, *Science of Campaigns,* p. 91.

46. Li, *Science of Joint Campaign Teaching Materials*, p. 69. See also pp. 69–72 for a fuller discussion of the interplay between information dominance and these other physical domains.

47. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 87.

48. Wu, *Theory of Informationized Conflict*, p. 168.

49. Wang, *Foundational Knowledge*, p. 111.

50. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 87.

51. Zhang, *Science of Campaigns,* p. 90.

52. Wang, *Foundational Knowledge*, p. 180.

53. All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology*, p. 255.

54. YUAN Wenxian, *The Science of Military Information* (Beijing, PRC: National Defense University Press, 2007), pp. 84–85.

55. Wang, *Foundational Knowledge,* p. 179.

56. Yuan, *Science of Military Information*.

57. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, pp. 93–94.

58. YE Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), pp. 21–22.

59. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, pp. 93–94.

60. Yuan, *Science of Military Information*, p. 71.

61. Ibid., p. 314.

62. This section draws from Ye, *Science of Information Operations Teaching Materials*, pp. 22–23.

63. YE Zheng, *Concepts of Informationized Operations* (Beijing, PRC: Military Science Publishing House, 2007), p. 158.

64. Wang, *Foundational Knowledge*, p. 180.

65. All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology*, p. 286; and Zheng, *Science of Information Operations Teaching Materials*, p. 24.

66. Ye, *Science of Information Operations Teaching Materials*, p. 28.

67. Ibid., pp. 24, 25.

68. YUAN Wenxian, *Joint Campaign Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2009), p. 14.

69. Yuan, *Science of Military Information*, p. 73.

70. Ye, *Science of Information Operations Teaching Materials*, p. 25.

71. Ibid., pp. 24–25.

72. Wu, *Theory of Informationized Conflict*, p. 168.

73. TAN Rukun, *Operational Strength Construction Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2012), p. 231.

74. Ye, *Science of Information Operations Teaching Materials*, p. 25.

75. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 101.

76. All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology*, pp. 262–263.

77. Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia*, p. 327.

78. Ye, *Concepts of Informationized Operations*, p. 157; and Ye, *Science of Information Operations Teaching Materials*, p. 27.

79. Ye, *Science of Information Operations Teaching Materials*, pp. 28–29.

80. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 101.

81. Ye, *Science of Information Operations Teaching Materials*, p. 28.

82. Ibid., pp. 25–26; and All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology*, p. 456.

83. Wu, *Theory of Informationized Conflict*, p. 192.

84. Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia*, p. 67.

85. Ibid.

86. Yuan, *Joint Campaign Information Operations Teaching Materials*, p. 15.

87. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 88.

88. Yuan, *Science of Military Information*, pp. 75, 314.

89. Ibid., p. 309.

90. Wu, *Theory of Informationized Conflict*, p. 201.

91. FAN Gaoyue and FU Linguo, *The First Conflict to Display Initial Informationization Conditions: The Iraq War* (Beijing, PRC: Military Science Publishing House, 2008), p. 195.

92. Ye, *Science of Information Operations Teaching Materials*, p. 27.

93. Ibid.

94. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 91.

95. All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology*, p. 288.

96. FENG Lixin, "An Examination of Several Issues Concerning Command Protection and Information Control," in *Research on Military Command*, ed. by Wei Konghu (Beijing, PRC: National Defense University Press, 2014), p. 222.

97. All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology*, p. 175.

98. Ibid., p. 175.

99. QIN Jirong, *Concepts of Command and Control* (Beijing, PRC: National Defense Industry Press, 2012), pp. 4–5.

100. Director for Joint Force Development J-7, *Department of Defense Dictionary of Military and Associated Terms*, JP 1–02 (Washington, DC: Pentagon, 2015), p. 49.

101. Ibid., p. 41.

102. Ibid., p. 179.

103. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 97.

104. GONG Cunchen, "Characteristics, Principles, and Methods of Command Conflict in Landing Campaigns," in *Research on Military Command*, ed. by WEI Konghu (Beijing, PRC: National Defense University Press, 2014), p. 141.

105. LI Jingxu, "Initial Discussions of Joint Operations Command Structure Mechanisms Based on Information Systems," in *Research on Military Command*, ed. by WEI Konghu (Beijing, PRC: National Defense University Press, 2014), p. 38.

106. SONG Yuejin, Chief Editor, *Command and Control Warfare* (Beijing, PRC: National Defense University Press, 2012), p. 201.

107. XU Guoqiang, "A Simple Discussion of Shared Operational Awareness," in *Research on Military Command*, ed. by WEI Konghu (Beijing, PRC: National Defense University Press, 2014), p. 48.

108. Tan, *Operational Strength Construction Teaching Materials*, pp. 205–206.

109. Wang, *Foundational Knowledge*, p. 112.

110. Feng, "An Examination of Several Issues Concerning Command Protection and Information Control."

111. WANG Yongming and LIU Xiaoli, *Iraq War Research* (Beijing, PRC: Military Science Publishing House, 2003), p. 151.

112. Ibid., p. 97; and Song, *Command and Control Warfare*, p. 57.

113. Song, *Command and Control Warfare*, p. 57.

114. Gong, "Characteristics, Principles, and Methods of Command Conflict in Landing Campaigns."

115. Wang, *Foundational Knowledge,* p. 113.

116. Ye, *Science of Information Operations Teaching Materials*, p. 29.

117. Song, *Command and Control Warfare*, p. 58.

118. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 98.

119. Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia*, p. 196; and Yuejin, *Command and Control Warfare*, p. 80.

120. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 91.

121. Yuan, *Science of Military Information*, pp. 192–195.

122. Song, *Command and Control Warfare*, p. 80; and Yuan, *Science of Military Information*, p. 309.

123. Li, "Reconsideration of the Mechanisms for Winning Informationized Warfare," p. 80.

124. Song, *Command and Control Warfare*, p. 80.

125. Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia*, p. 139.

126. Ibid., p. 197.

127. Ibid., pp. 196, 197.

128. Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia*, p. 196.

129. Wu, *Theory of Informationized Conflict*, p. 173.

130. Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia*, p. 198.

131. Song, *Command and Control Warfare*, p. 81.

132. Roger Hesketh, *Fortitude: The D-Day Deception Campaign* (Woodstock, NY: Overlook Publishers, 2000).

133. Xu, *Research on Our Military's Information Operations Strength Construction*, p. 27.

134. Song, *Command and Control Warfare*, p. 80.

CHAPTER 5

1. LI Yousheng, *Science of Joint Campaign Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2012), pp. 124–125.

2. This section is drawn from YUAN Wenxian, *The Science of Military Information* (Beijing, PRC: National Defense University Press, 2008), pp. 177–183.

3. Yuan, *Science of Military Information*, p. 178.

4. Li, *Science of Joint Campaigns Teaching Materials*, p. 124.

5. Drawn from YUAN Wenxian, *Joint Campaign Information Operations Teaching Materials* (Beijing, PRC: National Defense University Press, 2009), pp. 173–174.

6. "Advanced Persistent Threats: How They Work," Symantec, http://www.symantec.com/theme.jsp?themeid=apt-infographic-1.

7. U.S. Department of Justice, "US Charges Five Chinese Military Hackers for Cyber Espionage against US Corporations and Labor Organization for Commercial Advantage," Press Release (May 19, 2014), http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

8. Sophie Borland, "MI-5 Warns Firms over China Internet 'Spying,'" *Daily Telegraph* (April 12, 2008), http://www.telegraph.co.uk/news/worldnews/1571172/MI5-warns-firms-over-Chinas-internet-spying.html.

9. David Ljunggren and Alastair Sharp, "Hacking Attack in Canada Bears Signs of Chinese Army Unit: Expert," *Reuters* (August 1, 2014), http://www.reuters.com/article/us-china-canada-cybersecurity-idUSKBN0G13X220140801.

10. Information Warfare Monitor, *Tracking GhostNet: Investigating a Cyber-Espionage Network* (March 29, 2009), https://www.f-secure.com/weblog/archives/ghostnet.pdf.

11. Jeremy Wagstaff, "Hunt for Deep Panda Intensifies in Trenchs of US–China Cyberwar," *Reuters* (June 21, 2015), http://www.reuters.com/article/us-cybersecurity-usa-deep-panda-idUSKBN0P102320150621; and Dmitri Alperovich, *Deep in Thought: Chinese Targeting of National Security Think-Tanks*, Crowdstrike (July 7, 2014), http://www.crowdstrike.com/blog/deep-thought-chinese-targeting-national-security-think-tanks/.

12. RSA Research, *Terracotta VPN*, RSA (August 4, 2015), https://blogs.rsa.com/wp-content/uploads/2015/08/Terracotta-VPN-Report-Final-8–3.pdf.

13. Kaspersky Lab Global Research and Development Team, *The Icefog APT, a Tale of Cloak and Three Daggers*, Kaspersky Labs (January 20, 2014), http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/icefog.pdf.

14. Kaspersky Lab Global Research and Development Team, *The NetTraveler (aka "Travnet"),* Kaspersky Labs (June 4, 2013), https://cdn.securelist.com/files/2014/07/kaspersky-the-net-traveler-part1-final.pdf.

15. McAfee Foundstone Professional Services, *Global Energy Cyberattacks: "Night Dragon,"* McAfee Labs (February 10, 2011), http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

16. Google, "A New Approach to China," Google Official Blog (January 12, 2010), https://googleblog.blogspot.com/2010/01/new-approach-to-china.html; and Kim Zetter, "Google Hack Attack Was Ultra-Sophisticated, New Details Show," *Wired* (January 14, 2010), http://www.wired.com/2010/01/operation-aurora/.

17. Paul Rosenzweig, *Cyber Warfare* (Denver, CO: Praeger Publishers, 2013), pp. 38–39.

18. Tom Espiner, "Security Experts Lift Lid on Chinese Hack Attacks," ZDNet (November 23, 2005), http://www.zdnet.com/article/security-experts-lift-lid-on-chinese-hack-attacks/.

19. YE Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), pp. 154–155.

20. Elinor Mills, "Web Traffic Redirected to China Still a Mystery," CNET (October 8, 2010), http://www.cnet.com/news/web-traffic-redirected-to-china-still-a-mystery/.

21. Drawn from Yuan, *Joint Campaign Information Operations Teaching Materials*, pp. 174–176; and Ye, *Science of Information Operations Teaching Materials*, pp. 157–159 and 163–169.

22. Academy of Military Science Military Strategy Research Office, *The Science of Military Strategy* (Beijing, PRC: Military Science Publishing House, 2013), p. 192.

23. Ibid.

24. Yuan, *Joint Campaign Information Operations Teaching Materials*, p. 175.

25. Ye, *Science of Information Operations Teaching Materials*, p. 170.

26. Yuan, *Science of Military Information*, p. 310.

27. Ye, *Science of Information Operations Teaching Materials*, pp. 170–173.

28. Ibid., p. 171.

29. ZHANG Peigao, *Joint Campaign Command Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2012), p. 160.

30. Drawn from Ye, *Science of Information Operations Teaching Materials*, pp. 92–96.

31. Ibid., pp. 176–177.

32. WANG Ruqun, *The Battlefield Electromagnetic Environment* (Beijing, PRC: People's Liberation Army Press, 2006), pp. 219–223.

33. Jeffrey Lin and P.W. Singer, "The Missiles of Zhuhai: China Displays New Strike Arsenal," *Popular Science* (November 17, 2014), http://www.popsci.com/missiles-zhuhai-china-displays-new-strike-arsenal.

34. FCC, "Notice of Apparent Liability and Forfeiture, Illegal Marketing of Signal Jamming Devices," File Number: EB-SED-12–00005692 (June 19, 2014), http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db0619/FCC-14-92A1.pdf.

35. Ye, *Science of Information Operations Teaching Materials*, p. 96.

36. Ibid., pp. 182–184.

37. Ibid., p. 183.

38. Earl Zmijewski, "Accidentally Importing Censorship," Dynresearch (March 30, 2010), http://research.dyn.com/2010/03/fouling-the-global-nest/.

39. For an extensive discussion of Stuxnet, see Kim Zetter, *Countdown to Zero Day* (New York: Broadway Books, 2014).

40. WANG Hui, *Foundational Knowledge, Considerations, and Explanations of Informationized Warfare* (Beijing, PRC: Military Science Publishing House, 2009), pp. 301–302.

41. This section draws upon Bill Marczak, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ronald Deibert, and Vern Paxson, *China's Great Cannon Research Brief*, CitizenLab (April 2015), https://citizenlab.org/wp-content/uploads/2009/10/ChinasGreatCannon.pdf, "China's Man on the Side Attack on GitHub," Netresec (March 31, 2015), http://www.netresec.com/?

month=2015-03&page=blog&post=china%27s-man-on-the-side-attack-on-github; and Robert Graham, "Pinpointing China's Attack against GitHub," Errata Security (April 1, 2015), http://blog.erratasec.com/2015/04/pin-pointing-chinas-attack-against.html#.VSvhdJTF8nh.

42. Ben Brumfeld, "Study: China Cybercensors Attack outside Its Borders with 'Great Cannon,'" *CNN* (April 12, 2015), http://www.cnn.com/2015/04/12/china/china-cyber-censorship-weapon/.

43. "China's Man on the Side Attack on GitHub," Netresec (March 31, 2015), http://www.netresec.com/?month=2015-03&page=blog&post=china%27s-man-on-the-side-attack-on-github.

44. RSA Research, Terracotta VPN, RSA (August 4, 2015), p. 9, https://blogs.rsa.com/wp-content/uploads/2015/08/Terracotta-VPN-Report-Final-8-3.pdf.

45. Academy of Military Science Military Strategy Research Office, *Science of Military Strategy*, p. 191.

46. Wang, *Foundational Knowledge*, p. 124.

47. Ye, *Science of Information Operations Teaching Materials*, p. 30.

48. Wyatt Olson, "'Left Hook' Deception Hastened War's End," *Stars and Stripes* (2016), http://www.stripes.com/news/special-reports/the-gulf-war-25-year-anniversary/deception.

49. Liat Clark, "Chinese Military 'Hacked' Israel's Iron Dome," *Wired* (July 29, 2014), http://www.wired.co.uk/news/archive/2014-07/29/iron-dome-tech-stolen.

50. CHI Yajun and XIAO Yunhua, *Essentials of Informationized Warfare and Information Operations Theory* (Beijing, PRC: Military Science Publishing House, 2005), pp. 266–267.

51. Academy of Military Science Military Strategy Research Office, *Science of Military Strategy*, p. 188.

52. NI Tianyou, *Command Information Systems Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), pp. 200–209.

53. Ye, *Science of Information Operations Teaching Materials*, pp. 210–211.

54. Wang, *Foundational Knowledge*, p. 125.

55. Ye, *Science of Information Operations Teaching Materials*, p. 211.

56. Ni, *Command Information Systems Teaching Materials*, p. 207.

57. Ye, *Science of Information Operations Teaching Materials*, pp. 211–212.

58. Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia,* 2nd Edition, *Military Psychology* (Beijing, PRC: China Encyclopedia Publishing 2007), p. 92.

59. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide* (Beijing, PRC: Military Science Publishing House, November 2005), pp. 356–367; and Wenxian, *Science of Military Information*, pp. 210–216.

60. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, pp. 360–364.

61. Christopher C. Elisan, *Malware, Rootkits, & Botnets* (New York: McGraw-Hill, 2013), pp. 11, 18.

62. CHEN Bing, QIAN Hongyan, and HU Jie, *Network Security* (Beijing, PRC: National Defense Industry Press, 2012), p. 14.

63. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, pp. 366–367; and Bing et al., *Network Security*, p. 24.

64. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 366.

65. "Foreign Tech Firms Pose Threat on Internet," *China Daily* (June 4, 2014), http://en.people.cn/n/2014/0604/c207959-8736319.html.

66. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, pp. 365–366.

67. Ibid., pp. 352, 355.

68. This section draws upon HU Guangming, *Military Informationization Construction Teaching Materials* (Beijing, PRC: Military Science Press, 2012), p. 48. For a comparison, see Steven Bellovin, *Thinking Security* (New York: Addison-Wesley, 2016).

69. Hu, *Military Informationization Construction Teaching Materials*, p. 48.

70. Ni, *Command Information Systems Teaching Materials*, pp. 204, 205.

71. LIU Youfang and HAN Qiang, editors, *Military Information Security Principles* (Beijing, PRC: National Defense University Press, 2005), p. 83.

72. Ni, *Command Information Systems Teaching Materials*, p. 205; and Guo Ruobing, *Discussions of Military Information Security* (Beijing, PRC: National Defense University Press, 2013), pp. 201–202.

73. Suril Amin, "The People's Republic of China Will Stick with Windows XP," Microsoft News (April 23, 2014), http://microsoft-news.com/the-peoples-republic-of-china-will-stick-with-windows-xp/.

74. Eva Dou, "The Obscure Chinese Operating System Sold by Dell, HP," *Wall Street Journal* (September 15, 2015), http://blogs.wsj.com/chinarealtime/2015/09/15/the-obscure-chinese-operating-system-sold-by-dell-hp/.

75. Nikhil Sonnad, "A First Look at the Chinese Operating System the Government Wants to Replace Windows," *Quartz* (September 22, 2015), http://qz.com/505383/a-first-look-at-the-chinese-operating-system-the-government-wants-to-replace-windows/.

76. "China Said to Plan Sweeping Shift from Foreign Technology to Own," Bloomberg News (December 17, 2014), http://www.bloomberg.com/news/articles/2014-12-17/china-said-to-plan-sweeping-shift-from-foreign-technology-to-own?hootPostID=f047ce391d1e79bebf8d0f1b50ed2a0d.

77. Ye, *Science of Information Operations Teaching Materials*, p. 216.

78. Guo, *Discussions of Military Information Security*, p. 249.

79. Ibid., pp. 200–201; and Ni, *Command Information Systems Teaching Materials*, pp. 202, 205.

80. James Holmes, "China's Underground Great Wall," *The Diplomat* (August 20, 2011), http://thediplomat.com/2011/08/chinas-underground-great-wall/.

81. Russell Hsiao, "China's Underground 'Great Wall' and Nuclear Deterrence," *Jamestown Foundation China Brief* (December 16, 2009), http://www.jamestown.org/

programs/chinabrief/single/?tx_ttnews[tt_news]=35846&tx_ttnews[backPid]=459&no_cache=1.

82. The Office of Civil Air Defense of the People's Republic of China, PRC Civil Air Defense Law (May 5, 2011), http://www.ccad.gov.cn/view/zhengcefagui/falvfagui/20110505/15.html.

83. All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology*, p. 262.

84. Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia,* 2nd Edition, *Military Strategy* (Beijing, PRC: China Encyclopedia Publishing 2007), p. 283.

