NIDS CHINA SECURITY REPORT

NIDS China Security Report 2021

China's Military Strategy in the New Era

National Institute for Defense Studies, Japan

NIDS China Security Report 2021

China's Military Strategy in the New Era

Published by
The National Institute for Defense Studies
5-1 Honmura-cho, Ichigaya, Shinjuku-ku, Tokyo 162-8808 Japan
Website: http://www.nids.mod.go.jp

Translated by INTERBOOKS

The China Security Report 2021 comprises NIDS researchers' analyses and descriptions based on information compiled from open sources in Japan and overseas. The statements contained herein do not necessarily represent the official position of the Government of Japan or the Ministry of Defense.

This publication is a translation of the Japanese version originally published in November 2020.

ISBN978-4-86482-088-2 Printed in Japan

NIDS China Security Report 2021

Contents

Preface

The *NIDS China Security Report* published by the National Institute for Defense Studies (NIDS) was first released in March 2011. It is not difficult to find differences between this report—the 11th in this series—and the inaugural issue. Unlike the *East Asian Strategic Review* which takes an annual, fixed-point observation style, the *NIDS China Security Report* sets a particular theme each time and provides a detailed analysis related to China's military affairs and security from a mid- to long-term perspective. Initially, the report was written by several researchers studying China and Taiwan, and analyses focused on China's diplomacy, maritime policy, and the modernization of the People's Liberation Army (PLA). Beginning with the seventh issue, the report gradually broadened the scope of analysis, and has dealt with relations between China and countries/regions such as Taiwan, the United States, Southeast Asia, South Asia, Pacific Island countries, Russia, and Central Asia. Accordingly, the writing team was expanded to include not only members of the China Division but also experts on other regions as well as researchers of specific issues. Thus, the *NIDS China Security Report* has evolved into a platform for analyzing China by many NIDS researchers, and has become one of the flagship publications of NIDS that attracts significant interest from research institutes and the media in various countries and regions.

This latest *China Security Report 2021* selected Yatsuzuka Masaaki as the lead author. The report focuses on the PLA's efforts to use science and technology for military purposes. The primary areas of analysis are: the new cyber and space domains that are garnering attention; and China's military-civil fusion strategy aimed at making military use of science and technology. It further seeks to put in context and analyze China's concepts of informatized warfare and intelligentized warfare, taking into account changes in China's military strategy from Mao Zedong's era through the Xi Jinping administration. In writing this report, the authors have endeavored to present an objective analysis while taking note of suggestions gained by exchanging views with researchers, experts, and research institutes in Japan and abroad. While their names cannot be listed here, we would like to take this opportunity to express our deepest gratitude to everyone who supported us.

The *China Security Report 2021* has been written by Yatsuzuka Masaaki (the lead author and author of Introduction, Chapters 2 and 4, and Conclusions), Fukushima Yasuhito (Chapter 3), Iwamoto Hiroshi (Chapter 4), and Momma Rira (Chapter 1). The report has been written solely from the viewpoints of the individual researchers and does not represent an official view of the Japanese Government, the Ministry of Defense, or NIDS. The editorial team is led by Momma Rira (editor-in-chief), and includes Iida Masafumi (deputy editor-in-chief), Ohnishi Ken (editor of the Japanese edition), Jingushi Akira (editor of the English edition), Iwamoto Hiroshi (editor of the Chinese edition), Arie Koichi, Nakagawa Misa, Tanaka Ryosuke, Yatsuzuka Masaaki, and Fukushima Yasuhito.

The authors of the *China Security Report 2021* hope that it will contribute to a deepening of policy discussions concerning China at home and abroad, alongside dialogue, exchange, and cooperation among countries and regions regarding security.

November 2020
Momma Rira
Director, Regional Studies Department
The National Institute for Defense Studies

Summary

Chapter 1　China's Preparations for Informatized Warfare

In China, to date, the "active defense" military strategy has been adopted consistently. Gradually, it began to emphasize preemptive attacks as Mao Zedong and other leaders of the Chinese Communist Party of each period provided guidance to the army. Active defense in Mao Zedong's era was premised on "striking only after the enemy has struck [*houfa zhiren*, 后发制人]." In Deng Xiaoping's era, local war using conventional weapons was elevated to strategic level, and the active defense strategy came to encapsulate the concept of preemptive attack conceived in local wars. In Jiang Zemin's era, the goal was to win "local wars under high-tech conditions." As Hu Jintao's era neared, however, China recognized the importance of information in warfare, and the goal became winning "local wars under the conditions of informationization." Emphasis was now given to the growing importance of preemptive attacks.

After Xi Jinping came to power, China's aim shifted to winning informatized warfare that makes effective use of new domains, including space, cyber, and electromagnetic. In such warfare, armed forces, which are placed under unified command by eliminating barriers between military services and branches, strike physical targets based on human judgment. Furthermore, when China enters the phase of intelligentized warfare [*zhinenghua zhanzheng*, 智能化战争], it will have created a command system that integrates humans and machinery, in which artificial intelligence and game theory will be utilized to accurately analyze and determine the opponent's intentions. This information will then be relayed to commanders to make command and strategic decisions. The targets of attack in the intelligentized warfare will include not only physical objects but also nontangible targets in cyber and cognitive spaces.

