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

Chapter 1

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.

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 countercountermeasures. 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.