85. Thomas Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1967), p. 69.

86. Ibid.

87. Emphasis added. Glenn Snyder, "Deterrence and Defense," in *The Use of Force*, ed. by Robert Art (New York: University Press of America, 1988), p. 31.

88. All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology*, p. 51.

89. PENG Guangqian and YAO Youzhi, *The Science of Military Strategy* (Beijing, PRC: AMS Press, 2005), p. 215.

90. Emphasis added. National Defense University Science Research Department, *New Perspectives on Military Transformation: Explaining 200 New Military Concepts* (Beijing, PRC: PLA Press, 2004), p. 85.

91. LUO Youli, General Editor, *National Defense Theory* (Beijing, PRC: Academy of Military Science Publishing House, 2002), pp. 113–114.

92. Ibid., p. 114.

93. Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia,* 2nd Edition, *Military Strategy* (Beijing, PRC: China Encyclopedia Publishing 2007), p. 283.

94. Academy of Military Science Military Strategy Research Office, *The Science of Military Strategy* (Beijing, PRC: Military Science Publishing House, 2013), p. 196.

95. Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, pp. 15–16.

96. Ibid., p. 15.

97. Academy of Military Science Military Strategy Research Office, *Science of Military Strategy*, p. 190.

CHAPTER 6

1. LI Dayao, "A Survey of the Development of Space Technology in China," *China Aerospace* (June 1999), pp. 16–19, in FBIS-CHI (September 21, 1999).

2. Material drawn from *Guojia Gao Jishu Yanjiu Fazhan Jihua 863*, in FBIS-CHI (July 21, 2000). For further discussion of the creation of Plan 863, see Evan Feigenbaum, *China's Techno-Warriors* (Stanford: Stanford University Press, 2003), pp. 141–143.

3. WANG Houqing and ZHANG Xingye, Chief Editors, *The Science of Campaigns* (Beijing, PRC: National Defense University Publishing House, 2000), p. 400.

4. Gao, *Joint Campaign Course Materials*, p. 54.

5. GAO Qingjun, "Aerospace Reconnaissance Characteristics and Limits in High-tech Local Wars," *Journal of the Academy of Command Equipment and Technology* (XVI, #1, February 2005).

6. PLA Encyclopedia Committee, *Chinese Military Encyclopedia*, *Military Art*, Vol. III (Beijing, PRC: Military Science Publishing House, July 1997), p. 602.

7. PLA Encyclopedia Committee, *Chinese Military Encyclopedia*, Supplemental Volume (Beijing, PRC: Military Science Publishing House, 2002), p. 455.

8. ZHANG Yuwu, Dong Zean, et al., "Informationalized Warfare Will Make Seizing the Aerospace Technology 'High Ground' a Vital Factor," *People's Liberation Army Daily* (March 30, 2005).

9. JIANG Lianju, *Space Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), p. 65.

10. LIU Kejian and WANG Xiubo, *The First Conflict Won through Airpower: The Kosovo War* (Beijing, PRC: Military Science Publishing House, 2008), p. 44; and Jiang, *Space Operations Teaching Materials*.

11. HU Jintao, "See Clearly Our Military's Historic Missions in the New Period of the New Century" (December 24, 2004), http://gfjy.jxnews.com.cn/system/2010/04/16/011353408.shtml. For further discussion of the "new historic missions," see Daniel Hartnett, *Towards a Globally Focused Chinese Military: The Historic Missions of the Chinese Armed Forces* (Alexandria, VA: CNA Corporation, 2008).

12. ZHANG Yuliang, Chief Editor, *The Science of Campaigns* (Beijing, PRC: National Defense University Publishing House, 2006), p. 87.

13. Ibid., p. 81.

14. WANG Weiyu and ZHANG Qiancheng, *Discussing Military Theory Innovation with Chinese Characteristics* (Beijing, PRC: National Defense University Publishing House, 2009), pp. 202–203.

15. Zhang, *Science of Campaigns,* p. 83.

16. Academy of Military Science Military Strategy Research Office, *The Science of Military Strategy* (Beijing, PRC: Military Science Publishing House, 2013), pp. 146–147.

17. YUAN Wenxian, *The Science of Military Information* (Beijing, PRC: National Defense University Publishing House, 2008), p. 324.

18. "Lu Jin: Satellite Communications—The Information Bridge during Earthquake Relief Operations," Speech before the Chinese Communications Studies Association (September 26, 2008), http://www.ezcom.cn/Article/8591.

19. MA Ping, *Joint Operations Research* (Beijing, PRC: National Defense University Publishing House, 2013), p. 220.

20. Up until December 31, 2015, the PLA was managed by several general departments that oversee all the armed forces, including all the services. These were the General Staff Department (GSD), the General Political Department (GPD), the General Logistics Department (GLD), and since 1998 the General Armaments Department (GAD). These departments comprised the membership of the Central Military Commission (CMC) until 2004, when the PLA Navy, PLA Air Force, and Second Artillery were added to the CMC.

21. Leonard David, "China's Antisatellite Test; Worrisome Debris Cloud Encircles Earth," Space.com (February 2, 2007), http://www.space.com/3415-china-anti-satellite-test-worrisome-debris-cloud-circles-earth.html.

22. "China: Missile Defense System Test Successful," *USAToday* (January 11, 2010), http://www.usatoday.com/news/world/2010-01-11-china-missile-defense_N.htm.

23. William Matthews, "Chinese Puzzle," *Defense News* (September 6, 2010), http://www.defensenews.com/story.php?i=4767907.

24. Brian Weeden, *Through a Glass Darkly: Chinese, Russian, and American Anti-Satellite Testing in Space* (Washington, DC: Secure World Foundation, 2014).

25. Mike Gruss, "Space Surveillance Satellites Pressed into Early Service," *Space News* (September 18, 2015), http://spacenews.com/space-surveillance-sats-pressed-into-early-service/.

26. Jiang, *Space Operations Teaching Materials*, p. 40.

27. Ibid., p. 40.

28. LI Yousheng, *Joint Campaign Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2012), p. 98.

29. Jiang, *Space Operations Teaching Materials*, p. 43.

30. Ibid., p. 44.

31. YE Zheng, *Concepts of Informationized Operations* (Beijing, PRC: Military Science Publishing House, 2007), p. 154; and CHI Yajun and XIAO Yunhua, *Essentials of Informationized Warfare and Information Operations Theory* (Beijing, PRC: Military Science Publishing House, 2005), pp. 38–39.

32. XU Guoxing, *Research on Our Military's Information Operations Strength Construction* (Beijing, PRC: Military Science Publishing House, 2013), p. 50.

33. CHANG Xianqi, *Military Astronautics*, 2nd ed. (Beijing, PRC: National Defense Industries Press, 2005), pp. 219–220.

34. Academy of Military Science Military Strategy Research Office, *Science of Military Strategy*, p. 180.

35. WU Renhe, *Theory of Informationized Conflict* (Beijing, PRC: Military Science Publishing House, 2004), p. 102.

36. Ye, *Concepts of Informationized Operations*, p. 154.

37. Chi and Xiao, *Essentials of Informationized Warfare and Information Operations Theory*, pp. 38, 39.

38. This section draws upon Jiang, *Space Operations Teaching Materials*, pp. 126–154.

39. ZHOU Peng and WEN Enbing, "Developing the Theory of Strategic Deterrence with Chinese Characteristics," *China Military Science* (#3, 2004); and Academy of Military Science Military Strategy Research Office, *Science of Military Strategy*, p. 181.

40. LI Jingjun and DAN Yuquan, "The Strategy of Space Deterrence," *China Military Science* (#1, 2002).

41. Academy of Military Science Military Strategy Research Office, *Science of Military Strategy*, p. 181.

42. "Atlas 3 Scrubbed to Tuesday," *Space Daily* (May 21, 2000), http://www.spacedaily.com/news/eutelsat-00g.html; and Jessica Orwig, "A Rocket Launch Monday Was Delayed Because of a Boat," *Business Insider* (October 28, 2014), http://www.businessinsider.com/why-rocket-launch-delayed-by-a-boat-2014-10.

43. JIANG Lianju, *Space Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), p. 137.

44. Ibid., p. 142.

45. Chi and Xiao, *Essentials of Informationized Warfare and Information Operations Theory*, p. 39.

46. HONG Bin and LIANG Xiaoqiu, "The Basics of Space Strategic Theory," *China Military Science* (#1, 2002).

47. LI Dong, ZHAO Xinguo, and HUANG Chenglin, "Research on Concepts of Space Operations and Its Command," *Journal of the Academy of Equipment Command and Technology* (XIV, #5, 2003).

48. MA Ping, *Joint Operations Research* (Beijing, PRC: National Defense University Publishing House, 2013), p. 220.

49. The precise nature of such strategic targets, however, is not defined. Chang, *Military Astronautics*, p. 314.

50. ZHI Tao and LI Wei, "X-37B, the Mysterious Space Fighter," *China Youth Daily* (November 3, 2014), http://jz.chinamil.com.cn/n2014/tp/content_6209028.htm.

51. ZHANG Qinghai and LI Xiaohai, "Space Warfare: From Vision to Reality," *China Military Science* (#1, 2005).

52. Chang, *Military Astronautics*, p. 316.

53. BEI Chao, YANG Jiawei, and ZHANG Wei, "Nanosatellite Distributor Design Proposal," *Zhongguo Hangtian Bao* (August 23, 2002), p. 4, in FBIS-CHI.

54. Chang, *Military Astronautics*, p. 320.

55. XIE Zhaohui and ZHAO Dexi, "On the Fundamental Features of the Military Space Force," *China Military Science* (#1, 2009).

56. Hong and Liang, "The Basics of Space Strategic Theory."

57. Joint Chiefs of Staff, *Space Operations*, JP 3–14 (Washington, DC: Department of Defense, January 6, 2009), p. II-6.

58. Chang, *Military Astronautics*, pp. 304–309.

59. TAN Rukun, *Operational Strength Construction Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2012), p. 170.

60. Academy of Military Science Military Strategy Research Office, *Science of Military Strategy*, p. 181.

61. Jiang, *Space Operations Teaching Materials*, pp. 150–151.

62. Chang, *Military Astronautics*, pp. 306–307.

63. Ian Easton and Mark Stokes, *China's Electronic Intelligence (ELINT) Satellite Developments: Implications for U.S. Air and Naval Operations* (Washington, DC: Project 2049 Institute, 2011), p. 11.

64. Chang, *Military Astronautics*, p. 307.

65. Rui C. Barbosa, "Long March-3B Conducts Another Secretive Launch," NASA Spaceflight (September 12, 2015), http://www.nasaspaceflight.com/2015/09/long-march-3b-conducts-another-secretive-launch/.

66. Chang, *Military Astronautics*, pp. 307–308.

67. Jiang, *Space Operations Teaching Materials*, p. 151.

68. "China Launches First Data Relay Satellite," *Xinhua* (April 26, 2008), http://www.chinadaily.com.cn/china/2008-04/26/content_6645911.htm.

69. Gao, "Aerospace Reconnaissance Characteristics and Limits in High-tech Local Wars."

70. Ibid.; and Xianqi, *Military Astronautics*, p. 308.

71. Chang, *Military Astronautics*, p. 308; and Lianju, *Space Operations Teaching Materials*, pp. 151–152.

72. Chang, *Military Astronautics*, p. 309; and Jiang, *Space Operations Teaching Materials*, p. 152.

73. XU Guoxing, *Research on Our Military's Information Operations Strength Construction* (Beijing, PRC: Military Science Publishing House, 2013), p. 76.

74. Lanzhou Military Region Headquarters Communications Department, "Space Information Support and Its Influence on Future Terrestrial Operations," *Military Art* (#10, 2003).

CHAPTER 7

1. Alice Miller, "The Central Military Commission" in *The PLA as Organization, v. 2.0*, ed. by Kevin Pollpeter and Kenneth W. Allen (Merrifield, VA: DGI International, 2015), p. 96. www.pla-org.com (hereafter *PLA as Organization v2.0*).

2. Drawn from David Finkelstein, "The General Staff Department of the Chinese People's Liberation Army: Organization, Roles, & Missions," in *The People's Liberation Army as Organization*, ed. by James C. Mulvenon and Andrew N.D. Yang (Santa Monica, CA: RAND Corporation, 2002), pp. 122–224 (hereafter *PLA as Organization v1.0*); and Mark Stokes and Ian Easton, "The Chinese People's Liberation Army General Staff Department: Evolving Organization and Mission," in *PLA as Organization v2.0,* pp. 135–161.

3. Drawn from Larry Wortzel, "The General Political Department and the Evolution of the Political Commissar System," in *PLA as Organization v1.0,* pp. 225–246; and Roy Kamphausen, "The General Political Department," in *PLA as Organization v2.0,* pp. 162–173.

4. Drawn from Erin Richter, Leigh Ann Ragland, and Katherine Atha, "General Logistics Department Organizational Reforms: 2000–2012," in *PLA as Organization v2.0,* pp. 172–220; and Susan Puska, "The People's Liberation Army (PLA) General Logistics Department (GLD): Toward Joint Logistics Support" in *PLA as Organization v1.0*, pp. 247–272.

5. Drawn from Harlan Jencks, "The General Armament Department," in *PLA as Organization v1.0,* pp. 273–308, Kevin Pollpeter and Amy Chang, "General Armament Department," in *PLA as Organization v2.0*, pp. 221–258; and China Military Encyclopedia Editorial Committee, *China Military Encyclopedia, Supplemental Volume* (Beijing, PRC: Military Science Publishing House, 2002), pp. 658–659.

6. Stokes and Easton, "The Chinese People's Liberation Army General Staff Department," p. 146, David Finkelstein, "The General Staff Department of the Chinese People's Liberation Army: Organization, Roles, & Missions," in *PLA as Organization v1.0,* p. 155; and Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: Mandiant, 2013), p. 8.

7. Stokes and Easton, "The Chinese People's Liberation Army General Staff Department," pp. 149–150; and Mark Stokes, Jenny Lin, and L.C. Russell Hsiao, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure* (Arlington, VA: Project 2049, 2011), p. 5, http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf.

8. Stokes et al., *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, p. 6.

9. Drawn from Ibid., pp. 7–11, Crowdstrike Global Intelligence Team, "Crowdstrike Intelligence Report: Putter Panda" (Arlington, VA: Crowdstrike, 2014), https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf; and Mark Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure" in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), pp. 170–173.

10. Stokes et al., *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, pp. 8, 11. For a fuller discussion of this bureau and its activities, see Mark Stokes, *The PLA General Staff Department Third Department Second Bureau: An Organizational Overview of Unit 61398* (Arlington, VA: Project 2049, 2015), http://www.project2049.net/documents/Stokes_PLA_General_Staff_Department_Unit_61398.pdf.

11. Crowdstrike Global Intelligence Team, "Crowdstrike Intelligence Report: Putter Panda."

12. ThreatConnect and DGI, "Camerashy: Closing the Aperture on China's Unit 78020" (Arlington, VA: ThreatConnect, 2015), cdn2.hubspot.net/hubfs/454298/Project_CAMERASHY_ThreatConnect_Copyright_2015.pdf.

13. Drawn from Dennis Blasko, *The Chinese Army Today* (London: Routledge, 2006), p. 68; Edward O'Dowd, *Chinese Military Strategy in the Third Indochina War: The Last Maoist War* (New York: Routledge, 2007), p. 171; and Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure," p. 180.

14. Symantec, "Advanced Persistent Threats: A Symantec Perspective" (Mountain View, CA: Symantec, 2011), http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf.

15. Damballa, *Advanced Persistent Threats* (Atlanta, GA: Damballa, 2010), https://www.damballa.com/downloads/r_pubs/advanced-persistent-threat.pdf.

16. Mark Stokes and L.C. Russell Hsiao, *Countering Chinese Cyber Operations: Opportunities and Challenges for US Interests* (Arlington, VA: Project 2049, 2012), p. 4, http://project2049.net/documents/countering_chinese_cyber_operations_stokes_hsiao.pdf.

17. Academy of Military Science Military Strategy Research Office, *The Science of Military Strategy* (Beijing, PRC: Military Science Publishing House, 2013), p. 196.

18. Finkelstein, "The General Staff Department of the Chinese People's Liberation Army," pp. 160–166.

19. Desmond Ball, *Signals Intelligence in the Post-Cold War Era* (Singapore: Institute of Southeast Asian Studies, 1993), p. 50.

20. Stokes and Easton, "The Chinese People's Liberation Army General Staff Department," p. 158; and Finkelstein, "The General Staff Department of the Chinese People's Liberation Army," pp. 168–170.

21. Kamphausen, "The General Political Department."

22. Wortzel, "The General Political Department and the Evolution of the Political Commissar System."

23. Ibid., p. 236. Roy Kamphausen, in his chapter on the GPD, suggests that many of these entities, including the television and movie organizations, are part of the direct work department. Kamphausen, "The General Political Department," p. 170.

24. "A Development History of China's Aerospace Launch Facilities," *Liberation Army Daily* (November 2, 2005), www.jingning.gov.cn/zhxx/zhxx/t20051102_114819.htm.

25. "China's Aerospace Launch Centers," *Xinhuanet* (October 8, 2003), http://news.xinhuanet.com/ziliao/2003-10/08/content_1113971.htm.

26. Brian Harvey, *China's Space Program: From Conception to Manned Spaceflight* (Chichester, UK: Praxis Publishing, 2004), pp. 200–201.

27. Ibid.; and LONG Yuehao, "The Current State and Outlook for Chinese Launcher Systems," *China Aerospace* (August 2004), p. 10.

28. Harvey, *China's Space Program*, pp. 225–226; and Long, "The Current State and Outlook for Chinese Launcher Systems," p. 10.

29. Ibid., pp. 206–208; and John Lewis and Litai Xue, *China's Strategic Seapower* (Stanford: Stanford University Press, 1994), pp. 188–190.

30. "China's Aerospace Launch Centers," *Xinhuanet* (October 8, 2003), http://news.xinhuanet.com/ziliao/2003-10/08/content_1113971.htm.

31. Ibid.

32. Long, "The Current State and Outlook for Chinese Launcher Systems," p. 10.

33. "China's Aerospace Launch Centers," *Xinhuanet* (October 8, 2003), http://news.xinhuanet.com/ziliao/2003-10/08/content_1113971.htm.

34. DENG Liqun, ed., *China Today: Defense Science and Technology*, Vol. I (Beijing, PRC: National Defence Industries Press, 1993), pp. 445–446.

35. "Expert Interview: Xi'an Satellite Telemetry and Control Center as a Reserve Flight Control Center," *Xinhuanet* (October 15, 2005), http://www.sars.gov.cn/chinese/zhuanti/aytk/998964.htm.