Chapter 2　China's Cyber Strategy

The People's Liberation Army (PLA) has proceeded with its own informatization and evolved its cyber strategy, recognizing that "information dominance" is crucial for seizing core initiative in modern warfare. In this process, the Strategic Support Force (SSF) was established in late 2015. It appears that the SSF is responsible for achieving information dominance as well as providing information support for joint operations, including the space, cyber, and electromagnetic domains, and converting advanced technologies into military capabilities. To achieve information dominance, the PLA also attaches importance to information warfare and cyber operations for information theft in peacetime, as well as cyber attacks that preempt the enemy in the early stages of war.

At the same time, as a result of the informatization of the PLA which has deepened its dependence on information systems for military operations and foreign capital's inflow into the

information industry, concerns over security vulnerabilities are heightening within the PLA. To cope with these challenges, it has sought to indigenize core technologies and train specialists in the cyber field. Moreover, from the perspective of information dominance, the Chinese government strives to take the lead in expanding international norms and standards related to cyberspace. China's active efforts in cyberspace have, however, sparked alarm and harsh responses in the United States.

Chapter 3 China's Military Use of Space

China's space activities from their inception have been closely linked to military activities. However, it was only from the 1990s through the 2000s that the military value of space began to be recognized more widely in the PLA. Through observing other countries' wars, including the Gulf War, the PLA arrived at the view that information dominance was key to winning modern warfare, and that to this end space dominance was needed. Furthermore, the PLA considers space as an essential domain for the prospective intelligentized warfare.

The PLA uses space to provide information support for operations on land, sea, and air and is also developing capabilities to disrupt other countries' use of space. In China, emerging space enterprises have rapidly boosted their technological capabilities with government and military support. The future is expected to herald an era in which the military adopts the technologies developed by the private sector and uses their services.

China and the United States are highly wary of each other's activities in the space domain, and recently, the moon and surrounding area are beginning to become a new area of competition between the two countries. In 2019, India conducted a destructive ASAT test, likely with the intention of acquiring a deterrent against China. Meanwhile, a number of nations are eager to work with China in space activities, and China is enthusiastic about pursuing cooperation in such fields as arms control, satellite positioning, and space situational awareness.

Chapter 4 China's Military-Civil Fusion Strategy

In China, military capabilities are being enhanced through military-civil fusion (MCF) under the Xi Jinping administration. The MCF strategy advanced by the Xi administration aims to strengthen military capabilities and promote national development by tying together the military and socio-economy. Since its establishment, the PLA has maintained close relations with the private sector, including participating in production activities. However, this relationship has changed with the times. As science and technology takes on an increasing role in the security sector, and against the backdrop of the rising technological level of China's private companies in the shift to a market economy, emphasis has been placed on MCF to enhance the military capabilities of the PLA.

The Xi administration created the Central Commission for Military-Civil Fusion Development,

a powerful organization. It has launched measures in succession to ensure the smooth implementation of MCF. In conjunction, the commission promotes the prioritization of science, technology, and industry for national defense in new security domains, the active use of cutting-edge technologies for military purposes, and indigenization of core technologies. While China is advancing MCF internally, it also seeks to introduce overseas technologies through active investments and technology exchanges with foreign countries. This has fueled security concerns in the West and has led to their strengthening of trade and investment regulations.

Acronyms and Abbreviations

5G	fifth generation mobile communications system
AI	artificial intelligence
APOSOS	Asia-Pacific Ground-Based Space Object Observation System
APSCO	Asia-Pacific Space Cooperation Organization
APT	Advanced Persistent Threat
ASAT	anti-satellite
BDS	BeiDou Navigation Satellite System
C4ADS	Center for Advanced Defense Studies
C4ISR	command, control, communications, computers, intelligence, surveillance, reconnaissance
CASC	China Aerospace Science and Technology Corporation
CASIC	China Aerospace Science and Industry Corporation
CCP	Chinese Communist Party
CD	Conference on Disarmament
CETC	China Electronics Technology Group Corporation
CFIUS	Committee on Foreign Investment in the United States
CHEOS	China High-resolution Earth Observation System
CMC	Central Military Commission
COVID-19	coronavirus disease
DIA	Defense Intelligence Agency
EU	European Union
GAD	General Armament Department
GEO	geostationary orbit
GPD	General Political Department
GPS	Global Positioning System
GSD	General Staff Department
ICT	information communications technology
IGBT	power semiconductor device
IoT	Internet of Things
ITU	International Telecommunication Union
LEO	low Earth orbit
MCF	military-civil fusion
MIIT	Ministry of Industry and Information Technology
MND	Ministry of National Defense
NATO	North Atlantic Treaty Organization
NCSS	National Cyberspace Security Strategy
NDWP	National Defense White Paper
PLA	People's Liberation Army
PNT	positioning, navigation, and timing
PPWT	Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects
PRC	People's Republic of China
RMA	revolution in military affairs
RPO	rendezvous and proximity operation
S&T	science and technology
SASTIND	State Administration of Science, Technology and Industry for National Defense
SMS	*Science of Military Strategy*
SSA	space situational awareness
SSF	Strategic Support Force
TEL	transporter-erector-launcher
TT&C	telemetry, tracking, and control
UAV	unmanned aerial vehicle
UN	United Nations