36. Harvey, *China's Space Program*, pp. 183–185; and Deng, *China Today*, pp. 428–430, 442–446.

37. Deng, *China Today*, p. 428.

38. "Expert Interview: Xi'an Satellite Telemetry and Control Center as a Reserve Flight Control Center," *Xinhuanet* (October 15, 2005), http://www.sars.gov.cn/chinese/zhuanti/aytk/998964.htm.

39. YUAN Sanhu, "Our Country's Aerospace Tracking and Control Network Realizes a 'Large Triangle' Distribution," *Xinhua* (April 25, 2008), http://www.chinamil.com.cn/site1/xwpdxw/2008-04/25/content_1220073.htm.

40. "The Survey Troops behind 'Change'," *China Survey Newspaper* (October 30, 2007), http://www.sbsm.gov.cn/article//ztzl/chdf/200710/20071000003834.shtml.

41. This section draws from "Academy of Command Equipment and Technology," in *An Overview of Chinese Military Academies and Schools*, ed. by JIN Peng and DONG Ming (Beijing, PRC: Military Science Publishing House, 2002), p. 163.

42. Gao, *Joint Campaign Course Materials*, p. 34.

43. ZHANG Yuliang, Chief Editor, *The Science of Campaigns* (Beijing, PRC: National Defense University Publishing House, 2006), pp. 282–283.

44. YUAN Wenxian, *Joint Operations Command Office Work Teaching Materials* (Beijing, PRC: National Defense University Publishing House, 2008), pp. 208–211; and

LI Yousheng, *Science of Joint Campaign Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2012), pp. 154–155.

45. CAO Zhi, LI Xuanliang, and WANG Shibing, "Xi Jinping: Comprehensively Implement the Strategy of Reforming and Strengthening the Military, Firmly and Unswervingly Holding to the Path of a Strong Army with Chinese Characteristics," *Xinhuanet* (November 26, 2015), http://politics.people.com.cn/n/2015/1126/c1024-27860788.html.

46. LI Xuanliang, ZHANG Xuanjie, and LI Qinghua, "Establishment Ceremony for the Ground Forces Command, Strategic Support Force, Rocket Force Is Held in Beijing," *People's Daily* (January 2, 2016), http://politics.people.com.cn/n1/2016/0102/c1024-28003584.htm.

47. QIU Yue, "Expert: Strategic Support Force Will Permeate the Entire Course of Operations, Is a Key Factor in Achieving Victory," *People's Net* (January 5, 2016), http://military.people.com.cn/n1/2016/0105/c1011-28011251.html.

48. "CMC Offices Become 15 Functional Departments," *China Youth Daily* (January 12, 2016), http://politics.people.com.cn/n1/2016/0112/c70731-28039781.html.

49. LI Xuanliang, "Establishment Ceremony for People's Liberation Army War Zones Held in Beijing," *Xinhuanet* (February 1, 2016), http://military.china.com/important/11132797/20160201/21395968_all.html#page_2.

CHAPTER 8

1. YUAN Peng, "China's Strategic Opportunity Period Has Not Ended," *People's Daily Online* (July 31, 2012), http://en.people.cn/90883/7893886.html; XU Jian, "New Changes in the Next Decade of China's Period of Strategic Opportunity," *Guangming Ribao* (October 30, 2013), http://cpc.people.com.cn/n/2013/1030/c83083-23372744.html; and ZHANG Yunling, "Deeply Considering the International Environment Confronting Our Nation's Period of Strategic Opportunity," *Seeking Truth* (December 18, 2015), http://theory.people.com.cn/n1/2015/1218/c83846-27946374.html.

2. Eric W. Orts, "The Rule of Law in China," *Vanderbilt Journal of Transnational Law* (January 2001).

3. Murray Scot Tanner, *The Politics of Lawmaking in China* (Oxford, UK: Clarendon Press, 1999), p. 43; and Dwight Perkins, "Law, Family Ties, and the East Asian Way of Business," in *Culture Matters*, ed. by Lawrence E. Harrison and Samuel P. Huntington (New York: Basic Books, 2000), p. 235.

4. It is useful to examine the evolution of this joint publication, from the 1998 version (then entitled *Joint Doctrine for Information Operations*), through the 2006, 2012, and 2014 revisions. Joint Chiefs of Staff, *Information Operations*, Joint Publication 3–13 (Washington, DC: Office of the Joint Chiefs of Staff, 2014), http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

5. Paul Day, *CyberAttack* (London, UK: Carlton Books, 2014), p. 188.

6. Wayne Morrison, *China–U.S. Trade Issues*, CRS Report RL33536 (Washington, DC: Congressional Research Service, 2015), p. 8, https://www.fas.org/sgp/crs/row/RL33536.pdf.

7. Steven Millward, "Support for Windows XP Is Over, but China Still Has 200 Million PCs Using It," *Tech in Asia* (April 9, 2014), https://www.techinasia.com/windows-xp-now-dead-but-200-million-machines-in-china-still-using-it.

8. Bill Rigby and Paul Carsten, "Microsoft Tackles China Piracy with Free Upgrade to Windows 10," *Reuters* (March 18, 2015), http://www.reuters.com/article/us-microsoft-china-idUSKBN0ME06A20150318.

9. Michael Martina, "China Withholds Full Domestic-Security Spending Figure," *Reuters* (March 4, 2014), http://www.reuters.com/article/us-china-parliament-security-idUSBREA240B720140305.

10. Report on the Implementation of the 2015 National and Local Budgets and the Draft of the 2016 National and Local Budgets (Essentials), *Xinhuanet* (March 5, 2016), http://news.xinhuanet.com/politics/2016lh/2016-03/05/c_1118243992.htm.

11. Mike Ahlers, "World War II-Era Navigation System Shut Down," *CNN* (February 8, 2010), http://www.cnn.com/2010/TECH/02/08/loran.navigation.shutdown/.

12. Andrea Peterson, "Why Naval Academy Students Are Learning to Sail by the Stars for the First Time in a Decade," *Washington Post* (February 17, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/02/17/why-naval-academy-students-are-learning-to-sail-by-the-stars-for-the-first-time-in-a-decade/.

This page intentionally left blank

Bibliography

Abbreviations used in the Bibliography:

AMS	Academy of Military Science
CMS	*China Military Science*
CNDN	*China National Defense Newspaper*
FBIS-CHI	Foreign Broadcast Information Service (China)
JAECT	*Journal of the Academy of Equipment Command and Technology*
LAPH	Liberation Army Publishing House
MSPH	Military Science Publishing House
ND	*National Defense* magazine
NDIP	National Defense Industry Press
NDS&T	*National Defense Science and Technology*
NDUPH	National Defense University Publishing House
NYT	*New York Times*
PLAD	*People's Liberation Army Daily*
PN	*People's Net*
WP	*Washington Post*

Note:

Books or articles originally in Chinese are *italicized*.
Books or articles originally in English are ***bold italicized***.
Papers and testimonies are in plain text.
Chinese authors are listed LAST NAME, First Name.
Western authors are listed Last Name, First Name.

"Advanced Persistent Threats: How They Work," Symantec (Undated), http://www.symantec.com/theme.jsp?themeid=apt-infographic-1.

Ahlers, Mike, "World War II-Era Navigation System Shut Down," ***CNN*** (February 8, 2010), http://www.cnn.com/2010/TECH/02/08/loran.navigation.shutdown/.

Ahrens, Nathaniel, ***National Security and China's Information Security Standards***, CSIS (Washington, DC: Center for Strategic and International Studies, 2012).

All Army Military Terminology Management Commission (PRC), *Chinese People's Liberation Army Terminology* (Unabridged Volume) (Beijing, PRC: MSPH, 2011).

Alperovich, Dmitri, ***Deep in Thought: Chinese Targeting of National Security Think-Tanks***, Crowdstrike (July 7, 2014), http://www.crowdstrike.com/blog/deep-thought-chinese-targeting-national-security-think-tanks/.

Amin, Suril, "The People's Republic of China Will Stick with Windows XP," Microsoft News (April 23, 2014), http://microsoft-news.com/the-peoples-republic-of-china-will-stick-with-windows-xp/.

AMS Military Strategy Research Office (PRC), *The Science of Military Strategy* (Beijing, PRC: MSPH, 2013).

AMS Operations Theory and Regulations Research Department and AMS Informationized Operations Theory Research Office (PRC), *Informationized Operations Theory Study Guide* (Beijing, PRC: MSPH, November, 2005).

AMS Strategies and Campaigns Department (PRC), "New Developments in Campaign Theory," *Military Art* (#4, 1999).

"Announcement: Interim Regulations Regarding the Management and Development of Public Messaging Information Services," *Xinhua* (August 7, 2014), http://news.xinhuanet.com/2014-08/07/c_1111979566.htm.

Arkin, William M. "The Cyberbomb in Yugoslavia," ***WP*** (October 25, 1999), http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm.

Arsene, Severine, "The Impact of China on Global Internet Governance in an Era of Privatized Control," Paper presented at the 10th Annual Chinese Internet Research Conference (May 2012), https://hal.archives-ouvertes.fr/hal-00704196v2/document.

Art, Robert, editor, ***The Use of Force***, 3rd Edition (New York: University Press of America, 1988).

"Atlas 3 Scrubbed to Tuesday," ***Space Daily*** (May 21, 2000), http://www.spacedaily.com/news/eutelsat-00g.html.

Austin, Greg, ***Cyber Policy in China*** (Malden, MA: Polity Press, 2014).

BAI Bangxi and JIANG Lijun, "Systems of Systems Conflict Is Not the Same as Systems Conflict," *CNDN* (January 10, 2008), http://www.chinamil.com.cn/site1/xwpdxw/2008-01/10/content_1084469.htm.

BAI Suixue and WANG Jingguo, "National Defense White Paper Published, Describing the New Era Active Defense Military Strategic Guideline," *Xinhuanet* (January 20, 2009), http://news.xinhuanet.com/newscenter/2009-01/20/content_10689962.htm.

Baldwin, Clare, Pomfret, James, and Wagstaff, Jeremy, "On China's Fringes, Cyber Spies Raise Their Game," ***Reuters*** (November 30, 2015), http://www.reuters.com/article/us-cybersecurity-hongkong-insight-idUSKBN0TI0WF20151130.

Ball, Desmond, ***Signals Intelligence in the Post-Cold War Era*** (Singapore: Institute of Southeast Asian Studies, 1993).

Bamman, David, O'Connor, Bredan, and Smith, Noah, "Censorship and Deletion Practices in Chinese Social Media," ***First Monday*** (XVII, 3, March 5, 2012), http://firstmonday.org/article/view/3943/3169.

Bandurski, David, "Chinese Media Muzzled after Day of Glory," ***China Media Project*** (July 31, 2011), http://cmp.hku.hk/2011/07/31/14332/.

Bandurski, David, "Lu Wei: The Internet Must Have Brakes," ***China Media Project*** (September 11, 2014), http://scmp.hku.hk/2014/09/11/36011/.

Barbosa, Rui C., "Long March-3B Conducts Another Secretive Launch," ***NASA Spaceflight*** (September 12, 2015), http://www.nasaspaceflight.com/2015/09/long-march-3b-conducts-another-secretive-launch/.

BEI Chao, YANG Jiawei, and ZHANG Wei, "Nanosatellite Distributor Design Proposal," *China Aerospace Newspaper* (August 23, 2002), p. 4, in ***FBIS-CHI***.

Beijing University Office of Informationization Construction and Management, "Announcement Regarding the Promulgation of 'Implementing Views Regarding Information Security Classification Work'," Public Announcement #66 (for 2004) (September 15, 2004), http://oi.pku.edu.cn/xxaq/xxaqdjbh/22572.htm.

Bellovin, Steven M., ***Thinking Security*** (New York: Addison-Wesley, 2016).

Bissell, Benjamin, "More Tightening of Internet Restrictions by China," Lawfare blog.com (September 23, 2014), https://www.lawfareblog.com/more-tightening-internet-restrictions-china.

Blanchard, Ben, "China Takes Step at Openness, Allows Foreigners at Defense Briefing," ***Reuters*** (July 31, 2014), http://www.reuters.com/article/2014/07/31/us-china-defence-idUSKBN0G011K20140731.

Blanchard, Ben, "China's Effort to Muzzle News of Train Crash Sparks Outcry," ***Reuters*** (July 25, 2011), http://www.reuters.com/article/2011/07/25/us-china-train-censorship-idUSTRE76O1IG20110725.

Blasko, Dennis J., ***The Chinese Army Today*** (New York: Routledge Press, 2006).

Borger, Julian, "Pentagon Kept the Lid on Cyberwar in Kosovo," ***The Guardian*** (UK) (November 8, 1999), http://www.guardian.co.uk/world/1999/nov/09/balkans.

Borland, Sophie, "MI-5 Warns Firms over China Internet 'Spying'," ***Daily Telegraph*** (April 12, 2008), http://www.telegraph.co.uk/news/worldnews/1571172/MI5-warns-firms-over-Chinas-internet-spying.html.

Boswell, Matthew, "Media Relations in China's Military: The Case of the Ministry of National Defense Information Office," ***Asia Policy*** (#8, Jul 2009).

Brantly, Aaron F., "Strategic Cyber Maneuver," ***Small Wars Journal*** (October 17, 2015), http://smallwarsjournal.com/jrnl/art/strategic-cyber-maneuver.

Bright, Peter, "How Security Flaws Work: The Buffer Overflow," ***Ars Technica*** (August 25, 2015), http://arstechnica.com/security/2015/08/how-security-flaws-work-the-buffer-overflow/.

Brumfeld, Ben, "Study: China Cybercensors Attack Outside Its Borders with 'Great Cannon'," ***CNN*** (April 12, 2015), http://www.cnn.com/2015/04/12/china/china-cyber-censorship-weapon/.

Buckley, Chris, "China Train Crash Censorship Scorned on Internet," ***Reuters*** (August 1, 2011), http://www.reuters.com/article/2011/08/01/us-china-train-censorship-idUSTRE7700ET20110801.

Burns, John F., "China Plans More Manpower Cuts in the Military," ***NYT*** (January 4, 1985), http://www.nytimes.com/1985/01/04/world/china-plans-more-manpower-cuts-in-the-military.html.

CAO Zhi, LI Xuanliang, and WANG Shibing, "Xi Jinping: Comprehensively Implement the Strategy of Reforming and Strengthening the Military, Firmly and Unswervingly Holding to the Path of a Strong Army with Chinese Characteristics," *Xinhuanet* (November 26, 2015), http://politics.people.com.cn/n/2015/1126/c1024-27860788.html.

Carsten, Paul, "China Scrambles to Censor Social Media," ***Reuters*** (September 29, 2014), http://www.huffingtonpost.com/2014/09/29/china-social-media_n_5901362.html.

"Cat and Mouse," ***The Economist*** (April 6, 2013), http://www.economist.com/news/special-report/21574629-how-china-makes-sure-its-internet-abides-rules-cat-and-mouse.

"Central Military Commission Offices Become 15 Functional Departments," *China Youth Daily* (January 12, 2016), http://politics.people.com.cn/n1/2016/0112/c70731-28039781.html.

"C4ISR Technology Innovation Team: 'War Will Not Wait Until We Are Mature to Occur'," *Seeking Truth* (August 19, 2011), http://big5.qstheory.cn/dd/2011/ypgf/201108/t20110819_103443.htm.

"C4ISR Technology Innovation Teams: Won't Suffer Hits in Future Wars," National University of Defense Technology (PRC) Web-site (July 27, 2011), http://www.cnr.cn/junshi/ztl/gfkd/burm/201107/t20110727_508291369.html.

Chang, Amy, ***Warring State: China's Cybersecurity Strategy*** (Washington, DC: Center for a New American Security, 2014), http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WarringState_Chang_report_010615.pdf.

CHANG Long, "Tightly Grasping the Trends of the New Military Transformation—Reflections and Outlook from the Gulf War to the Iraq War," *PLAD* (October 28, 2003), http://www.xslx.com/htm/gjzl/jsgc/2003-10-38-15176.htm.

CHANG Ming, "Discussing 'Air Dominance' and 'Network and Electromagnetic Spectrum' Dominance," *PLAD* (October 29, 2002).

CHANG Xianqi, *Military Astronautics*, 2nd ed. (Beijing, PRC: NDIP, 2005).

CHE Xianming and WANG Wei, "Key Guidance on Informationized Operations," *CMS* (#5, 2004).

CHEN Bing, QIAN Hongyan, and HU Jie, *Network Security* (Beijing, PRC: NDIP, 2012).

CHEN Zhou, "A Comparison of Chinese Modern Local War Theory and American Limited War Theory," *CMS* (#2, 2002).

CHEN Zhou, "On the Development of China's Defense National Defense Policy in the new Situation," *CMS* (#6, 2009).

CHENG Xuan and WANG Jiasheng, "Examining America's 'Sensor to Shooter' Combat Style," *China Aerospace* (#11, 2003).

CHEUNG, Anne S.Y., and ZHAO Yun, "An Overview of Internet Regulation in China," University of Hong Kong Faculty of Law Research Paper #2013/040 (November 21, 2013), http://ssrn.com/abstract=2358247.

CHI Yajun and XIAO Yunhua, Chief Editors, *Essentials of Informationized Warfare and Information Operations Theory* (Beijing, PRC: MSPH, 2005).

Chin, Josh, "Cyber Sleuths Track Hacker to China's Military," ***Wall Street Journal*** (September 13, 2015), http://www.wsj.com/articles/cyber-sleuths-track-hacker-to-chinas-military-1443042030.

"China Censors May Have Caused Huge Internet Outage," ***AFP*** (January 22, 2014), http://phys.org/print309592839.html.

"China Employs Two Million Microblog Monitors, State Media Say," ***BBC News*** (October 4, 2013), http://www.bbc.com/news/world-asia-china-24396957.

China Internet Network Information Center, ***Statistical Report on Internet Development in China*** (January 2014).

"China Launches First Data Relay Satellite," *Xinhua* (April 26, 2008), http://www.chinadaily.com.cn/china/2008-04/26/content_6645911.htm.

"China Military Aerospace Equipment Has a Vital Role in Forging Strategic Deterrence," *Xinhuanet* (May 20, 2007), http://news.xinhuanet.com/politics/2007-05/20/content_6125528.htm.

"China: Missile Defense System Test Successful," ***USAToday*** (January 11, 2010), http://www.usatoday.com/news/world/2010-01-11-china-missile-defense_N.htm.

"China Said to Plan Sweeping Shift from Foreign Technology to Own," ***Bloomberg News*** (December 17, 2014), http://www.bloomberg.com/news/articles/2014-12-17/china-said-to-plan-sweeping-shift-from-foreign-technology-to-own?hootPostID=f047ce391d1e79bebf8d0f1b50ed2a0d.

"China Sets Up Office for Internet Information Management," ***Xinhuanet*** (May 4, 2011), http://news.xinhuanet.com/english/2010/china/2011-05/04/c_138579.htm.

"China's Aerospace Launch Centers," *Xinhuanet* (October 8, 2003), http://news.xinhuanet.com/ziliao/2003-10/08/content_1113971.htm.

"China's C3I Systems," *PLAD* (July 31, 2003), http://jczs.sina.com.cn/2003-07-31/140848.html.

"China's Cyber Security Under Severe Threat: Report," ***Xinhua*** (March 19, 2013), http://news.xinhuanet.com/English/china/2013-03/19/c_132246098.htm.

Chinese Communist Party Central Committee General Office and State Council General Office, "Announcement of '2006–2020 National Informationization Development Strategy'" (March 19, 2006), http://oi.pku.edu.cn/jsgh/ghgy/22527.htm.

Chinese Military Encyclopedia Committee, *Chinese Military Encyclopedia*, various volumes (Beijing, PRC: MSPH, July 1997).

Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia,* 2nd Edition, various volumes (Beijing, PRC: China Encyclopedia Publishing House, 2007).

Chinese War Mobilization Encyclopedia Editorial Committee, *Chinese War Mobilization Encyclopedia* (Beijing, PRC: MSPH, 2003).

Clark, Liat, "Chinese Military 'Hacked' Israel's Iron Dome," ***Wired*** (July 29, 2014), http://www.wired.co.uk/news/archive/2014-07/29/iron-dome-tech-stolen.

Clarke, Richard A., and Knake, Robert K., ***Cyber War*** (New York: Ecco Publishing, 2010).

Command and Control in the Information Era: Proceedings of the 2014 Maritime Command & Control, and Firepower and Command & Control Studies Annual Conference (Beijing, PRC: NDIP, 2014).

Crandall, Jed, and Wallach, Dan, "The Astonishing Speed of Chinese Censorship," ***BBC News*** (March 27, 2013), http://www.bbc.com/news/world-asia-china-21743499.

Crowdstrike Global Intelligence Team, ***Crowdstrike Intelligence Report: Putter Panda***, Crowdstrike (Arlington, VA: Crowdstrike, 2014), https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf.

CUI Shizeng and WANG Junyi, "Advancing Military Transformation with Chinese Characteristics, Strengthening 'Integrated-Style Joint Operations," *PLAD* (July 7, 2004), http://news.xinhua.net.com/mil/2004-07/07/content_1578870.htm.

DAI Qingmin, "Innovating and Developing Views on Information Operations," *CMS* (#8, 2000), pp. 72–77, in ***FBIS-CHI.***

DAI Qingmin, "On Integrating Network Warfare and Electronic Warfare," *CMS* (#2, 2002), pp. 112–117, in ***FBIS-CHI.***

Damballa, ***Advanced Persistent Threats***, Damballa (Atlanta, GA: Damballa, 2010), https://www.damballa.com/downloads/r_pubs/advanced-persistent-threat.pdf.

David, Leonard, "China's Antisatellite Test: Worrisome Debris Cloud Encircles Earth," Space.com (February 2, 2007), http://www.space.com/3415-china-anti-satellite-test-worrisome-debris-cloud-circles-earth.html.

Day, Paul, ***CyberAttack*** (London, UK: Carlton Books, 2014).

Defense Intelligence Agency (U.S.), Intelligence Information Report, ***PLA Modernizes Its Military Training Program***, June 23, 1995, http://nsarchive.gwu.edu/NSAEBB/NSAEBB39/document13.pdf.

"Defense Ministry: 'Mission Action-2013' Exercise Is Typical Training Activities," *China Newsnet* (September 26, 2013), http://www.chinanews.com/mil/2013/09-26/5327377.shtml.

"Defense Ministry Spokesman Explains Why the War Zones Have Been Entirely Adjusted and Redrawn," *PN* (February 1, 2016), http://military.people.com.cn/n1/2016/0201/c1011-28102649.html.

Deibert, Ronald, Palfrey, John, Rohozinski, Rafal, and Zittrain, Jonathan, editors, ***Access Contested: Security, Identity, and Resistance in Asian Cyberspace*** (Cambridge, MA: MIT Press, 2011).

DENG Liqun, editor, ***China Today: Defense Science and Technology***, Vol. I (Beijing, PRC: National Defence Industries Publishing House, 1993).

DENG Xiaoping, "Peace and Development Are the Two Outstanding Issues in the World Today," Remarks to a visiting delegation of the Japanese Chamber of Commerce and Industry (March 4, 1985), http://en.people.cn/dengxp/vol3/text/c1330.html.

DENG Yifei, "A Transformation in Military Thinking in the Information Age," *CMS* (#6, 2007).

Denyer, Simon, and XU Yangjingjing, "Unable to Clean Air Completely for APEC, China Resorts to Blocking Data," ***WP*** (November 10, 2014), https://www.washingtonpost.com/news/worldviews/wp/2014/11/10/unable-to-clean-air-completely-for-apec-china-resorts-to-blocking-data/.

"A Development History of China's Aerospace Launch Facilities," *PLAD* (November 2, 2005), www.jingning.gov.cn/zhxx/zhxx/t20051102_114819.htm.

DING Jianjun and ZHANG Kunping, "A Certain Technical Unit of the Beijing MR Develops Joint Repair Bases on the 'Battlefield'," *PLAD* (June 26, 2004).

DING Jun, "Central Network Security and Informationization LSG Established by Xi Jinping: Building a Strong Network Nation," 21st Century Financial Reporting (February 28, 2014), http://finance.sina.com.cn/chanjing/cyxw/20140228/023818359508.shtml.

Director for Joint Force Development J-7 (U.S.), ***Department of Defense Dictionary of Military and Associated Terms***, JP 1–02 (Washington, DC: Pentagon, 2015).

DONG Chongmin, *Research on Non-Linear Operations* (Beijing, PRC: LAPH, 2005).

DONG Wentao and JIE Jianshe, "Integrated Mobilization under Information Warfare Conditions," *PLAD* (June 7, 2004).

Dou, Eva, "The Obscure Chinese Operating System Sold by Dell, HP," ***Wall Street Journal*** (September 15, 2015), http://blogs.wsj.com/chinarealtime/2015/09/15/the-obscure-chinese-operating-system-sold-by-dell-hp/.

Dunlap, Charles J., Jr., "Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts," Working Paper, Carr Center for Human Rights, Harvard University Kennedy School of Government (Cambridge, MA; November 29, 2001).

Earnshaw, Graham, ***China Economic Review's China Business Guide 2005*** (Shanghai, PRC: SinoMedia Holdings, 2005).

Easton, Ian, and Stokes, Mark, ***China's Electronic Intelligence (ELINT) Satellite Developments: Implications for U.S. Air and Naval Operations*** (Washington, DC: Project 2049 Institute, 2011).

Einhorn, Bruce, "A Cybersecurity Law in China Squeezes Foreign Tech Companies," ***Bloomberg News*** (January 21, 2016), http://www.bloomberg.com/news/articles/2016-01-21/a-cybersecurity-law-in-china-squeezes-foreign-tech-companies.

Elisan, Christopher C., ***Malware, Rootkits, & Botnets*** (New York: McGraw-Hill, 2013).

Ermert, Monika, "ITU Secretary General Visits Old Arch-Rival IETF," ***Intellectual Property Watch*** (July 21, 2015), http://www.ip-watch.org/2015/07/21/itu-secretary-general-visits-old-arch-rival-ietf/.

Ernst, Dieter, and Martin, Sheri, "The Common Criteria for Information Technology Security Evaluation—Implications for China's Policy on Information Security Standards," East-West Center Report #108 (Honolulu, HI: East-West Center, 2010).

Espiner, Tom, "Security Experts Lift Lid on Chinese Hack Attacks," ***ZDNet*** (November 23, 2005), http://www.zdnet.com/article/security-experts-lift-lid-on-chinese-hack-attacks/.

"Establishment of the Central Network Security and Informationization Leading Small Group," *Xinhuanet* (February 27, 2014), http://news.xinhuanet.com/politics/2014-02/27/c_119538719.htm.

"Examining Four Major Post-Cold War Russian Conflicts," *PLAD* (December 27, 2014), http://news.sciencenet.cn/htmlnews/2014/12/310146.shtm.

"Expert Interview: Xi'an Satellite Telemetry and Control Center as a Reserve Flight Control Center," *Xinhuanet* (October 15, 2005), http://www.sars.gov.cn/chinese/zhuanti/aytk/998964.htm.

FAN Gaoming, "Public Opinion Warfare, Psychological Warfare, and Legal Warfare, the Three Major Combat Methods to Rapidly Achieving Victory in War," *Global Times* (March 8, 2005), http://big5.xinhuanet.com/gate/big5/news.xinhuanet.com/mil/2005-03/08/content_2666475.htm.

FAN Gaoyue and FU Linguo, *The First Conflict to Display Initial Informationization Conditions: The Iraq War* (Beijing, PRC: MSPH, 2008).

FAN Xuejun, "Militarily Strong Nations Are Steadily Developing 'Space Information Warfare'," *PLAD* (April 13, 2005).

FANG Qiuming, "Four Major Development Trends Derived from Observing Modern Warfare in the Iraq War," *ND* (#9, 2009).

Faris, Robert, Roberts, Hal, and Wang, Stephanie, ***China's Green Dam: The Implications of Government Control Encroaching on the Home PC***, Open Net Initiative Bulletin (June 2009), http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc.

Federal Communications Commission (U.S.), Notice of Apparent Liability and Forfeiture, Illegal Marketing of Signal Jamming Devices, File Number: EB-SED-12-00005692 (June 19, 2014), http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db0619/FCC-14-92A1.pdf.

Feigenbaum, Evan, ***China's Techno-Warriors*** (Stanford: Stanford University Press, 2003).

FENG Shuxing and CUI Yang, "Research Questions on Space Operations Command Structures," *JAECT* (XV, #1, February, 2004).

Finkle, Jim, "Beijing to Bar Kaspersky, Symantec Anti-Virus in Procurement: Report," ***Reuters*** (August 3, 2014), http://www.reuters.com/article/2014/08/03/us-china-software-ban-idUSKBN0G30QH20140803.

Foreign Correspondents Club of China, ***Position Paper on Working Conditions for Foreign Correspondents in China*** (September 12, 2014), http://www.fccchina.org/2014/09/12/fccc-position-paper-2014/.

"Foreign Tech Firms Pose Threat on Internet," *China Daily* (June 4, 2014), http://en.people.cn/n/2014/0604/c207959-8736319.html.

"Four Methods of Information Warfare That Are under Consideration," *PLAD* (June 1, 2006), http://www.china.com.cn/chinese/junshi/1226095.htm.

Frayvel, Taylor, ***Strong Borders, Secure Nation*** (Princeton: Princeton University Press, 2008).

FU Quanyou, "Deepen the Study of the Characteristics and Laws of High-Technology Local War and Raise the Standard of Guidance for Winning High-Technology Local War of the Future," *CMS* (February 1999), in ***FBIS-CHI***.

Gallagher, Sean S., "Newly Discovered Chinese Hacking Group Hacked 100+Websites to Use as 'Watering Holes'," ***Ars Technica*** (August 5, 2013), http://arstechnica.com/security/2015/08/newly-discovered-chinese-hacking-group-hacked-100-websites-to-use-as-watering-holes/.

GAO Qingjun, "Aerospace Reconnaissance Characteristics and Limits in High-Tech Local Wars," *JAECT* (XVI, #1, February 2005).

GAO Yubiao, Chief Editor, *Joint Campaign Course Materials* (Beijing, PRC: MSPH, August 2001).

Garrity, Patrick J., ***Why the Gulf War Still Matters***, Report #16 (Los Alamos, NM: Center for National Security Studies, Los Alamos National Laboratory, 1993), http://www.osti.gov/scitech/servlets/purl/10178236.

"General Staff Department Military Training Expert: Fighting and Winning Requires First Simulating Fighting," *Xinhuanet* (September 26, 2014), http://military.people.com.cn/n/2014/0926/c172467-25740468.html.

"General Zhang Qinsheng Discusses the Strategic Thought of the Active Defense," *Study Times* (July 18, 2011), http://news.xinhuanet.com/mil/2011-07/18/c_121682519.htm.

Gierow, Hauke Johannes, "Cyber Security in China: New Political Leadership Focuses on Boosting National Security," Mercator Institute for China Studies (#20, December 9, 2014).

Google, "A New Approach to China," Google Official Blog (January 12, 2010), https://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

Gourley, Bob, ***The Cyber Threat*** (2014). Thecyberthreat.com.

Graham, Robert, "Pinpointing China's Attack against GitHub," ***Errata Security*** (April 1, 2015), http://blog.erratasec.com/2015/04/pin-pointing-chinas-attack-against.html#.VSvhdJTF8nh.

"Great Firewall 'Upgrade' Troubles VPN Users in China," ***AFP*** (December 21, 2012), http://www.securityweek.com/great-firewall-upgrade-troubles-vpn-users-china.

Greenemeier, Larry, "China's Cyber Attacks Signal New Battlefield Is Online," ***Scientific American*** (September 18, 2007), http://www.scientficamerican.com/article/chinas-cyber-attacks-sign/.

Griffiths, James, "White House Should Threaten Great Firewall to Curb Chinese Cyber Attacks, Experts Say as Obama-Xi Summit Nears," ***South China Morning Post*** (August 28, 2015), http://www.scmp.com/tech/enterprises/article/1853235/white-house-must-threaten-great-firewall-any-hope-curbing-chinas.

Gross, Jon, and Cylance SPEAR Team, "Operation Dust Storm," ***Cylance*** (2016), https://www.cylance.com/hubfs/2015_cylance_website/assets/operation-dust-storm/Op_Dust_Storm_Report.pdf?t=1456276906648.

Gruss, Mike, "Space Surveillance Satellites Pressed into Early Service," ***Space News*** (September 18, 2015), http://spacenews.com/space-surveillance-sats-pressed-into-early-service/.

GUAN Weiqiang, QIN Daguo, and XIAO Lianggang, "Research on Requirements for Aerospace TT&C Systems for Integrated-Style Joint Operations," *JAECT* (XVII, #6, 2006).

GUO Jian, *60 Examples of Electronic Warfare Activities* (Beijing, PRC: LAPH, 2007).

GUO Liang, ***Under the Golden "Shine": China's Effort to Bridge Government and Citizens*** (Beijing, PRC: Chinese Academy of Social Sciences, January 2006), http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan042815.pdf.

GUO Ruobing, *Discussions of Military Information Security* (Beijing, PRC: NDUPH, 2013).

GUO Yanhua, *Study Volume on Psychological Warfare* (Beijing, PRC: NDUPH, 2005).

HAN Yanrong, "Legal Warfare: Military Legal Work's High Ground: An Interview with Chinese Politics and Law University Military Legal Research Center Special Researcher Xun Dandong," *Legal Daily* (PRC) (February 12, 2006).

Hannas, William C., Mulvenon, James, and Puglisi, Anna B., ***Chinese Industrial Espionage*** (New York: Routledge Press, 2013).

HAO Weixue, editor, *Psychological Warfare: Discussion of 100 Examples and Solutions* (Beijing, PRC: LAPH, 2004).

Harrison, Lawrence E., and Huntington, Samuel P., editors, ***Culture Matters*** (New York: Basic Books, 2000).

Hartnett, Daniel, ***Towards a Globally Focused Chinese Military: The Historic Missions of the Chinese Armed Forces*** (Alexandria, VA: CNA Corporation, 2008).

Harvey, Brian, ***China's Space Program: From Conception to Manned Spaceflight*** (Chichester, UK: Praxis Publishing, 2004).

HE Qingcheng, "Combat Command Capability: The Core of Military Capability's 'Core,'" *PLAD* (September 10, 2009), http://news.mod.gov.cn/edu/2009-09/10/content_4086660.htm.

HE Zhu, *Experts Assess the Iraq War* (Beijing, PRC: MSPH, 2004).

Helft, Miguel, "YouTube Blocked in China, Google Says," ***NYT*** (March 25, 2009), https://www.nytimes.com/2009/03/25/technology/internet/25youtube.html.

Hermann-Seaton, Penny, "Security Features in IPv6," SANS Institute Reading Room (2002), https://www.sans.org/reading-room/whitepapers/protocols/security-features-ipv6-380.

Hersh, Seymour, "King's Ransom: How Vulnerable Are the Saudi Royals," ***New Yorker*** (September 22, 2001).

Hesketh, Roger, ***Fortitude: The D-Day Deception Campaign*** (Woodstock, NY: Overlook Publishers, 2000).

Hjortdal, Magnus, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," ***Journal of Strategic Security*** (IV, #2, Summer 2011).

Holmes, James, "China's Underground Great Wall," ***The Diplomat*** (August 20, 2011), http://thediplomat.com/2011/08/chinas-underground-great-wall/.

HONG Bin and LIANG Xiaoqiu, "The Basics of Space Strategic Theory," *CMS* (#1, 2002).

"How to Steal a Trillion," ***The Economist*** (February 19, 2013).

Hsiao, Russell, "China's Underground 'Great Wall' and Nuclear Deterrence," ***Jamestown Foundation China Brief*** (December 16, 2009), http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews[tt_news]=35846&tx_ttnews[backPid]=459&no_cache=1.

HU Guangming, *Military Informationization Construction Teaching Materials* (Beijing, PRC: MSPH, 2012).

HU Guangzheng, "Melded Civil-Military Development: A Major Strategic Thought on the Overall Planning of National Defense and Economic and Social Development," *CMS* (#1, 2009).

HU Jintao, "Understanding Our Military's New Historic Missions in the New Phase of the New Century," Jiangxi Defense Education Network website (December 24, 2004), http//gfjy.jxnews.com.cn/system/2010/04/16/011353408.shtml.

HU Tianjiang and HUANG Gang, *"PRC National Defense Mobilization Law" Study Questions and Answers* (Beijing, PRC: NDUPH, 2010).

HUANG Renquan and LI Weimin, "The Impact of Expanding the Air Defense Conflict Battlefield to the Network-Electronic Space on Future National Air Defense," *NDS&T* (PRC) (#3, 2012).

HUANG Xing and ZUO Quandian, "Holding the Initiative in Our Hands in Conducting Operations, Giving Full Play to Our Own Advantages to Defeat Our Enemy," *CMS* (4, 1996), in ***FBIS-CHI***.

"Information Strength: The Key Factor Determining Victory or Defeat in Informationalized Warfare," *PLAD* (January 28, 2005), http://www.it.com.cn/f/news/051/28/74245.htm.

Information Warfare Monitor, "Tracking GhostNet: Investigating a Cyber-Espionage Network" (March 29, 2009), https://www.f-secure.com/weblog/archives/ghostnet.pdf.