Introduction

Yatsuzuka Masaaki

Introduction

The Chinese People's Liberation Army (PLA) has stepped up efforts to enhance its military capabilities through introducing advanced technologies. In a speech delivered to the 19th National Congress of the Chinese Communist Party (CCP) held in October 2017, President Xi Jinping (CCP General Secretary) stated a long-term goal of turning the PLA into "world-class forces" by the middle of this century. "World-class forces" implies becoming a military power commensurate with the United States. The large-scale PLA reforms under the Xi Jinping administration are precisely for realizing this goal. In this speech, he articulated the importance of the PLA's incorporation of scientific and technological achievements for building "world-class forces," vowing: "We must keep it firm in our minds that technology is the core combat capability, encourage innovations in major technologies, and conduct innovations independently. We will strengthen the system for training military personnel, and make our people's forces more innovative."[1]

It is believed that behind such remarks by President Xi Jinping lies a perception that strengthening military capabilities centered around science and technology (S&T) will be key to overturning the PLA's military inferiority to the U.S. forces. He sets forth "strengthening the military through S&T [*keji qiangjun*, 科技强军]" as one of his policies for building up the PLA. Against this backdrop, in the National Defense White Paper *China's National Defense in the New Era* published in July 2019 (NDWP 2019), the PLA expressed the following view: "Driven by the new round of technological and industrial revolution, the application of cutting-edge technologies such as artificial intelligence (AI), quantum information, big data, cloud computing and the Internet of Things (IoT) is gathering pace in the military field." The PLA perceives that military use of such state-of-the-art technologies holds the key to the fate of future warfare, and that progressively adopting the new trend for military revolution may enable the PLA to "overtake [the U.S. forces] at the bend [*wandao chaoche*, 弯道超车]."[2]

The PLA's pursuit of military use of S&T is evident in the restructuring of its military strategy and development of military capabilities in new security domains. Regarding the prevailing form of warfare, the PLA indicated in NDWP 2019 that "War is evolving in form towards informationized warfare, and intelligent warfare [*zhinenghua zhanzheng*, 智能化战争] is on the horizon." Intelligentized warfare is described as "integrated warfare waged in land, sea, air, space, electromagnetic, cyber, and cognitive domains using intelligent weaponry and equipment and their associated operation methods, underpinned by the IoT information system."[3] In July 2019, the PLA announced the formulation of "The Military Strategic Guideline for a New Era" to adapt to changes in the form of warfare.[4] In short, the PLA is in the midst of building a military force for what China calls the "new era" in order to win this intelligentized warfare.

A clear-cut example of how military capabilities are being developed for intelligentized warfare is the establishment of the Strategic Support Force (SSF) as part of the military reforms. It is

thought that the SSF is tasked with the military use of new security domains, including space, cyber, and electromagnetic domains, and is also in charge of the military use of AI, robotics, nanotechnology, and other advanced technologies. The establishment of such a force is garnering attention as an illustration of the PLA's priority on the military value of new security domains.

Meanwhile, to understand this issue, it cannot be overlooked that the PLA's recent moves to make military use of advanced technologies extend to the mobilization of China's societal and private-sector resources. The Xi Jinping administration identifies S&T promotion as a national project for achieving the "Chinese Dream" of "the great rejuvenation of the Chinese nation," reasoning that "an innovation-driven development strategy determines the future destiny of the Chinese nation."[5] Furthermore, recent S&T have an increasingly dual-use nature (i.e., both military and civilian applications) with versatility, and many advanced technologies developed by the private sector can be diverted to military use. To encourage the transformation of wide-ranging private sector-led innovations into military technologies, the Xi administration actively promotes the "military-civil fusion strategy" as a national strategy.

These efforts of the Chinese government to use S&T for military purposes have sent shock waves through the international community, primarily developed countries in the West. The reason is: if China gains military capabilities and voice in new security domains governed by international norms that are still immature, this will unmistakably have significant implications for the future international order. In addition, there are emerging concerns that foreign trade and investments by Chinese companies—heretofore not perceived as a security issue—may prompt the outflow of technologies, information, and talent from developed countries and lead to strengthening the PLA's military capabilities. Consequently, the West is quickening efforts to institute more stringent trade and investment regulations that take account of Chinese companies. China, as a country whose economic growth has been founded on exchanges with foreign countries, cannot afford to disregard such changes in the international environment.

As noted above, the PLA seeks to bolster military capabilities by using advanced technologies. How are these initiatives positioned in China's military strategy in the new era, and how will they affect the international security environment? To answer these questions, it is necessary to analyze the PLA's military strategy in the new era with case studies and shed light on the international community's responses to the PLA's moves. This report therefore takes the following structure. Chapter 1 examines the evolution of the PLA's military strategy and the direction that the military strategy will take in the new era. The remaining chapters are devoted to case studies. Chapter 2 considers the cyber strategy of the PLA based on its organizational trends, including the SSF, and their cyber warfare concepts. Chapter 3 sheds light on the PLA's use of outer space that is gaining attention as a new strategic high ground. Chapter 4 analyzes China's efforts related to the military-civil fusion strategy aimed at military use of S&T and then discusses their impacts on the international security environment.