International Corporation for the Assignment of Names and Numbers, "Beginner's Guide to ICANN," ICANN (Los Angeles, CA: ICANN, 2013), https://www.icann.org/en/system/files/files/participating-08nov13-en.pdf.

International Institute for Strategic Studies, ***The Military Balance 1981–1982*** (New York: Facts on File, 1981).

International Institute for Strategic Studies, ***The Military Balance 1985–1986*** (London, UK: IISS, 1985).

International Institute for Strategic Studies, ***The Military Balance 2003–2004*** (New York: Oxford University Press, 2003).

International Institute for Strategic Studies, ***The Military Balance 2016*** (London, UK: Routledge Press, 2016).

Internet World Stats, "China: Internet Usage Stats and Population Report, 2010," www.internetworldstats.com/asia/cn.htm.

"Is China Fraying?" ***The Economist*** (July 9, 2009), http://www.ecnomist.com/node/13988479.

Jacobs, Andrew, "China Faces Criticism over New Software Censor," ***NYT*** (June 11, 2009), http://www.nytimes.com/2009/06/11/world/asia/11censor.html.

Jacobs, Andrew, "For Foreign Journalists in Beijing, It's All about Asking the Right Question," ***NYT*** (March 13, 2014), http://sinosphere.blogs.nytimes.com/2014/03/13/for-foreign-journalists-in-beijing-its-all-about-asking-the-right-question/.

Jacobs, Andrew, and Buckley, Chris, "Tales of Army Discord Show Tiananmen Square in a New Light," ***NYT*** (June 2, 2014).

JI Chenjie and LIU Wei, "A Brief Discussion of Public Opinion Warfare on the Web," *Military Correspondent* (PRC) (#1, 2009), http://www.chinamil.com.cn/site1/jsjz/2009-01/14/content_1619064.htm.

JI Jianliang, YANG Bin, and TAN Xueping, "Several Issues Regarding Establishing Battlefield Dominance Under Informationized Conditions," *NDS&T* (PRC) (#2, 2010).

JI Peilin and JI Kaiyun, "The Iran–Iraq War and Psychological Warfare," *Journal of Shangluo University* (XXVIII, #3, June 2014).

JIA Fengshan, "The New Military Transformation Ushers in New Theories of Dominance," *CNDN* (September 11, 2003), http://www.chinamil.com.cn/gb/pladaily/2003/09/11/20030911001137_gdyl.html.

JIA Fengshan, "The Revelation of the Iraq War: Information Advantage Determines Battlefield Advantage," *PLAD* (May 21, 2003), http://mil.eastday.com/epublish/gb/paper462/20030521/class046200002/hwz1128473.htm.

JIANG Fangran, *Command of Combined Combat Under High-Tech Conditions* (Beijing, PRC: LAPH, 1995).

JIANG Han, YIN Hao, LI Xuejin, and CAO Kejing, "Level of Information Advantage in C4ISR System-of-Systems Conflict Simulations," *Aerospace Electronics Information Engineering and Control* (PRC) (#1, XXVIII, January 2006).

JIANG Lianju, *Space Operations Teaching Materials* (Beijing, PRC: MSPH, 2013).

JIANG Yibing, "Information Deterrence and Its Applications in Joint Operations," *Journal of the Xi'an Politics Institute* (XXIV, #5, October 2011).

JIANG Zemin, "Work Report to the 16th Party Congress," ***Xinhua*** (November 17, 2002), http://www.china.org.cn/english/features/49007.htm.

JIN Jingchun, *Research on Space Information Support and Safeguarding in Unified Joint Operations* (Beijing, PRC: NDUPH, 2008).

JIN Peng and DONG Ming, editors, *An Overview of Chinese Military Academies and Schools* (Beijing, PRC: MSPH, 2002).

"Jinan MR Continues Three Years of Organizing Joint Training Experiments, Innovative Results Are Pushed to the Entire Military," *China Newswire* (July 1, 2012), http://www.china.com.cn/military/txt/2012-07/01/content_25776864.htm.

Joint Chiefs of Staff (U.S.), ***Information Operations***, Joint Publication 3–13 (Washington, DC: Office of the Joints Chiefs of Staff, 2006).

Joint Chiefs of Staff (U.S.), ***Information Operations***, Joint Publication 3–13 (Washington, DC: Office of the Joint Chiefs of Staff, 2014), http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

Joint Chiefs of Staff (U.S.), ***Joint Doctrine for Information Operations***, Joint Publication 3–13 (Washington, DC: Office of the Joint Chiefs of Staff, 1998).

Joint Chiefs of Staff (U.S.), ***Space Operations***, JP 3–14 (Washington, DC: Department of Defense, January 6, 2009).

Jong-Chen, Jing de, "US–China Cybersecurity Relations: Understanding China's Current Environment," ***Georgetown Journal of International Affairs*** (September 15, 2014).

Kahn, Joseph, "China Is Filtering Phone Text Messages to Regulate Criticism," ***NYT*** (July 3, 2004), http://www.nytimes.com/2004/07/03/international/asia/03chin.html.

Kahn, Joseph, "China Shuts down Influential Weekly Newspaper in Crackdown on Media," ***NYT*** (January 25, 2006), http://www.nytimes.com/2006/01/25/international/asia/25china.html.

Kamphausen, Roy, and Scobell, Andrew, editors, ***Right-Sizing the People's Liberation Army: Exploring the Contours of China's Military*** (Carlisle, PA: Strategic Studies Institute, 2007).

Kamphausen, Roy, Lai, David, and Scobell, Andrew, editors, ***Beyond the Strait: PLA Missions Other than Taiwan*** (Carlisle, PA: Strategic Studies Institute, 2009).

Kaspersky Lab Global Research and Development Team, ***The Icefog APT, a Tale of Cloak and Three Daggers***, Kaspersky Labs (January 20, 2014), http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/icefog.pdf.

Kaspersky Lab Global Research and Development Team, ***The NetTraveler (aka 'Travnet')***, Kaspersky Labs (June 4, 2013), https://cdn.securelist.com/files/2014/07/kaspersky-the-net-traveler-part1-final.pdf.

KE Jinjun and CHEN Bojiang, *Air-Land Coordinated Combat Concepts* (Beijing, PRC: LAPH, 1996).

King, Gary, Pan, Jennifer, and Roberts, Margaret E., "How Censorship in China Allows Government Criticism but Silences Collective Expression," ***American Political Science Review*** (May 2013).

Knobler, Stacey, and Adel Mahmoud, Adel, editors, ***Learning from SARS: Preparing for the Next Disease Outbreak, a Workshop Summary*** (Washington, DC: National Academies Press, 2004), http://www.ncbi.nlm.nih.gov/books/NBK92479/.

Kockritz, Angela, "They Have Miao," ***Die Zeit*** (January 14, 2015), http://www.zeit.de/feature/freedom-of-press-china-zhang-miao-imprisonment.

KONG Ying, "Viewing News and Media Warfare in the Context of Informationized Warfare," *PLAD* (June 1, 2004), http://news.xinhuanet.com/mil/2004-06/01/content_1500707.htm.

KOU Shiqiang, "A Clarification of Unified Joint Operations," *PLAD* (August 11, 2004), http://www.china.com.cn/military/zhuanti/sjxjsbg/txt/2004-08/11/content_5632264.htm.

Kristof, Nicholas, "Privately, More and More Chinese Say It's Past Time for Deng to Go," ***NYT*** (April 17, 1989), http://www.nytimes.com/1989/04/17/world/privately-more-and-more-chinese-say-it-s-past-time-for-deng-to-go.html.

Lam, Oiwan, "China: When the Network Was Cut in Xinjiang," Global Voices Advocacy (October 13, 2010), https://advocacy.globalvoicesonline.org/2010/13/13/china-when-network-was-cut-in-xinjiang.

Lanzhou Military Region Headquarters Communications Department, "Space Information Support and Its Influence on Future Terrestrial Operations," *Military Art* (#10, 2003).

Large Phrase Dictionary Editorial Committee, *Large Phrase Dictionary, Military Volume* (Shanghai, PRC: Shanghai Phrasebook Publishing Committee, 2003).

"A Letter to Yiyi: Chinese Newspaper's Defiant Commentary on Train Collision," ***Wall Street Journal*** (July 31, 2011), http://blogs.wsj.com/chinarealtime/2011/07/31/a-letter-to-yiyi-chinese-newspapers-defiant-commentary-on-train-collision/.

Levy, Steven, ***Crypto*** (New York: Penguin Books, 2001).

Lewis, John, and XUE Litai, ***China's Strategic Seapower*** (Stanford: Stanford University Press, 1994).

LI Chunming, CHEN Yilai, JIN Guomin, and WANG Yunlei, "Some Thoughts on Innovating Informationized Operational Command," *CMS* (#5, 2004).

Li Daguang, "The Characteristics and Rules of Law of Space Strategy," *CMS* (#1, 2002).

Li Daguang, "Reconsideration of the Mechanisms for Winning Informationized Warfare," *CMS* (#6, 2014).

LI Dayao, "A Survey of the Development of Space Technology in China," *China Aerospace* (June 1999), pp. 16–19, in ***FBIS-CHI***.

LI Dong, ZHAO Xinguo, and HUANG Chenglin, "Research on Concepts of Space Operations and Its Command," *JAECT* (XIV, #5, 2003).

LI Fuyuan, ZHANG Jialiang, ZHAO Liguo, and GAO Xingzhuo, "Military Command Decisions for Seizing Comprehensive Dominance on the Battlefield," *Fire Control & Command Control* (XXXV, #11, November 2010).

LI Guoqiang and CHEN Wei, "Several Issues That Must Be Addressed in Establishing Scientific and Technological Mobilization Preparations," *ND* (#9, 2003).

LI Jian and LIU Guichou, "Development and Changes in Integrated Joint Operations Command," *CNDN* (April 21, 2005).

LI Jingjun and DAN Yuquan, "The Strategy of Space Deterrence," *CMS* (#1, 2002).

LI Qi, "A Brief Discussion of Chinese Military Intelligence Activities in Informationized Wars," *Science and Technology News* (PRC) (#36, 2010).

LI Suijin, "Intense Battle at the "Crossroads of Asia and Europe," *PLAD* (August 8, 2014), http://jz.chinamil.com.cn/n2014/tp/content_6084860.htm.

LI Xuanliang, "Establishment Ceremony for People's Liberation Army War Zones Held in Beijing," *Xinhuanet* (February 1, 2016), http://military.china.com/important/11132797/20160201/21395968_all.html#page_2.

LI Xuanliang, ZHANG Xuanjie, and LI Qinghua, "Establishment Ceremony for the Ground Forces Command, Strategic Support Force, Rocket Force Is Held in Beijing," *People's Daily* (January 2, 2016), http://politics.people.com.cn/n1/2016/0102/c1024-28003584.htm.

LI Yingming, LIU Xiaoli, et al., "An Analysis of Integrated Joint Operations," *PLAD* (April 12, 2005).

LI Yinnian, DONG Aiguo, and HU Haijun, "The Status and Future of Joint Tactics," *CMS* (#3, 2001).

LI Yinnian, SUN Qiangying, and SUN Jianjun, "Basic Features of Information Operations," *CMS* (#5, 2004).

LI Yinnian, WANG Xiangsheng, and GAO Zheng, "Categories of Operational Forms under High-Technology Conditions," *CMS* (#2, 1995).

LI Yousheng, *Science of Joint Campaigns Teaching Materials* (Beijing, PRC: MSPH, 2012).

LI Yunlong and YU Xiaohong, "Exploration of US Military 'Air-Sea Battle' Space Operations," *Journal of the Academy of Equipment* (XXIV, #4, August 2013).

LI Zhengjun, ZHANG Jinlong, and MOU Aijun, "An Analysis of Electromagnetic Defense Based on Information Dominance," *NDS&T* (#4, 2011).

LI Zicai, "Analyzing Military Information Network Security and Defense," *Communications Design and Applications* (March, 2014).

LIANG Fengfei, "GSD, GPD: Military Training Is of Strategic Importance," *PLAD* (August 21, 2014), http://www.81.cn/jmywyl/2014-08/21/content_6104098.htm.

LIANG Fengfei, "GSD Military Training Department Announcement to the Entire PLA of 40 Areas Where Training Does Not Support Real Warfare," *PLAD* (October 12, 2014), http://www.chinanews.com/mil/2014/10-12/6669069.shtml.

Lin, Jeffrey, and Singer, P.W., "The Missiles of Zhuhai: China Displays New Strike Arsenal," ***Popular Science*** (November 17, 2014), http://www.popsci.com/missiles-zhuhai-china-displays-new-strike-arsenal.

LIN Pingzhong, "Information Systems and Network Security," *Journal of the PLA Nanjing Institute of Politics* (#6, 2013).

Lindsay, Jon R., Cheung, Tai Ming, and Reveron, Derek S., ***China and Cybersecurity*** (New York: Oxford University Press, 2015).

LING Peixiong and LI Xucheng, "New Efforts at Teaching Joint Operations Command at National Defense University," *PLAD* (June 5, 2005).

LIU Chuanyang, "Shifts in Advantage and Disadvantage in High Tech Local Wars," *Study Times* (April 16, 2004), http://www.china.com.cn/xxsb/txt/2004-04/16/content_5546646.htm.

LIU Congxin and ZHU Guoqing, "The Impact of Information Aerospace Strength on Local Wars," *NDS&T* (#1, 2012).

LIU Gaoping, *Study Volume on Public Opinion Warfare* (Beijing, PRC: NDUPH, 2005).

LIU Jiaxin, "General's Views: Legal Warfare—Modern Warfare's Second Battlefield," *Guangming Ribao* (November 3, 2004).

LIU Jiong, WANG Zhe, and WANG Yinchuan, "Research into Civil–Military Melded Develpoment of Network Security and Protection Systems," *ND* (#3, 2013).

LIU Kejian and WANG Xiubo, *The First Conflict Won through Airpower: The Kosovo War* (Beijing, PRC: MSPH, 2008).

LIU Kexin, *Study Volume on Legal Warfare* (Beijing, PRC: NDUPH, 2006).

LIU Shilong, FU Xiaohui, et al., "Jinan War Zone Joint Campaign Combined/Accumulated/Group Training: Researching Operational Issues Has Become a Foremost Concern," *China Newsnet* (July 2, 2012), http://www.takung.cn/military/content/2012-07/02/content_609838.htm.

LIU Wanping and CHEN Xiaoqing, "National People's Congress Standing Committee Passes National Defense Mobilization Law," *PLAD* (February 27, 2010), http://www.mod.gov.cn/reports/201002/gfdyf/2010-02/27/content_4127069.htm.

LIU Youfang and HAN Qiang, editors, *Military Information Security Principles* (Beijing, PRC: NDUPH, 2005).

Ljunggren, David, and Sharp, Alastair, "Hacking Attack in Canada Bears Signs of Chinese Army Unit: Expert," ***Reuters*** (August 1, 2014), http://www.reuters.com/article/us-china-canada-cybersecurity-idUSKBN0G13X220140801.

LONG Yuehao, "The Current State and Outlook for Chinese Launcher Systems," *China Aerospace* (August 2004).

"Looking back on the Foundational Projects of Military Informationization Construction." *China Aerospace Newspaper* (April 7, 2004), http://www.ldyx.org/a/liangdanyixing/xinzengzilei/2009/0926/939_2.html.

LU Jin, "Lu Jin: Satellite Communications—The Information Bridge during Earthquake Relief Operations," Speech before the Chinese Communications Studies Association (September 26, 2008), http://www.ezcom.cn/Article/8591.

Lum, Thomas, Figliola, Patricia Moloney, and Weed, Matthew, ***China, Internet Freedom, and US Policy***, R42601 (Washington, DC: Congressional Research Service, 2012), https://www.fas.org/sgp/crs/row/R42601.pdf.

LUO Youli, General Editor, *National Defense Theory* (Beijing, PRC: MSPH, 2002).

MA Ping, *Joint Operations Research* (Beijing, PRC: NDUPH, 2013).

MA Shuming, "Issues on the Theory and Practice of the PLA's Joint Logistics," *CMS* (#2, 2001).

MacKinnon, Rebecca, "China's Censorship 2.0: How companies Censor Bloggers," ***First Monday*** (XIV, #2, February 2, 2009), http://firstmonday.org/article/view/2378/2089.

MAO Zedong, *Six Essays on Military Affairs* (Beijing, PRC: Foreign Languages Press, 1972).

Marble, Andrew D., Testimony to the US China Economic and Security Review Commission (December 7, 2001).

Marczak, Bill, Weaver, Nicholas, Dalek, Jakub, et al., "China's Great Cannon Research Brief," CitizenLab (April 2015), https://citizenlab.org/wp-content/uploads/2009/10/ChinasGreatCannon.pdf.

Martina, Michael, "China Withholds Full Domestic-Security Spending Figure," ***Reuters*** (March 4, 2014), http://www.reuters.com/article/us-china-parliament-security-idUSBREA240B720140305.

Matthews, William, "Chinese Puzzle," ***Defense News*** (September 6, 2010), http://www.defensenews.com/story.php?i=4767907.

McAfee Foundstone Professional Services, ***Global Energy Cyberattacks: "Night Dragon,"*** McAfee Labs (February 10, 2011), http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

McGregor, Richard, ***The Party: The Secret World of China's Communist Rulers*** (New York: Harper Collins Publishing, 2010).

McMillan, Robert, "China Policy Could Force Foreign Security Firms Out," ***Network World*** (August 26, 2010), http://www.networkworld.com/article/2217282/security/china-policy-could-force-foreign-security-firms-out.html.

"Military Newspaper Editorial: PLA Commanders Face Unprecedented Military Culture Challenges," *PLAD* (February 3, 2015), http://www.chinanews.com/mil/2015/02-03/7028403.shtml.

Miller, Alice, "More Already on the Central Committee's Leading Small Groups," ***China Leadership Monitor*** #44 (Summer 2014), http://www.hoover.org/sites/default/files/research/docs/clm44am.pdf.

Mills, Elinor, "Web Traffic Redirected to China Still a Mystery," ***CNET*** (October 8, 2010), http://www.cnet.com/news/web-traffic-redirected-to-china-still-a-mystery/.

Millward, Steven, "Support for Windows XP Is Over, but China Still Has 200 Million PCs Using It," ***Tech in Asia*** (April 9, 2014), https://www.techinasia.com/windows-xp-now-dead-but-200-million-machines-in-china-still-using-it.

"Ministry of Public Security Information and Communications Bureau Chief Ma Xiaodong Speaks," *Sohu.com* (September 13, 2003), http://it.sohu.com/63/81/article213158163.shtml.

"'Mission Action-2013C' Employs Unified Command, Typhoon Becomes Special Topic," *PLAD* (September 26, 2013), http://www.chinanews.com/mil/2013/09-26/5323816.shtml.

Morrison, Wayne, ***China–U.S. Trade Issues***, CRS Report RL33536 (Washington, DC: Congressional Research Service, 2015), https://www.fas.org/sgp/crs/row/RL33536.pdf.

Mozur, Paul, and Perlez, Jane, "Gregarious and Direct: China's Web Doorkeeper," ***NYT*** (December 1, 2014), http://nyti.ms/1tuxRxl.

Mulvenon, James, ***Soldiers of Fortune*** (Armonk, NY: M.E. Sharpe Publishers, 2001).

Mulvenon, James, and Finkelstein, David, editors, ***China's Revolution in Doctrinal Affairs*** (Alexandria, VA: Center for Naval Analysis, 2005).

Mulvenon, James, and Yang, Andrew N.D., editors, ***The People's Liberation Army as Organization*** (Santa Monica, CA: RAND Corporation, 2002).

Mulvenon, James, and Yang, Andrew, editors, ***The People's Liberation Army in the Information Age*** (Santa Monica, CA: RAND Corporation, 1999).

Murphy, Zoe "China Struggles to Censor Train Crash Coverage," ***BBC News*** (July 28, 2011), http://www.bbc.com/news/world-asia-pacific-14321787.

Nanjing Political Academy Military News Department Study Group, "Study of the Journalistic Media Warfare in the Iraq War," *CMS* (#4, 2003).

National Defense University Science Research Department (PRC), *New Perspectives on Military Transformation: Explaining 200 New Military Concepts* (Beijing, PRC: LAPH, 2004).

"National Security Law of the People's Republic of China," *China Daily* (July 1, 2015), http://www.chinadaily.com/cn/hqcj/zgjj/2015-07-01/content_13912103.html.

NetReSec, ***China's Man on the Side Attack on GitHub***, NetReSec (March 31, 2015), http://www.netresec.com/?month=2015-03&page=blog&post=china%27s-man-on-the-side-attack-on-github.

NI Tianyou, *Command Information Systems Teaching Materials* (Beijing, PRC: MSPH, 2013).

NIU Shulai, LIU Jun, HUO Yaozhong, "Comprehensive Information Systems Under Future Conditions of Unified Joint Operations," *Fire Control & Command Control* (PRC) (XXXIV, #3, March 2009).

O'Dowd, Ed, ***Chinese Military Strategy in the Third Indochina War*** (New York: Routledge Press, 2007).

The Office of Civil Air Defense of the People's Republic of China, PRC Civil Air Defense Law (May 5, 2011), http://www.ccad.gov.cn/view/zhengcefagui/falvfagui/20110505/15.html.

Olson, Wyatt, "'Left Hook' Deception Hastened War's End," ***Stars and Stripes*** (2016), http://www.stripes.com/news/special-reports/the-gulf-war-25-year-anniversary/deception.

Onley, Dawn S., "Red Storm Rising," ***GCN*** (August 17, 2006), https://gcn.com/articles/2006/08/17/red-storm-rising.aspx.

Open Net Initiative, ***Internet Filtering in China in 2004–2005: A Country Study***, Open Net Initiative (April 14, 2005), https://opennet.net/sites/opennet.net/files/ONI_China_Country_Study.pdf.

"The Operational Applications of C4ISR Systems," *PN* (September 23, 2011), http://mil.news.sohu.com/20110923/n320326987.shtml.

Orts, Eric W., "The Rule of Law in China," ***Vanderbilt Journal of Transnational Law*** (January 2001).

Orwig, Jessica, "A Rocket Launch Monday Was Delayed Because of a Boat," ***Business Insider*** (October 28, 2014), http://www.businessinsider.com/why-rocket-launch-delayed-by-a-boat-2014-10.

"Ours, All Ours," ***The Economist*** (April 6, 2013).

PENG Guangqian and YAO Youzhi, ***The Science of Military Strategy*** (Beijing, PRC: MSPH, 2005).

People's Liberation Army, *Military Terminology of the PLA* (*Complete Volume*) (Beijing, PRC: MSPH, 1997).

"People's Liberation Army Commander: Joint Operations Requires Breaking away from Old Thoughts and Stovepiped Interests," *PLAD* (July 9, 2014), http://military.people.com.cn/n/2014/0709/c1011-25256858.html.

"People's Liberation Army Jinan War Zone Joint Campaign Combined Training," *China Newsnet* (June 30, 2012), http://mil.sina.cn/?sa=t134d294002v76&vt=4.

"People's Liberation Army Leader: Joint Operations Must Break through the Thought-Interest Walls," *PLAD* (July 9, 2014), http://military.people.com.cn/n/2014/0709/c1011-25256858.html.

"PLA General Staff Department Issues New All-Army Military Training Work Regulations," *PLAD* (January 15, 2005).

"People's Republic of China National Security Law," *China Daily* (July 1, 2015), http://www.chinadaily.com.cn/hqcj/zgjj/2015-07-01/content_13912103.html.

Perlroth, Nicole, "Hackers in China Attacked the Times for Last Four Months," ***NYT*** (January 30, 2013), http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html.

Perlroth, Nicole, "Wall Street Journal Announces That It, Too, Was Hacked by the Chinese," ***NYT*** (January 31, 2013), http://www.nytimes.com/2013/02/01/technology/wall-street-journal-reports-attack-by-china-hackers.html.

Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan, "Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary General" (September 14, 2011), https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.

Peterson, Andrea, "Why Naval Academy Students Are Learning to Sail by the Stars for the First Time in a Decade," ***WP*** (February 17, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/02/17/why-naval-academy-students-are-learning-to-sail-by-the-stars-for-the-first-time-in-a-decade/.

Pollpeter, Kevin, and Allen, Kenneth W., editors, ***The PLA as Organization, v. 2.0*** (Merrifield, VA: DGI International, 2015). www.pla-org.com.

PU Duanhua, "On Wartime Public Opinion Mobilization," *Journal of the PLA Nanjing Institute of Politics* (#2, 2006).

"Public Opinion Warfare, Psychological Warfare, and Legal Warfare in Modern Conflict Are All Becoming More Intense," *PLAD* (April 1, 2004), http://mil.anhuinews.com/system/2004/04/01/000608647.shtml.

QIN Jirong, *Concepts of Command and Control* (Beijing, PRC: NDIP, 2012).

QIU Yue, "Expert: Strategic Support Force Will Permeate the Entire Course of Operations, Is a Key Factor in Achieving Victory," *PN* (January 5, 2016), http://military.people.com.cn/n1/2016/0105/c1011-28011251.html.

Racicot, Jonathan, "The Past, Present, and Future of Chinese Cyber Operations," *Canadian Military Journal* (XIV, #3, Summer 2014).

Rashid, Fahmida Y., "Chinese Attackers Hacked Forbes Website in Watering Hole Attack: Security Firms," *Security Week* (February 11, 2015), http://www.securityweek.com/chinese-attackers-hacked-forbes-website-watering-hole-attack-security-firms.

REN Min, *The Science of National Defense Mobilization* (Beijing, PRC: MSPH, 2008).

"Report on the Implementation of the 2015 National and Local Budgets and the Draft of the 2016 National and Local Budgets (Essentials)," *Xinhuanet* (March 5, 2016), http://news.xinhuanet.com/politics/2016lh/2016-03/05/c_1118243992.htm.

Reporters without Borders, "Survey of Blocked Uyghur Websites Shows Xinjiang Still Cut Off from the World" (October 29, 2009), https://www.rsf.org/china-survey-of-blocked-uyghur-websites-29-10-2009,34859.html.

Reporters without Borders, ***2015 World Press Freedom Index***, http://index.rsf.org/#!/.

"Research on Network Security and Defense Under Conditions of Network Warfare," *Science Times* (#5, 2013), http://www.xzbu.com/8/view-4168149.htm.

Ricks, Thomas E., "Target Approval Delays Irks Air Force Officers," ***WP*** (November 18, 2001), http://www.washingtonpost.com/wp-srv/nation/Airwar18.html.

Rigby, Bill, and Carsten, Paul, "Microsoft Tackles China Piracy with Free Upgrade to Windows 10," ***Reuters*** (March 18, 2015), http://www.reuters.com/article/us-microsoft-china-idUSKBN0ME06A20150318.

Romjue, John, ***From Active Defense to AirLand Battle*** (Ft. Monroe, VA: TRADOC, 1984).

Rosenzweig, Paul, ***Cyber Warfare*** (Denver, CO: Praeger Publishers, 2013).

RSA Research, ***Terracotta VPN***, RSA (August 4, 2015), https://blogs.rsa.com/wp-content/uploads/2015/08/Terracotta-VPN-Report-Final-8-3.pdf.

Ryan, Mark A., Finkelstein, David M., and McDevitt, Michael A., editors, ***Chinese Warfighting: The PLA Experience Since 1949*** (Armonk, NY: M.E. Sharpe, 2003).

Schelling, Thomas, ***Arms and Influence*** (New Haven, CT: Yale University Press, 1967).

Segal, Adam, "The Top Ten Cybersecurity Incidents in China of 2014," Council on Foreign Relations Net Politics Blog (December 10, 2014), http://blogs.cfr.org/cyber/2014/12/10/the-top-ten-cybersecurity-incidents-in-china-of-2014/.

Shambaugh, David, ***Modernizing China's Military: Progress, Problems, and Prospects*** (Berkeley, CA: University of California Press, 2002).

SHEN Lutao, "Huang Pu: Ensuring the Smooth Operation of the 'Golden Shield' Project, Serving National Informationization," *Xinhuanet* (September 2, 2003), http://news.xinhuanet.com/newscenter/2003-09/02/content_1059383.htm.

SHEN Shilu, FENG Shuxing, WANG Jia, LI Yadong, "Initial Research into Military Aerospace Mission Command Decision-making," *JAECT* (XVIII, #1, February 2007).

SHEN Yaxin, "Five Key Phrases for Understanding Xi Jinping's Push for a New Approach to Internet Security," *PN* (August 6, 2015), http://politics.people.com.cn/n/2015/0806/c1001-27419302.html?utm_content=buffer4b50d&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.

SHENG Peilin, WANG Lin, and LIU Ya, editors, *Public Opinion Warfare: Discussion of 100 Examples and Solutions* (Beijing, PRC: LAPH, 2006).

SHI Yukun, "Lt. Gen. Li Jijun Answers Questions on Nuclear Deterrence, Nation-State, and Information Age," *CMS* (#3, 1995), in ***FBIS-CHI*** (August 1995).

Shirk, Susan, editor, ***Changing Media, Changing China*** (New York: Oxford University Press, 2011).

Singer, P.W., "How the United States Can Win the Cyberwar of the Future," ***Foreign Policy*** (December 18, 2015), http://foreignpolicy.com/2015/12/18/how-the-united-states-can-win-the-cyberwar-of-the-future-deterrence-theory-security/.

Solis, Gary, ***The Law of Armed Conflict*** (New York: Cambridge University Press, 2010).

SONG Yuejin, Chief Editor, *Command and Control Warfare* (Beijing, PRC: NDUPH, 2012).

SONG Yunxia, *Legal Warfare Under Informationized Conditions* (Beijing, PRC: AMS Publishing, 2007).

Sonnad, Nikhil, "A First Look at the Chinese Operating System the Government Wants to Replace Windows," ***Quartz*** (September 22, 2015), http://qz.com/505383/a-first-look-at-the-chinese-operating-system-the-government-wants-to-replace-windows/.

Standing Committee of the National People's Congress, "Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security" (December 28, 2000), http://english.gov.cn/laws/2005-09/22/content_68771.htm.

State Council Information Office (PRC), *China's Active Defense* (Beijing, PRC: State Council Information Office, 2015).

State Council Information Office (PRC), *China's National Defense in 2004* (Beijing, PRC: State Council Information Office, 2004), http://news.xinhuanet.com/mil/2004-12/27/content_2384964.htm.

State Council Information Office (PRC), ***China's National Defense in 2006*** (Beijing, PRC: State Council Information Office, 2006), http://fas.org/nuke/guide/china/doctrine/wp2006.html.

State Council Information Office (PRC), "Notification of the State Council on Authorizing the State Internet Information Office for Responsibility Regarding Internet Information and Content Management," State Council Information Office (August 26, 2014), http://politics.people.com.cn/n/2014/0828/c70731-25558093.html.

State Council Information Office (PRC), *Tenth Five Year Plan for National Economic and Social Development, Informationization Key Point Special Plans* (October 18, 2002), http://www.cia.org.cn/information/information_01_xxhgh_3.htm.

State Council Information Office (PRC), ***The Internet in China*** (Beijing, PRC: State Council Information Office, 2010), http://www.china.org.cn/government/whitepaper/node_7093508.htm.

State Council Information Office (PRC), *White Paper on China's National Defense in 2002* (Beijing, PRC: State Council Information Office, 2002), http://www.mod.gov.cn/affair/2011-01/06/content_4249946_2.htm.

Stokes, Mark, ***The PLA General Staff Department Third Department Second Bureau: An Organizational Overview of Unit 61398*** (Arlington, VA: Project 2049, 2015), http://www.project2049.net/documents/Stokes_PLA_General_Staff_Department_Unit_61398.pdf.

Stokes, Mark, and Hsiao, L.C. Russell, ***Countering Chinese Cyber Operations: Opportunities and Challenges for US Interests*** (Arlington, VA: Project 2049,

2012), http://project2049.net/documents/countering_chinese_cyber_operations_stokes_hsiao.pdf.

Stokes, Mark, Lin, Jenny, and Hsiao, L.C. Russell, ***The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*** (Arlington, VA: Project 2049, 2011), http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf.

SU Jinchang and SHI Yansheng, "Psychological Warfare: New Methods under Informationized Conditions," *CNDN* (June 22, 2004), http://www.people.com.cn/GB/junshi/1078/2589687.html.

SUN Jinwei, *Research on Laws Governing Campaign Dilemmas and Activities* (Beijing, PRC: NDUPH, 2013).

SUN Lihua, "Battlefield Deceit for Attacking and Disrupting Psychological Defenses—American Military Psychological Warfare Methods," *PN* (January 11, 2002), http://www.people.com.cn/GB/junshi/62/20020111/646108.html.

"The Survey Troops Behind 'Change'," *China Survey Newspaper* (October 30, 2007), http://www.sbsm.gov.cn/article//ztzl/chdf/200710/20071000003834.shtml.

Symantec, ***Advanced Persistent Threats, A Symantec Perspective***, Symantic (Mountain View, CA: Symantec, 2011), http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf.

"System-of-Systems Combat, the Sword Points to the Future Battlefield—An Outline of the 'Mission Action 2013C' Trans-Military Region Mobile Campaign Exercise," *Xinhuanet* (September 30, 2013), http://war.163.com/13/0929/20/99VGB1LF00014OMD.html.

TAN Rukun, *Operational Strength Construction Teaching Materials* (Beijing, PRC: MSPH, 2012).

TAN Wenfang, "The Impact of Information Technology on Modern Psychological Warfare," *NDS&T* (#5, 2009).

Tanner, Murray Scot, ***The Politics of Lawmaking in China*** (Oxford, UK: Clarendon Press, 1999).

Technolytics, ***Cyber Commander's Handbook*** (McMurray, PA: Technolytics, 2009).

Thomas, Timothy L., ***Dragon Bytes: Chinese Information War Theory and Practice*** (Fort Leavenworth, KS: Foreign Military Studies Office, 2004).

ThreatConnect and DGI, ***Camerashy: Closing the Aperture on China's Unit 78020***, ThreatConnect (Arlington, VA: ThreatConnect, 2015). cdn2.hubspot.net/hubfs/454298/Project_CAMERASHY_ThreatConnect_Copyright_2015.pdf.

United States Congressional-Executive Commission on China, "Agencies Responsible for Censorship in China," http://www.cecc.gov/agencies-responsible-for-censorship-in-china.

United States Council for International Business, "Statement on China's Compliance with Its World Trade Organization (WTO) Commitments," Statement submitted to the U.S. Trade Representative (September 20, 2013), http://uscib.org/docs/USCIB_Submission_to_USTR_China_Compliance_with_WTO_Commitments.pdf.

United States Department of Defense, ***The National Defense Strategy of the United States of America*** (Washington, DC: Office of the Secretary of Defense, June 2008).

United States Department of Justice, "US Charges Five Chinese Military Hackers for Cyber Espionage against US Corporations and Labor Organization for Commercial Advantage," Press Release (May 19, 2014), http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

Wagstaff, Jeremy, "Hunt for Deep Panda Intensifies in Trenchs of US–China Cyberwar," ***Reuters*** (June 21, 2015), http://www.reuters.com/article/us-cybersecurity-usa-deep-panda-idUSKBN0P102320150621.

"Walk the Path of Chinese Information Systems Security," *Guangming Ribao* (January 15, 2016), http://roll.sohu.com/20160115/n434583116.shtml.

WANG Baocun, "China and the Revolution in Military Affairs, Part 1" *CMS* (#4, 2001).

WANG Baocun, "Information Warfare in the Kosovo Conflict," *PLAD* (May 25, 1999).

WANG Houqing and ZHANG Xingye, Chief Editors, *The Science of Campaigns* (Beijing, PRC: NDUPH, May 2000).

WANG Hui, *Foundational Knowledge, Considerations, and Explanations of Informationized Warfare* (Beijing, PRC: MSPH, 2009).

WANG Jianming and SHEN Jiamin, "Some Reflections on the Integrated Development of National Information Warfare," *NDS&T* (PRC) (#6, 2009).

WANG Ruqun, *The Battlefield Electromagnetic Environment* (Beijing, PRC: LAPH, 2006).

WANG Weiyu and ZHANG Qiancheng, *Discussing Military Theory Innovation with Chinese Characteristics* (Beijing, PRC: NDUPH, 2009).

WANG Xingsheng, WU Zhizhong, and LUO Xinqin, "Revelations from Psychological Warfare in the Iraq War," *ND* (#6, 2003).

WANG Yongming and LIU Xiaoli, *Iraq War Research* (Beijing, PRC: MSPH), 2003.

WANG Yueting, "The Power of Psychological Warfare in Modern Warfare," *Study Times* (March 27, 2005, #113), http://www.china.com.cn/xxsb/txt/2005-10/11/content_5994663.htm.

WANG Yukai, "Wang Yukai: Central Network Security and Informationization Leading Small Group's Origins and Impact," *PN* (March 3, 2014), http://theory.people.com.cn/n/2014/0303/c40531-24510897.html.

WANG Yuping, "Strengthen Research into Psychological Warfare under Informationized Conditions," *PLAD* (May 18, 2004), http://news.xinhuanet.com/mil/2004-05/18/content_1475394.htm.

WANG Zhengde and YANG Shisong, Chief Editors, *Information Security Management Theory* (Beijing, PRC: MSPH, 2009).