This page is intentionally left blank

Chapter 1

China's Preparations for Informatized Warfare

Momma Rira

1. Changes in China's Military Strategy

(1) The Era of Mao Zedong (1927–1976)[1]: The Curse of the Final War and Active Defense

China's military strategy stipulates the operational doctrine of the People's Liberation Army (PLA), force structure, and training, according to M. Taylor Fravel, professor at Massachusetts Institute of Technology.[2] "Active defense," the essence of Mao Zedong's military strategy, has been upheld as China's military strategy to the present day.[3] While the term "active defense" has been used consistently from the eras of Mao Zedong to Xi Jinping, its meaning has been changing gradually over the years that Mao and other Chinese Communist Party (CCP) leaders exercised leadership over the CCP Army.[4] This has been influenced by factors such as China's state power, international environment, changes in industrial structure, and advances in military technology.

The concept of active defense was articulated explicitly for the first time in Chapter V of *Problems of Strategy in China's Revolutionary War* (1936)—one of Mao's writings that most systematically describes his military thought and military theory. In this work, Mao, citing historical events, advocates the importance of luring the enemy deep into one's base, waiting for an opportunity to counterattack, and launching a counterattack when the enemy's supplies run short. "The only real defense is active defense, defense for the purpose of counterattacking and taking the offensive."[5] As Mao's comment indicates, active defense has offensive implications.

However, the active defense strategy calls for turning one's base into a battlefield and thus required tolerance for damages inflicted on the people and the land of CCP-controlled areas. Underlying circumstances enabled the "lure the enemy troops in deep" operations under the military strategic guideline of active defense. Namely, the areas controlled by the CCP at the time were rural areas, which meant that even if enemy troops were lured deep into a base, it did not cause total devastation of agriculture, a primary industry employing the people. These operations would likely have been impossible if the CCP and its Army at the time were a political party and a military force based in urban areas.

Following the CCP's victory in the Chinese Civil War and the founding of the People's Republic of China (PRC), "lure the enemy troops in deep" was no longer a viable starting point for a counterattack, even if the active defense strategy was maintained. The reason is that, while the purpose of the civil war was successful revolution, the founding of the PRC made it necessary for the CCP to protect the nation. Under such circumstance, the PLA created the Navy in April 1949 and the Air Force in November of the same year, expanding its area of activity from land to sea and airspace. At a meeting of the Secretariat of the CCP Central Committee in April 1955, Mao Zedong stated, "China's strategic guideline is active defense; it never strikes first" [*houfa zhiren*, 后发制人]. Active defense was formally established as a military strategic guideline at an expanded meeting of

the Central Military Commission (CMC) on March 6, 1956.[6]

Meanwhile, amidst the U.S.-Soviet confrontation during the Cold War, there was a growing recognition within China's leadership that the final war (nuclear war) was approaching. In March 1955, at the CCP National Congress, Mao Zedong raised the possibility of a war with imperial powers.[7] Mao urged that China must be prepared to fight a decade-long World War III, projected that the capitalist world would no longer exist when the war comes to an end, and at times advocated that imperialism had to be eliminated.[8] For China to survive this final war, it was essential for the country itself to develop and possess nuclear weapons and secure their delivery systems. China conducted its first successful nuclear test in October 1964, followed by its first successful hydrogen bomb test in June 1967, and created the Second Artillery Force in August 1966 (reorganized into the Rocket Force in December 2015). Ever since the postwar period when the economy had not yet prospered, China determined which science and technologies (S&T) had primacy for maintaining the nation and eventually secured them.

From the mid-1960s to the early 1970s, China's relations deteriorated with not only the United States but also the Soviet Union. Coupled with a border dispute with India, China had to deal with threats on three fronts.[9] This situation was eased to some extent by President Richard Nixon's visit to China in 1972, leaving only the Soviet Union as a major threat.[10] Subsequently, the Cultural Revolution ended, and until Deng Xiaoping took over the reins of power, no significant changes were made to Mao Zedong's military strategic concept of active defense which assumed an outbreak of a final war.

As seen, "lure the enemy troops in deep" under this strategy is not only a spatial concept of luring enemy troops deep into one's territory; it also has a temporal dimension of luring enemy troops into a long war. This is reflected very much in Mao Zedong's work, "On Protracted War" (1938), which explains the logic that while China cannot immediately defeat the massive Imperial Japanese Army, it can win the Chinese people over to its side, endure, gradually reverse the situation, and ultimately achieve victory.

(2) The Era of Deng Xiaoping (1976–1989): A Break from the Final War and a Shift to Local War

Deng Xiaoping is known for adopting the "Reform and Opening Up" policy and improving China's relations with the West. The background underlying this change was Deng's forecast that "a large world war will not occur for a relatively long period, and we can stay hopeful that world peace will be maintained."[11] While China could not rule out the possibility of local wars or armed clashes with neighboring states over territory and maritime interests,[12] the PLA shifted from a war readiness posture to building a military force for a relatively peaceful period.[13] As a result, the notion gained traction in China that expected wars in the future are local wars using conventional weapons.