WANG Zijun, CHEN Tao, and MO Jinshan, "Explaining People's Armed Police Public Opinion Warfare Thought," *Hebei Legal Newspaper* (April 6, 2010), http://jiuzhan.hbfzb.com/html/article/201004/201046104703823.html.

Weeden, Brian, ***Through a Glass Darkly: Chinese, Russian, and American Anti-Satellite Testing in Space*** (Washington, DC: Secure World Foundation, 2014).

WEI Konghu, editor, *Research on Military Command in the Journal of National Defence University* (Beijing, PRC: NDUPH, 2014).

Weibo Corporation, Form F-1 Registration Statement with US Securities and Exchange Commission (March 14, 2014), p. 36, http://www.sec.gov/Archives/edgar/data/1595761/000119312514100237/d652805df1.htm.

Wemple, Erik, "Chinese Leader Xi Jinping Blames Western News Outlets for Visa Problems in China," ***WP*** (November 12, 2014), https://www.washingtonpost.com/blogs/erik-wemple/wp/2014/11/12/chinese-president-xi-jinping-blames-news-outlets-for-visa-problems-in-china/.

WEN Haihong, "Examining Modern Psychological Warfare's Characteristics from Multiple Different Perspectives," *NDS&T* (PRC) (#1, 2008).

"With the Permission of CMC Chairman Xi Jinping: The CMC Promulgates the Newly Updated 'Military Grassroots Construction Gangyao'," *PLAD* (February 4, 2015), http://www.81rc.mil.cn/news/2015-02/04/content_6339667.htm.

Wong, Edward, "After Long Ban, Western China Is Back Online," ***NYT*** (May 14, 2010), http://www.nytimes.com/2010/05/15/world/asia/15china.html.

WU Jianchu, "Joint Operations—The Basic Form of Combat on High-Tech Terms," *CMS* (#4, 1995), in ***FBIS-CHI***.

WU Renhe, *Theory of Informationized Conflict* (Beijing, PRC: MSPH, 2004).

WU Xiu, LI Qiang, and ZHOU Hongzai, "A Particular GSD Research Office Seeks to Create a Phalanx of High Quality Talent," *Seeking Truth* (April 26, 2012), http://www.qstheory.cn/special/2012/xinxihuayanjiusuo/rencaijianshe/201204/t20120426_154158.htm.

WU Zhiyong, *Operational Mobilization Studies Teaching Materials* (Beijing: MSPH, 2001).

WU Zhizhong, *Wartime Political Work Teaching Materials* (Beijing, PRC: MSPH, 2013).

"Xi Jinping Leads Internet Security Group," ***Xinhua*** (February 27, 2014), http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm.

"Xi Jinping: Building Our Nation from a Network Power to a Network Major Power," *Xinhuanet* (February 27, 2014), http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm.

XIA Liping, "The Chinese Military Strategy of the Active Defense," *Study Times* (December 14, 2005), http://www.china.com.cn/xxsb/txt/2005-12/14/content_6060925.htm.

XIA Wenjun, *Science of Military Command Teaching Materials* (Beijing, PRC: MSPH, 2012).

XIAO Li, "Emphasize the Building of Network and Information Security Management Standards, Improve Our Nation's Network Security Management Level," *Xinhuanet* (November 30, 2014), http://politics.people.com.cn/n/2014/1130/c70731-26120705.html.

XIE Zhaohui and ZHAO Dexi, "On the Fundamental Features of the Military Space Force," *CMS* (#1, 2009).

XU, Beina, "Media Censorship in China," Council on Foreign Relations (September 25, 2014), http://www.cfr.org/china/media-censorship-china/p11515.

XU Guoxing, *Research on Our Military's Information Operations Strength Construction* (Beijing, PRC: MSPH, 2013).

XU Hezhen, "A Discussion of the Main Differences between the Characteristics of Unified Joint Operations and Coordinated Joint Operations," *Military Art* (#5, 2004).

XU Jian, "New Changes in the Next Decade of China's Period of Strategic Opportunity," *Guangming Ribao* (October 30, 2013), http://cpc.people.com.cn/n/2013/1030/c83083-23372744.html.

XU Shiyong, WANG Tingting, and ZHANG Haitao, "An Examination of the Development Trend of Defensive Operations under Informationized Conditions," *NDS&T* (PRC) (#5, 2009).

XU Xinzhao, "Examining How Information Has Become a Key Factor in Combat Power," *Jianghui Forum* (#2, 2001).

XUE Xinglin, editor, *Campaign Theory Learning Guide* (Beijing: NDUPH, November 2001).

YAN Gaohong, "Informationized Warfare and Changes in the Essentials of Military Thinking," *CMS* (#5, 2004).

Yan, Sophia, "China Crackdown Makes It Harder to Get around Great Firewall," ***CNN*** (January 28, 2015), http://money.cnn.com/2015/01/28/technology/china-censorship-vpn-great-firewall/.

YANG Chunchang and SHEN Hetai, Chief Editors, *Political Operations under Informationized Conditions* (Beijing, PRC: Long March Publishing House, 2005).

YANG Genyuan, DONG Kuiyi, and WANG Ziming, "Research on Unified Information–Firepower Operations," *NDS&T* (PRC) (#2, 2010).

YANG Guoqiang and CHANG Ailing, "Deputy Chief of the General Staff Xiong Guangkai Discusses the Six Salient Issues of the International Strategic Situation," *PLAD* (January 2, 2004). http://jczs.news.sina.com.cn/2004-01-02/1731175221.html

YANG Ming, "Grasping the Generation of Psychological Information Dominance," *PLAD* (April 12, 2005), http://military.people.com.cn/GB/1078/3314642.html.

YAO Fei, "Some Thoughts Regarding Our Military's Anti-Secessionist Public Opinion and Propaganda Policies," *Military Correspondent* (PRC) (#5, 2009), http://www.chinamil.com.cn/site1/jsjz/node_22972.htm.

YAO Yunzhu, "The Evolution of Military Doctrine of the Chinese PLA from 1985 to 1995," ***Korea Journal of Defense Analyses*** (Winter, 1995).

Yardley, Jim, "A Hundred Million Cellphones Bloom, and Chinese Take to the Streets," ***NYT*** (April 25, 2005), http://www.nytimes.com/2005/04/25/world/asia/a-hundred-cellphones-bloom-and-chinese-take-to-the-streets.html?_r=0.

YE Zheng, *Concepts of Informationized Operations* (Beijing, PRC: MSPH, 2007).

YE Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: MSPH, 2013).

YI Youxue, "Considerations for Strengthening Information Mobilization Work in the New Circumstances," *ND* (#9, 2012).

YING Desong, "Information Warfare: A Main Pillar of Joint Combat," *PLAD* (September 11, 2001).

YOU Jun, "Research into the Characteristics and Development of Informationization in the Recent Several High-Technology Local Wars," *Civil-Military Dual-Use Technologies and Products* (#6, 2014).

YUAN, Li, "Text Messages Sent by Cellphone Finally Catch on in US," ***Wall Street Journal*** (August 11, 2005), http://www.wsj.com/articles/SB112372600885810565.

YUAN Peng, "China's Strategic Opportunity Period Has Not Ended," ***People's Daily Online*** (July 31, 2012), http://en.people.cn/90883/7893886.html.

YUAN Sanhu, "Our Country's Aerospace Tracking and Control Network Realizes a 'Large Triangle' Distribution," *Xinhua* (April 25, 2008), http://www.chinamil.com.cn/site1/xwpdxw/2008-04/25/content_1220073.htm.

YUAN Wenxian, *Joint Campaign Information Operations Teaching Materials* (Beijing, PRC: MSPH, 2009).

YUAN Wenxian, *Joint Operations Command Office Work Teaching Materials* (Beijing, PRC: NDUPH, 2008).

YUAN Wenxian, *The Science of Military Information* (Beijing, PRC: NDUPH, 2007).

YUAN Wenxian, *Science of Military Information* (Beijing, PRC: NDUPH, 2008).

YUAN Wenxian, Chief Editor, *Treatise on Headquarters Department Work* (Beijing: NDUPH, June 2001).

ZENG Qingyang, "Deliberations on Principles of Information Warfare," *CMS* (#6, 2002).

Zetter, Kim, ***Countdown to Zero Day*** (New York: Broadway Books, 2014).

Zetter, Kim, "Google Hack Attack Was Ultra-Sophisticated, New Details Show," ***Wired*** (January 14, 2010), http://www.wired.com/2010/01/operation-aurora/.

ZHANG Baojun, XU Xinzhao, XU Jun, and XUE Renjie, "Considerations on Improving the Command and Control Decision-Making Organization in Information Operations," *NDS&T* (PRC) (XXXIV, #1, February 2013).

ZHANG Huajun, "Seeking New Developments in Economic Mobilization Appropriate to the New Conditions of the Military Revolution," *ND* (#8, 2003).

ZHANG Jiali and MIN Zengfu, "Exploring the Extension of Local Wars to Air and Space," *CMS* (#1, 2005).

ZHANG Junguo, "Science and Technology Information Mobilization in Informationized War," *Journal of the Academy of Equipment* (XXIII, #2, April 2012).

ZHANG Ming, "Discussing 'Air Dominance' and 'Network and Electromagnetic Spectrum' Dominance," *PLAD* (October 29, 2002).

ZHANG Peigao, Chief Editor, *Joint Campaign Command Teaching Materials* (Beijing, PRC: MSPH, 2001).

ZHANG Peigao, *Joint Campaign Command Teaching Materials* (Beijing, PRC: MSPH, 2012).

ZHANG Qinghai and LI Xiaohai, "Space Warfare: From Vision to Reality," *CMS* (#1, 2005).

ZHANG Weihua, "New Theories of Dominance: Issues Concerning Information Dominance," *Journal of Information* (#12, 2007).

ZHANG Weiping, *Research into Command Information Systems and System-of-Systems Combat Structures* (Beijing, PRC: NDUPH, 2011).

ZHANG Xiao, "A Discussion of the Development and Employment of Civil-Use Information Resources," *Military Economic Research* (#1, 2007).

ZHANG Xingye, "The Important Aspects of the Conduct of Joint Campaigns," *CMS* (#2, 2001).

ZHANG Yining, "Informationized War Changes 'Future Battlefields'," *PLAD* (March 5, 2005), http://military.people/com.cn/BG/1078/3220196.html.

ZHANG Yuliang, Chief Editor, *The Science of Campaigns* (Beijing, PRC: NDUPH, 2006).

ZHANG Yunling, "Deeply Considering the International Environment Confronting Our Nation's Period of Strategic Opportunity," *Seeking Truth* (December 18, 2015), http://theory.people.com.cn/n1/2015/1218/c83846-27946374.html.

ZHANG Yuwu and DONG Zean, "Informationalized Warfare Will Make Seizing the Aerospace Technology 'High Ground' a Vital Factor," *PLAD* (March 30, 2005).

ZHAO Jin, "NDU and JFJB Society Jointly Hold 'Learn and Implement Chairman Xi's Vital Talk to the CMC Reform Work Conference and Its Spirit' Theoretical Conference," *PN* (December 18, 2015), http://theory.people.com.cn/n1/2015/1218/c40531-27945726.html.

ZHAO Lin and MENG Baohong, "Several Questions on Military Informationization Development Strategy," *CMS* (#5, 2015).

ZHENG Weiping and LIU Mingfu, Chief Editors, *Discussions on the Military's New Historic Missions* (Beijing, PRC: People's Armed Police Publishing House, 2005).

ZHI Tao and LI Wei, "X-37B, the Mysterious Space Fighter," *China Youth Daily* (November 3, 2014), http://jz.chinamil.com.cn/n2014/tp/content_6209028.htm.

ZHONG Songlai, "The Military Reform of the United States in the Post-Vietnam War Era," *CMS* (#1, 2002).

ZHOU Peng and WEN Enbing, "Developing the Theory of Strategic Deterrence with Chinese Characteristics," *CMS* (#3, 2004).

ZHOU Wang, *Research on China's "Leading Small Groups"* (Tianjin, PRC: Tianjin People's Publishing House, 2010).

ZHOU Xiaopeng, "On the Development of Joint Operations Theory," *CMS* (May 1996), in ***FBIS-CHI***.

ZHOU Xiaoyu, editor, *Campaign Research in the "Journal of National Defence University"* (Beijing, PRC: NDUPH, 2014).

ZHOU Xiaoyu, PENG Xiwen, and AN Weiping, *New Discussions on Joint Campaigns* (Beijing: NDUPH, January 2000).

ZHU, Tao, Phipps, David, Pridgen, Adam, et al., "Tracking and Quantifying Censorship on a Chinese Microblogging Site" (November 26, 2012), arXiv:1211.6166[cs.IR].

ZHU, Tao, Phipps, David, Pridgen, Adam, et al., "The Velocity of Censorship: High Fidelity Detection of Microblog Post Deletions," Paper presented at the 22nd USENIX Security Symposium (August 2013).

Zmijewski, Earl, ***Accidentally Importing Censorship***, Dynresearch (March 30, 2010), http://research.dyn.com/2010/03/fouling-the-global-nest/.

ZONG Wenshen, editor, *Legal Warfare: Discussion of 100 Examples and Solutions* (Beijing, PRC: LAPH, 2004).

ZOU Zhenning and CHA Rui, *Command Information Capabilities Research, Based on Systems Combat between Information Systems* (Beijing, PRC: Oceans Publishing House, 2011).

Index

Academy of Military Science (AMS), 24
Accurate data, 84
Administrative defensive measures, 149
Advanced persistent threat (APT), 184
Afghanistan, 46, 50–51, 53, 115
American Airlines, 123
Ansari X-Prize, 220
Anti-Secession Law of 2005, 49
Apple, 145
Arab-Israeli wars, 20
Arab Spring, 71, 74
Argentina, 28
Ascent, kinetic kill antisatellite (ASAT), 160
Ashley Madison, 123
Asia-Pacific Network Information Center (APNIC), 62
Association of Southeast Asian Nations (ASEAN), 124, 183
Attack: electronic, 97–98; network, 100–101
Australia, 134

Backward keyword searches, 77
Backward reposts searches, 77–78
Baidu, 74, 134, 135
Balkans, the. *See* Kosovo conflict
Battlefields: command-and-control system, 87; conditions, intelligence gathering on, 112; information transmission system, 87; sensor system, 87; support systems, 119–20
Battles, 31
Battleships, 89
Bezos, Jeff, 220
Bigelow, Robert, 220
Bigelow Aerospace, 220
Bing Dian, 10–11
Blockades, 45
Bloomberg News, 11, 12
Blue Origin, 220
Bo Xilai, 12, 75
Boxun.com, 12
Branson, Richard, 220

C2 centers. *See* Command-and-control systems
Camouflage, concealment, and deception measures (CCD), 84, 138, 142
Campaigns, 31; guiding thought, 90–93; information war at level of, 85–88; integrated operations, 90–92. *See also* Joint operations
CCP. *See* Chinese Communist Party (CCP)

Censorship, press, 9–11. *See also* Internet, the
Central Group for Internet Security and Informationization, 4
Central Military Commission (CMC), 42–43, 177, 179; reorganization of, 194–97
Central Propaganda Department (CPD), 8–11
Chiang Kai-shek, 19
China. *See* People's Republic of China (PRC)
China Aerospace Science and Industry Corporation (CASIC), 160
China Aerospace Science and Technology Corporation (CASC), 160
China Brazil Earth Resources Satellite (CBERS), 158
China Central Television (CCTV), 8, 9
China Cyberspace Administration, 59
China Internet Network Information Center (CNNIC), 7
China Military Science, 14
China Telecom, 126
China Youth Daily, 10–11
Chinese Communist Party (CCP), 1, 3–4, 6, 15, 177; Central Propaganda Department (CPD), 8–9; control of news by, 8; control of the Internet by, 57–72; future warfare views of, 200–203; information control by, 55–57; People's Liberation Army (PLA) and, 21, 22, 177–80; strategic information defense and, 53–78
Chinese language, translations of, 17
Chinese Military Encyclopedia, 38
Chinese National High-Technology Research and Development Plan, 3
Chinese National Security Law of 2015, 66
Cisco, 145
CitizenLab, 135
Civil Air Defense Law, 149–50
Clausewitz, Carl von, 88
Cognitive systems, 103
Combined arms operations, 27–28
Command-and-control systems, 118; battlefield, 87; at the operational level, 190–93; warfare, 106–9
Communications: offensive electronic operations against, 132; reliable, 84–85; space, 172–73; systems, 119
Competition, future warfare and Chinese/American, 206–11
Computer operating systems, 148
Conflict, informationization of. *See* Informationized conflict
Counterintelligence activities, 113–14
CPD. *See* Central Propaganda Department (CPD)
C.T.S. Technology, 132
Cyberespionage, 122–25, 145, 200
Cyber warfare. *See* Information warfare; Internet, the

Data: accurate, 84; collection, 84; encryption, 147–48; real-time, 83; relay, space, 172–73
Deep packet filtering, 69
Deep Panda, 123–24, 136
Defeatism among the troops, 143
Defense: civil, 149–50; electronic, 98–99; network, 101; psychological, 104–5
Defensive engineering measures, 149
Defensive information operations, 139–44; protecting military information systems, 140–42; psychological, 142–44
Defensive space operations, 169–71
Dell Computers, 148
Deng Xiaoping, 3, 35, 57, 155, 160; rise of, 20–22
Deterrence: information, 150–54; policy makers giving greater consideration to demands of, 218–19
Distributed denial-of-service (DDoS) attacks, 134, 136, 145, 153
Diversification, 220–21
DNS poisoning, 69

Dominance, information: campaign guiding thought and, 90–93; Chinese view of space and, 174–76; command and control at the operational level and, 190–93; establishing, 93–105, 120–50; importance of, 35–36; PLA organizations responsible for securing, 181–90; reconnaissance operations and, 121–28; reforms of 2016 and, 193–99; seizing the initiative and, 88–90; space dominance and, 163–64

Earth-surveying, space-based, 174
Economic sanctions, 45
Eighth Five-Year Plan (1991–1995), 27
Eisenhower, Dwight, 119
Electronic attack, 97–98
Electronic counter-countermeasures (ECCM), 147, 186
Electronic defense, 98–99
Electronic operations, offensive, 130–32
Electronic reconnaissance, 97, 126–27
Electronic warfare, 95–99; integrated network and, 101–2, 109
E-mail, 141
Emissions control (EMCON), 141
Encryption, data, 147–48
Equipment Academy, GAD, 190

Facebook, 68, 70, 73, 134
Falklands War, 20, 29
Firewalls, 146
Fisher, Jackie, 89
Foreign media in China, 11–13
Fourth Department, GSD, 186
Future warfare: American policy makers and Chinese views of, 206–11; Chinese conclusions shaping Chinese actions regarding, 203–6; how China sees information and, 200–203; policy don'ts for the United States and, 211–17; policy do's for the United States and, 217–21

General Administration of Press and Publication (GAPP), 8
General Armaments Department (GAD), 179, 187–90
General Logistics Department (GLD), 120, 178–79
General Political Department (GPD), 42, 117, 144, 178, 186–87
General Staff Department (GSD), 42, 178, 181–86; Fourth Department, 186; Informationization Department, 185; Third Department, 181–85
Georgia, 73
"Ghostnet," 123
GitHub.com, 135, 136
Global Times, 9
Gorbachev, Mikhail, 23
Golden Bridge, 5
Golden Card, 5
Golden Shield project, 70, 71
Golden Tax, 5
Google, 70, 74, 124, 145
Great Cannon program, 134–36, 146–47, 153
GreatFire.org, 136
Great Firewall of China (GFWC), 67–71, 134–36, 147
Great Proletarian Cultural Revolution, 21
Greece, 124
Green Dam software, 71
Ground forces command, 193–94
Gulf War, 24, 53, 56, 85, 94, 104, 115, 138, 156

Hackers, 145, 200
Hard-kill methods, 93, 95, 97, 138, 162
Heightened operations, 153
HMS *Dreadnought,* 89
Hong Kong, 75, 124
Houlin Zhao, 63
Hu Jintao, 2, 12, 35, 57, 159
Human censors of the Internet, 71–72

Hussein, Saddam, 56, 104
Hu Yaobang, 22

Icefog, 124
Implicit filtering, 76
India, 143, 144, 175
Indonesia, 134
Information: accurate data, 84; collection systems, 117; components of systems for military, 117–20; control and Chinese news, 7–13; control to counter political warfare, 55–57; deterrence, 150–54; display systems, 118; growing awareness of importance of, 33–34; integrated network and electronic, 101–2; management systems, 118; and network safeguarding, 144–50; processing, intelligent, 84; real-time, 83, 111; sanctions or blockades, 46; security systems, 120; strategic defense, 53–78; support operations, space, 171–74; transmission systems, 87, 117
Information dominance: campaign guiding thought and, 90–93; Chinese view of space and, 174–76; command and control at the operational level and, 190–93; establishing, 93–105, 120–50; importance of, 35–36; PLA organizations responsible for securing, 181–90; reconnaissance operations and, 121–28; reforms of 2016 and, 193–99; seizing the initiative and, 88–90; space dominance and, 163–64
Informationization, 1–2; bureaucracy and, 5; Department, GSD, 185; increasing, 2–7; space and local wars under conditions of, 157–58
Informationized conflict, 2, 15–16, 37–41; government limitation of the Internet and, 57–72; political warfare as, 41–53
Information operations: defensive, 139–44; defined, 116; deterrence, 150–54; establishing information dominance and, 120–50; heightened, 153; integrated information-firepower warfare (IIFW), 138–39; and network safeguarding, 144–50; offensive, 128–39, 153; psychological, 137; reconnaissance, 121–28; support, 116–20
Information support operations, 116–20
Information technology, focusing high-technology concerns on, 34–36
Information warfare, 16, 38; assessing Chinese views of, 115; at the campaign level, 85–88; command-and-control, 106–9; defined, 79; electronic warfare in, 95–99; emerging forms of, 105–14; growing emphasis on joint operations and, 79–88; integrated information-firepower warfare (IIFW), 138–39; integrated network and electronic warfare (INEW), 101–2, 109, 147; intelligence warfare as, 109–14; network warfare in, 99–102; psychological warfare in, 44–48, 102–5. *See also* Warfare
Information Warfare Monitor, 123
Institute of High Energy Physics, 3
Integrated information-firepower warfare (IIFW), 138–39
Integrated network and electronic warfare (INEW), 101–2, 109, 147
Integrated operations, 90–92
Intelligence: systems, 118–19; warfare, 109–14
International Olympic Committee, 124

International Telecommunications Union (ITU), 7, 62, 63
Internet, the: Central Group for Internet Security and Informationization, 4; China Internet Network Information Center (CNNIC), 7; China's joining of, 3; content providers (ICPs), 65–66; domestic legal controls on, 63–66; government control of social media on, 72–78, 134; government limitation of, 57–72; Great Firewall of China and, 67–71, 134–36; human censors, 71–72; National Internet Registries (NIR), 62; service providers (ISPs), 62–63, 66; sovereignty of, 60–63; technological means of limiting access to, 66–71; use demographics in China, 7
Internet Corporation for Assigned Names and Numbers (ICANN), 61–62
Intrusion detection systems, 147
Iran–Iraq War, 52; Stuxnet attack against, 134
Iraq War, 56–57, 104
"Iron Dome" defense system, 138–39
Islamic State, 144
Israel, 138–39, 149

Japan, 19, 124, 144
Jiang Zemin, 3, 5, 6, 35, 57, 158, 159, 185; People's Liberation Army (PLA) and, 22–26
Jian Yanyong, 73
Jiuquan Satellite Launch Center, 188
Joint campaign command headquarters (JCCH), 43, 190–93, 197
"Joint Campaign Regulations," 30
Joint operations, 27–28; growing emphasis on, 79–88; PLA concepts of coordinated, 30–33; unified C3I system in, 81; unified combat activities in, 82; unified combat systems of systems in, 82; unified command in, 80–81; unified knowledge in, 81; unified operational theory in, 80. *See also* Campaigns
Journalists. *See* News
Journal of the Academy of Equipment, 14
Juntuan plan, 31–34

Kaspersky, 65
Kazakhstan, 62, 124
Keyword searches, backward, 77
Korean War, 19, 24, 28
Kosovo conflict, 31, 51, 94, 99, 104, 115
Kuomintang, 19
Kuwait, 56
Kylin operation system, 148
Kyrgyzstan, 62, 73

Leading Small Groups (LSGs), 3–6
Legal controls on the Internet, 63–66
Legal warfare, 48–51
Liaoning (aircraft carrier), 18
Liberation Army Daily, 187
Li Keqiang, 59
Linux, 148
Liu Yunshan, 59
Logic bombs, 145
Logistics systems, 120
Lu Wei, 4, 59, 60

MacArthur, Douglas, 19
MacKinnon, Rebecca, 54
Mao Zedong, 8, 19, 22, 155
McAfee Security, 124
Microsoft, 145, 148
Military Aerospace, 171
Military Astronautics, 164, 174
Military districts, replacement of, 197
Military region air forces (MRAFs), 32
Milosevic, Slobodan, 31, 51
Ministry of Industry and Information Technology (MIIT), 7, 66
Ministry of Information Industries (MII), 5, 66

Ministry of National Defense (MND), 177
Ministry of National Defense Information Office (MNDIO), 52
Ministry of Public Security (MPS), 63, 70
Missile early warning systems, 172
Mobile computing, 7, 72
Multi-Level Protection Scheme (MLPS), 65
Musk, Elon, 220

National Defense University, 24
National Internet Registries (NIR), 62
National People's Congress (NPC), 64
National Security Agency (NSA), U. S., 145–46
"National Strategy for Informationization Development, 2006–2020," 6
NATO (North Atlantic Treaty Organization), 46, 99, 115, 157
Navigation systems, 119, 132; space, 173
NeoKylin operating system, 148
Netresec, 135
NetTraveler, 124
Network attack, 100–101
Network defense, 101
Network operations, offensive, 132–37
Network reconnaissance, 100, 127–28
Network warfare, 99–102; integrated electronic and, 101–2, 109
"New Generation Operations Regulations," 30
News: Chinese censorship of, 7–13; Chinese efforts to control foreign, 11–13; Internet limitation and, 59–60
New York Times, 11–12, 135, 136
Night Dragon, 124
1984, 78
Ninth Five-Year Plan (1996–2000), 5, 27, 30
Noncontact wars, 25
Nonlinear wars, 25
Nonsymmetric wars, 25–26
North Korea, 49

Obama, Barack, 11, 220
Observe-orient-decide act (OODA), 89, 108, 163
Offense and defense, psychological, 104–5
Offensive information operations, 128–39; electronic, 130–32; key considerations for, 129–30; limited actual, 153; network, 132–37; psychological, 137–39
Omar, Mullah, 50–51
Operation Aurora, 124
Operation Desert Shield/Storm, 56, 156
Operations, information: defensive, 139–44; defined, 116; deterrence, 150–54; establishing information dominance and, 120–50; heightened, 153; integrated information-firepower warfare (IIFW), 138–39; and network safeguarding, 144–50; offensive, 128–39, 153; psychological, 137; reconnaissance, 121–28; support, 116–20
Operations, joint, 27–28; growing emphasis on, 79–88; PLA concepts of coordinated, 30–33; unified C3I system in, 81; unified combat activities in, 82; unified combat systems of systems in, 82; unified command in, 80–81; unified knowledge in, 81; unified operational theory in, 80. *See also* Campaigns
Operations, military space, 160–63
Operations, space: defensive, 169–71; information support, 171–74; strike, 168–69
Operation Shady RAT, 124
"Ordinance of Joint Campaigns of the Chinese People's Liberation Army," 30

Organizational structure, PLA, 177–80
Orwell, George, 78

Passivity among the masses, 143
Peace: deterrence ladder and, 152–53; intelligence warfare straddling war and, 111–12
Peng Guangqian, 151
People's Daily, 8, 9, 59
People's Liberation Army (PLA), 2, 15, 177; Academy of Military Science (AMS), 24; brief history of, 19–26; concepts of coordinated joint operations, 30–33; concepts of political warfare operations, 41–44; cyberespionage by, 122–25; establishing information dominance, 93–105; focusing high-technology concerns on information technology, 34–36; focus on qualitative improvements, 18–19; future warfare views of China and, 200–203; group armies, 21; on information deterrence, 150–54; informationization of conflict and, 37–41; information war at campaign level, 85–88; information warfare and, 79–81; on intelligence warfare, 110; Jiang Zemin and transformations of, 22–26; joint operations and combined arms operations, 27–28; *juntuan* plan, 31–34; on military information systems, 117–20; new historic missions and importance of cyber domain, 35–36; organizational structure, 177–80; organizations responsible for securing information dominance, 181–90; professional military education (PME), 21; pursuing and promoting joint operations, 26–30; reductions in, 22; reforms of 2016 and, 193–99; rise of Deng Xiaoping and decline of "people's war" and, 20–22; thinking on future wars, 13–14; as the world's largest military, 18. *See also* Information dominance; Operations, information
People's Liberation Army Daily, 14
People's Republic of China (PRC): cyberespionage by, 122–25; evolving views of information and power, 1–2, 15–17; government limitation of the Internet, 57–72; informationalized warfare and, 2, 15–16; Leading Small Groups, 3–6; news and control over information, 7–13; policy setting in, 3–4; shaping of future actions of, 203–206; strategic information defense, 53–78; views on information and future warfare, 200–203
Philippines, the, 49
PLA. *See* People's Liberation Army (PLA)
PLA Military Encyclopedia, 156
Policy setting, 3–4
Politburo Standing Committee (PSC), 3–4, 5, 6, 42, 59
Political warfare, 41–53; controlling information to counter, 55–57; legal warfare in, 48–51; PLA concepts of, 41–44; psychological warfare in, 44–48; public opinion warfare in, 51–53; waged through the "three warfares," 44–53
Positioning systems, 119; space, 173
Power and authority, government, 3–4
Precision attacks, 92–93
Professional military education (PME), 21
Professional military journals, PLA, 14
Professional reading materials, PLA, 14
Propaganda department, GSD, 187
Psychological operations: defensive, 142–44; offensive, 137
Psychological passivity among the masses, 143

Psychological reconnaissance, 103–4, 128
Psychological warfare, 44–48, 102–5
Public opinion warfare, 51–53

QQ, 75

Radar networks, 131–32, 186
Real-time information, 83, 111
Reconnaissance: electronic, 97, 126–27; network, 100, 127–28; operations, information, 121–28; psychological, 103–4, 128; space, 171–72; systems, 118–19
Reference materials, PLA, 13
Reforms of 2016, 193–99
Reporters without Borders, 8
Reposts searches, backward, 77–78
Resiliency, 220–21
Rocket force, PLA, 194
ROK (North Korea), 49
Russia, 23, 143, 144, 155, 164; internet governance in, 62; reliance on software attacks, 96. *See also* Soviet Union, the

Safeguarding systems, 120, 144–50
Sanctions, economic, 45
Satellites, 159, 172, 175–76; General Armaments Department and, 188–90. *See also* Space
Schelling, Thomas, 151
Science of Campaigns, The, 80, 90, 158, 191
Science of Military Strategy, The, 137, 151, 158, 164, 171, 185
SecDev Group, 123
Security systems, information, 120
Sensor system, battlefield, 87
Serbia, 99
Sina Weibo, 72, 74, 75–76, 77
Singapore, 49
Sino-Indian War of 1962, 20
Sino-Soviet border clashes of 1969, 20, 23
Sino-Vietnam War of 1979, 20
Six-Day War of 1967, 149
Snowden, Edward, 65, 145
Social media, government control of, 72–78, 134
Soft-kill methods, 93, 95, 96–97, 138, 162
Sohu, 72
Southern Weekly, 9, 10
South Korea, 124, 134, 175
Sovereignty of the Internet, 60–63
Soviet Union, the: conflicts in Asia, 20, 28; joint operations with China, 28; missile early warning satellites, 172; strategic partnership with China, 23. *See also* Russia
Space: -based earth surveying, 174; -based weather observation, 174; blockade, 167; brief review of Chinese capacities in, 158–60; Chinese concepts of military operations in, 160–63; Chinese view of dominance over information and, 174–76; communications and data relay, 172–73; defensive operations, 169–71; dominance and information dominance, 163–64; evolution of Chinese thinking about military, 155–58; force deployments, 166; information support operations, 171–74; and local wars under informationized conditions, 157–58; and local wars under modern, high-technology conditions, 156–57; missile early warning systems, 172; navigation and positioning systems, 173; reconnaissance and surveillance, 171–72; shock and awe strikes, 166–67; strike operations, 168–69
SpaceX, 220
State Administration for Science, Technology, and Industry for National Defense (SASTIND), 7

State Administration of Press and Publication, Radio, Film, and Television (SAPPRFT), 8–9, 11
State Council Informationization Work Leading Small Group, 4–5
State Council Information Office, 8
State Economic Informationization Joint Council, 3
State Informationization Leading Small Group (SILSG), 5–6, 7
State Internet Information Office (SIIO), 59–60
Strategem, 114
Strategic information defense, 53–55; countering political warfare using, 55–57
Strategic Support Force, PLA, 194
Stuxnet attack, 134
Surveillance systems, 118–19, 141; space, 171–72
Symantec, 65
Synthetic aperture radar (SAR), 127
Systems of systems, 86–87, 133

Tactical defensive measures, 141
Taiwan, 62, 124, 144, 175
Taiyuan Satellite Launch Center, 188–89
Taliban, the, 46, 115
Teaching materials, PLA, 13–14
Technical Reconnaissance Bureaus (TRB), 182
Tencent, 72, 74, 75
Tenth Five-Year Plan (2001–2005), 6
Terracotta network, 136–37
Terrorism, 144
Textbooks, PLA, 13
Thailand, 49
Third Department, GSD, 181–85
"Three warfares," 42, 44–53
Tiananmen Square massacre, 23, 53, 56, 77
Tibet, 54, 124, 144
Timing systems, 119
Titan Rain, 125
Translations, 17
TT&C Network, 189–90
Twitter, 72, 73, 74, 134

Ubuntu, 148
Uighur people, 124, 144
Ukraine, 73
Unified C3I system, 81
Unified combat activities, 82
Unified combat systems of systems, 82
Unified command, 80–81
Unified knowledge, 81
Unified operational theory, 80
United Airlines, 123
United Kingdom, the, 28–29; British Meteorological Office, 99; HMS *Dreadnought,* 89
United Nations: Convention on the Law of the Sea, 49; Development Programme (UNDP), 183
United States, the, 155, 200; Afghanistan War and, 46, 50–51, 53, 115; armed forces, 27, 125, 197; cyberespionage against, 122–25; Federal Communications Commission, 132; Gulf War and, 53, 56, 85, 94, 104, 115, 138, 156; implications of Chinese view on future warfare for, 206–11; information blockade on the Taliban, 46; informationization organizations, 185; informationized warfare by, 51; Iraq War and, 56–57, 104; keeping calm and carrying on, 221; Kosovo conflict, 31, 51, 94, 99, 104, 115; missile early warning satellites, 172; National Defense Strategy, 2008 50; National Security Agency, 145–46; Operation Desert Storm, 56; policy options for, 211–21; promoting resiliency and diversification, 220–21; promoting "whole-of-society" participation, 219–20; USS *Theodore Roosevelt,* 99
USS *Theodore Roosevelt,* 99

Vietnam War, 20
Virgin Galactic, 220
Virtual private networks (VPNs), 69–70, 133, 136

Wall Street Journal, 12
Wang Chen, 59
Warfare: command-and-control, 106–9; electronic, 95–99; how China sees information and future, 200–203; integrated information-firepower, 138–39; intelligence, 109–14; joint operations and combined arms operations, 27–28, 30–33; legal, 48–51; levels of, 31; local wars under modern conditions, 26; network, 99–102; noncontact, 25; nonlinear, 25; nonsymmetric, 25–26; political, 41–53; precision attacks, 92–93; psychological, 44–48, 102–5; public opinion, 51–53; real-time information in, 83, 111; as science, 27. *See also* Informationized conflict; Information warfare; Joint operations
Wargames and exercises, 153
War Powers Act, 49
Weaknesses of political indoctrination, 143
Weather observation, space-based, 174
"Westernization," 57–58
"Whole-of-society" participation, 219–20
World Economic Forum, 60
World Press Freedom Index, 8
World Trade Organization, 49
World War II, 24, 28, 119

Xi'an Satellite Telemetry and Control Center, 189
Xichang Satellite Launch Center, 160, 189
Xi Jinping, 4, 11, 12, 159, 161; emphasis on information security and Internet control, 58–59, 60, 204; reforms of 2016 and, 193
Xinhua News Agency, 8, 59
Xinjiang region, 54–55
Xu Qinxian, 56

Yao Youzhi, 151
Yom Kippur War of 1973, 149
Youku, 74
YouTube, 74

Zhang Xinfeng, 59
Zhao Ziyang, 22
Zhu Rongji, 5–6
Zou Jiahua, 4

About the Author

DEAN CHENG is senior research fellow for Chinese political and security affairs in the Asia Studies Center at the Heritage Foundation. He has worked at the Center for Naval Analyses, Science Applications International Corporation, and the U.S. Congress's Office of Technology Assessment. Cheng has written extensively on Chinese military and security developments; testified before Congress; and spoken at the Army War College, National Defense University, and U.S. Air Force Academy.