In 1985, the CMC adopted a new military strategic guideline to prepare for "local wars under

modern conditions."[14] In connection with Deng Xiaoping's adherence to active defense under modern conditions, Liu Jixian, Vice President of the PLA Academy of Military Science, explained the need to adapt flexibly to small and medium local wars and to struggles to defend territory and the sea for protecting national sovereignty.[15] From this wording, it can be read that the PLA was ready to allow preemptive attacks as necessary. The active defense strategy from Mao Zedong's era is based on "striking only after the enemy has struck," i.e., luring the enemy into one's territory and then making a counterattack. However, steady progress in China's "Reform and Opening Up," along with full-scale development of industrial areas mainly in coastal areas, meant such a strategy would result in actions too late and have direct implications on the fate of the nation. Herein also lies the reason that Liu Huaqing was able to press forward with naval modernization backed by Deng Xiaoping during this period.[16]

In late 1988, China shifted the basis of preparations for military struggle from full-scale anti-aggression war to armed conflicts and local wars. Local wars were traditionally considered campaign-level operations. A campaign consists of several battles that are waged to complete an established strategy, and is positioned at the lower levels of a strategy.[17] After this shift, however, local war was elevated to the status of strategic level. This brought to the surface the aspect of "striking the enemy first (preemptive attack)" inherent in local wars, and the active defense strategy came to embody the conflicting concepts of "striking only after the enemy has struck" and "striking the enemy first," according to Saito Makoto, research fellow of the National Institute for Defense Studies.[18] On this point, professor Andrew J. Nathan of Columbia University and others note that the CMC at the time reconstructed Mao Zedong's concept of "active defense" from a tactical and operational tenet to a strategic-level principle, and that the PLA decided it would prepare to make a preemptive attack if it is necessary to interdict an imminent attack or prevent a rapid decline in capabilities to secure their claimed territories.[19]

Deng Xiaoping himself states that active defense is not just any defense but making advances and attacks while defending.[20] Nevertheless, not even Deng Xiaoping could completely cast aside the influences of Mao Zedong's military thought, and terms and phrases such as "active defense," "striking only after the enemy has struck," and "people's war" remained. Therefore, Deng Xiaoping decided to adapt these terms and phrases by changing their implications while leaving the terms and phrases intact. He did this by formulating a new military strategy known as "local wars under modern conditions," namely, wars that use conventional weapons, do not let an enemy enter one's territory, and do not turn the whole country into a battlefield.

Waging a conventional war under modern conditions requires updating weapons and equipment to those commensurate with such conditions. The "Four Modernizations" proposed by Zhou Enlai and inherited by Deng Xiaoping include defense and S&T, in addition to agriculture and industry. The modernizations of defense and S&T were intricately linked. Rather than defense modernization, including development and acquisition of PLA weapons and equipment, Deng

Xiaoping gave priority to economic development by introducing advanced S&T from the West and injecting significant financing. Under these circumstances, Deng sought to modernize the PLA that can execute "local wars under modern conditions" while implementing bold troop reductions. Modernization of PLA weapons and equipment had to wait until a considerable budget was allocated in Jiang Zemin's era.

(3) The Era of Jiang Zemin (1989–2004): Local Wars under High-Tech Conditions

The Gulf War began in early 1991, a little over a year after Jiang Zemin took over Deng Xiaoping as Chairman of the CMC in November 1989. The sight of Iraqi forces overwhelmed by U.S. forces using high-tech weapons shocked Jiang Zemin and other members of the party leadership as well as senior officers of the PLA. While acknowledging shortly after the war that high-tech weapons were important, some PLA members contended that the fundamental elements that determine victory or defeat were still: the nature of the war; endorsement of the masses; and the quality of military personnel.[21] The PLA subsequently continued to uphold this view, which was in line with the thinking of the people's war. In 1993, however, Jiang Zemin's military leadership set the goal of winning "local wars under high-tech conditions."[22] Furthermore, in December 1995, the CMC made it clear that it would implement the "Science and Technology Power Strategy," announcing the transitions from quantitative scale to qualitative effect and from labor intensive to S&T intensive.[23] Based on this trend, it is understandable that troop strength was reduced during Jiang Zemin's era from 500,000 personnel in 1997 to 200,000 personnel in 2003.[24]

Notwithstanding the unveiling of the "local wars under high-tech conditions" military strategic guideline in 1993, the concept did not appear in official documents until April 1995.[25] It hints at military disagreement over the military strategic guideline and over the establishment of Jiang Zemin's military leadership structure, and that it had failed to gain agreement.[26] In addition, there was inadequate understanding of high tech within the PLA. General Fu Quanyou, PLA Chief of General Staff from 1995 to 2002, made high-tech awareness an "urgent matter" for the duties of the General Staff Department and encouraged its officers to learn about high tech.[27]

"Local wars under high-tech conditions" gradually gained acceptance in the PLA, owing to senior officers' realization that command, control, communications, computers, intelligence, surveillance,

reconnaissance (C4ISR), alongside firepower and mobility, constituted assets critical for winning a war. Although high tech came to be understood at last, key leaders of the PLA stopped using the phrase, "local wars under high-tech conditions," from around 2002. According to Chinese security expert professor Asano Ryo at Doshisha University, this was because at this point the leaders began to foreshadow that the future form of warfare was informatized warfare.[28]

(4) The Era of Hu Jintao (2004–2012): Informatized Local Wars

The military thought in Hu Jintao's era is considered to have maintained Mao Zedong's military thought, Deng Xiaoping's thought on army building in the new period, and Jiang Zemin's thought on defense and army building.[29] In 2004, Hu Jintao's military leadership set out "winning local wars under the conditions of informationization." The change from "under high-tech conditions" to "under the conditions of informationization" was influenced by post-Gulf War events, namely, the Kosovo War (1999), the War in Afghanistan (2001), and the Iraq War (2003).[30] "Local wars under high-tech conditions" recognized the importance of C4ISR and employed precision-guided munitions, but they were meant for destroying physical targets. Simply put, high-tech weapons at the time were an extension of mechanized warfare. In contrast, the target of attacks in informatized warfare did not necessarily exist in physical space. The National Defense White Paper published in 2006 during Hu Jintao's era states that the PLA would adhere to the military strategic guideline of active defense, and taking mechanization as its foundation, lead informatization of the PLA and promote the composite development of informatization and mechanization. With respect to the buildup of each military service, the white paper makes explicit that the PLA would accelerate upgrades of the Army's main equipment to adapt to informatization, enhance maritime information systems, build an informatized air fighting force, and raise the informatization level of the Second Artillery Force's weaponry and equipment systems.

It can be inferred from such statements that the PLA shifted its focus to informatization. The white paper adds that to become an armed force compatible with "local wars under the conditions of informationization," the PLA will transform into a more compact force, integrate force formation, intelligentize force command and operational means, and promote force modularization. The PLA repeatedly downsized the troop strength beginning from Deng Xiaoping's era through Hu Jintao's era, making the Army the focus of force reduction. The Army also increased the number of combined corps based on a system of corps, brigade, and battalion, and established numerous new high-tech equipment units. Looking ahead to fighting in informatized battlefields in the future, the PLA aspired to transition to a force that enables integrated operations of military services and branches. To this end, it aimed to: (1) automate and intelligentize command and control means in an advanced manner; and (2) introduce large quantities of intelligent weapons systems and platforms into the military force and into operations.[31]

The parallel achievement of mechanization and informatization of the PLA is not necessarily

a contradiction in principle; however, this is difficult to realize in reality due to budget competition between the two, coupled with involvement of organizational and individual gains.[32] The informatization-focused posture was likely decided by the end of 2007, the year that the first Party Congress was held after Hu Jintao seized control of the CMC. CMC Chairman Hu stated that enhancing the capability to win "local wars under the conditions of informationization" will serve as an adequate foundation for resolving other military tasks. Hence he decided to actively shift from training for mechanization conditions to training for informatization conditions in order to strengthen the capability to win "local wars under the conditions of informationization."[33] In his report to the 17th CCP National Congress in 2012, the last report he made as General Secretary and CMC Chairman, Hu Jintao vowed to enhance the capability to accomplish diverse military tasks, at the core of which was the capability for "local wars under the conditions of informationization" Emphasis began to be placed on keeping with the modernization of army building and advancement through informatization, along with accelerating and advancing informatization building.[34] Hu's report suggests that the PLA placed greater priority on informatization than on mechanization.

As observed above, preparations for transitioning from the strategy of "local wars under high-tech conditions" to the strategy of "local wars under the conditions of informationization" had been under way since the end of the Jiang Zemin administration. The Iraq War made this shift decisive and led to formal actions in the era of Hu Jintao. As some considerations were initially given to mechanization that the PLA had long strived for, mechanization was pursued in tandem with informatization.

China began to actively focus on non-warfare military activities during the Hu Jintao administration,[35] and from December 2008, sent naval vessels to waters off the coast of Somalia and the Gulf of Aden to conduct counter-piracy operations. These activities are believed to have prompted the PLA, which conducts a range of activities in remote regions from mainland China, to recognize the importance of collecting, analyzing, processing, and transmitting reliable intelligence accurately, quickly, and without interference, in addition to the importance of intelligence in military activities from operating to replenishing units. The activities also led the PLA to reexamine which unit formations as well as weaponry and equipment were commensurate with such activities. It is thought that in this process the PLA became increasingly aware of the importance of new domains such as the space, cyber, and electromagnetic domains that support military activities.

2. The Era of Xi Jinping (2012–Present): Shift to Informatized Warfare and Intelligentized Warfare

(1) Informatized Warfare

Unveiled in Hu Jintao's era, the military strategic guideline of "local wars under the conditions of

informationization" began to be pursued seriously under the Xi Jinping administration. The 2015 edition of *Science of Military Strategy* (SMS) published by the National Defense University notes that "informationized local wars" have the following general characteristics.[36] First, "informationized local wars" are susceptible to the impacts of global politics and the world economy, given the multipolarization trend, strategic coordination and cooperation among major powers, and growing inter-linkages and interdependence of economies under globalization. At the same time, wars are increasingly constrained by social factors, such that domestic and international public opinion inevitably influences leaders' war guidance and decisions. Secondly, as the side which has superior intelligence capabilities and which can convert them effectively into policy decisions and command can seize the initiative in strategy and the battlefield, "information dominance" is a prerequisite for achieving dominance in air, sea, and other domains. Thirdly, the battlefield is multidimensional, expanding to include not only confrontations in tangible battlefields such as land, sea, airspace, and space, but also intangible battlefields such as electromagnetic, cyberspace, and cognitive domains. As a result, wars are more sophisticated and three-dimensional, and accordingly, the battlefield space will rapidly expand to outside one's borders. To this end, air and space battlefields will merge and integrate and become a strategic high ground for seizing the initiative in war. Fourthly, due to the "systems confrontation" nature of "informationized local wars," integrated joint operations will gradually become the basic operation format. Seamlessly linked operational capabilities of military services, branches, and domains are unified under the command of a unified organization. Fifthly, war progress, strike target, and means are controlled accurately, and "informationized local wars" will further shift to low-risk, low-cost small and medium precision operations with high efficiency and high cost effectiveness.

Furthermore, the 2015 edition of SMS emphasizes the offensive aspect of the active defense strategic thought. The book highlights the plausible characteristics of China's "informationized local wars," notably, informatized maneuvers with ambiguous operational stage classifications, continuously improving medium- and long-range precision strike capabilities, and faster-paced operations. Based on this trend, the book notes that "preemptive attacks" have gained further importance and that the strategic status of offensive operations is higher than ever.

On the other hand, the book also notes the challenges of fighting "informationized local wars." First, it states that many countries may intervene in wars over maintaining unification of the motherland, national territorial sovereignty, and maritime interests that China may face in the future. The book adds that, in these times of political multipolarization, economic globalization, and social informatization, China confronts increasingly multidimensional and complex security threats and that the threats may cause a chain reaction. The 2015 edition of SMS stresses the need to prevent chain reactions, and if such reactions occur, to be aware of the strategic center of gravity in order to provide accurate strategic guidance. In addition, the book states that, while China is increasing the number of informatized weaponry and equipment and has rudimentary information system

operational capability, mechanized equipment still make up a relatively large part of China's weaponry and equipment and little progress has been made in integrating the comprehensive logistics support system necessary for intelligence, command and control, firepower attacks, and operation execution. Regarding the space, cyber, and electromagnetic domains, the book notes that China has some technological means and is enhancing medium- and long-range strike capabilities on the one hand, while on the other hand it still has low-level capabilities to control them and to keep abreast of the real-time situation of battlefields and to know and assess the effects of the attacks.[37]

Predating this book, the 2013 edition of *The Science of Military Strategy* was published by the PLA Academy of Military Science following the inauguration of the Xi Jinping administration. Interestingly, this edition already foreshadowed that future wars will be "informationized warfare" that focuses on using advanced information operational capabilities to conduct efficient joint operations and on using non-physical means such as cyber attacks to paralyze the enemy's chain of command system. This was in contrast to conventional wars that had been "mechanized warfare" won by utilizing materials and energy to cause human and physical destruction to the enemy.[38]

"Informationized warfare" refers to "wars that use informationized weaponry and equipment and related operational methods based on networked information systems, and take place mainly in the form of systems confrontation in land, sea, air, space, cyber, and electromagnetic spaces and the cognitive domain," according to the *Glossary of the Chinese People's Liberation Army*, a dictionary of PLA military terms.[39] Informatized military forces have chain of command systems and weaponry and equipment that are networked in a sophisticated manner via cyberspace to create an integrated system. Therefore, informatized warfare is a battle between the system of one's military and the system of the opponent's military. The PLA calls this type of warfare "systems confrontation." This concept came into widespread usage among PLA strategists from around the mid-2000s following the 1999 Kosovo War, when North Atlantic Treaty Organization (NATO) forces centered around the United States paralyzed the operational system of Yugoslav forces and waged an effective war.[40]

Against the backdrop of this discourse, the 2015 edition of the National Defense White Paper, *China's Military Strategy* (NDWP 2015), states that, "The basic point for preparation for military struggle will be placed on winning informationized local wars," and that China's armed forces "aim at building an informationized military and winning informationized wars." It also expresses the view that, "Long-range, precise, smart, stealthy and unmanned weapons and equipment are becoming increasingly sophisticated. Outer space and cyber space have become new commanding heights in strategic competition among all parties. The form of war is accelerating its evolution to informationization."

From the above, it can be seen that the military strategic guideline of "local wars under the conditions of informationization" was proposed during the era of Hu Jintao, whereas the concept of "informationized warfare" was added when Xi Jinping assumed office, and the type of war aspired

by the PLA gradually shifted from the former to the latter. The former represents local wars, a large portion of which is mechanized warfare in which an attack physically destroys an enemy and depletes its combat capability, with priority given to war intelligence. Conversely, the latter warfare to be executed by the PLA in the future is understood as wars that focus on striking against the enemy's information nodes and making the enemy powerless through cyber attacks. The PLA omitted the term "local," possibly to indicate that informatized warfare will often focus on targets of attack that do not exist in physical space. Or the omission may have been due to the PLA's recognition that confining wars to "local" will be difficult, given that cyber and electromagnetic domains cannot be split into physically measurable units. Even if the targets of attack are limited to the servers or infrastructure control systems of adversary countries and regions, the effects could spill over to third countries and other regions.

As will be examined in more detail in Chapters 2 and 3, a question that deserves attention is how the PLA will operate the space and cyber domains to conduct informatized warfare effectively. Space is a new strategic high ground, and "space dominance" is an important element of seizing the initiative in the battlefield, alongside the dominances of air, sea, and information. In global warfare, 95% of reconnaissance information, 90% of military communications, and 100% of positioning and meteorological information relied on space systems as of 2004.[41] As such, it is deemed that operations integrating space capabilities with those at land, sea, and air will be the main form of operation in future informatized warfare. Close coordination among military services will be vital to the success of military operations in informatized warfare, more than in any war in the past.[42] Future informatized warfare will likely see an enemy on land or at sea attacked from space and pose significant threats to the enemy's maneuvers.[43] As was already mentioned, information acquisition from space and information transmission via communications satellites are some of the key components of C4ISR. By using space as nodes, one can have real-time awareness of the battlefield situation. One can also acquire and transmit various information across all combat spaces and reconfigure battlefields to integrate the land, sea, air, space, cyber, and electromagnetic domains for maximum command and control accuracy, promptness, high efficiency, and mutual cooperation. The PLA seems to aim for the mode of fighting in informatized warfare mentioned above.

An informatized battlefield is a battlefield between networks. Attacking the enemy's military information systems and defending against an enemy's attacks of the same sort through cyberspace are essential means of informatized warfare. Informatized warfare embodies diverse operational means, including: obtaining strategic and tactical information for reconnaissance, information on military facilities, and information on unit organization and formation; destroying an enemy's information organization and information routes or causing information disruption; and creating false information and passwords to intentionally leak false information to cause the enemy to make an erroneous judgment.[44] Going forward, it is believed that the use of cyberspace in warfare will continue to increase in importance and that cyberspace will become a major

battlefield in informatized warfare.

(2) Intelligentized Warfare

Published four years after NDWP 2015, the 2019 edition of the National Defense White Paper, *China's National Defense in the New Era*, takes the informatized warfare discussion further and presents the new concept of intelligentized warfare [*zhinenghua zhanzheng*, 智能化战争]. The discourse in the white paper changed to: "Driven by the new round of technological and industrial revolution, the application of cutting-edge technologies such as artificial intelligence (AI), quantum information, big data, cloud computing and the Internet of Things (IoT) is gathering pace in the military field. International military competition is undergoing historic changes. New and high-tech military technologies based on IT are developing rapidly. There is a prevailing trend to develop long-range precision, intelligent, stealthy or unmanned weaponry and equipment. War is evolving in form towards informationized warfare, and intelligent warfare is on the horizon."

Underlying this change was the remark by President Xi Jinping (CCP General Secretary) to "speed up development of intelligent military" to the 19th CCP National Congress,[45] which further stimulated the discussion in China. Li Minghai, associate professor at the National Defense University, defines intelligentized warfare as "integrated warfare based on IoT systems that uses intelligent weaponry and equipment and their corresponding operational methods in the land, sea, air, space, electromagnetic, cyber, and cognitive domains."[46] AI-equipped weapons systems are capable of actions and combat that are similar to or surpass humans', heralding a stage where decisions on command and strategic guidelines rely on AI-assisted decision-making systems.

Pang Hongliang, associate professor at the College of National Security, PLA National Defense University, predicts that the intelligentization of the military that would largely alter operational methods, theories, systems, and organizations will lead to the replacement of informatized

Table 1.1 Past and Present Leaders, the Science and Technologies Emphasized by the PLA, and Military Strategy

Leader	Science, technologies, and weapons emphasized by the PLA	Military strategy that was adopted (besides active defense which has been adopted throughout)
Mao Zedong	Atomic bomb, hydrogen bomb	People's war (while its content has changed, the term itself has survived in succeeding eras)
Deng Xiaoping	Advanced conventional weapons	Local wars under modern conditions
Jiang Zemin	High tech, high-tech weapons	Local wars under high-tech conditions
Hu Jintao	Information and weapons operated based on information	Local wars under the conditions of informatization
Xi Jinping	Information, intelligence, and weapons operated on their basis	Informatized warfare (shift to intelligentized warfare)

Source: Compiled by the author, based on 建国以来毛泽东军事文稿　中卷 [*Mao Zedong's Military Manuscripts since the Founding of the PRC, Vol. II*] (Beijing: 军事科学出版社 [Military Science Publishing House] and 中央文献出版社 [Central Party Literature Press], 2010).

warfare systems with higher order intelligentized warfare systems.[47] Since the early Hu Jintao era, analysts had already noted the "intelligentization" of informatized warfare, forecasting that informatized weaponry and equipment will gradually play a central role in battlefields and that "intelligentization" will be key to the combat capability of the armed forces.[48] While this over a decade-old prediction was an accurate outlook of the current situation, it was confined to combat and tactical-level impacts. Associate professor Pang, in contrast, contends that the impacts of intelligentization could extend to decision-making on military and national strategies.

What do the Xi Jinping administration and the PLA senior officers envision as the future for the PLA? In his report to the 19th CCP National Congress held in October 2017, General Secretary Xi stated, "[We will] see that, by the year 2020, mechanization is basically achieved, IT application has come a long way, and strategic capabilities have seen a big improvement," reaffirming Beijing's intention presented at the 18th CCP National Congress five years earlier. He also announced a new goal: "We will make it our mission to see that by 2035, the modernization of our national defense and our forces is basically completed; and that by the mid-21st century our people's armed forces have been fully transformed into world-class forces."[49] While the Xi Jinping administration promotes the "Chinese Dream" of "the great rejuvenation of the Chinese nation" as well as the dream of becoming a military power, it has not presented a concrete future vision, neither for "world-class forces" nor the dream of becoming a military power.

It appears all right to assume, however, that the leadership of both the CCP and the military agree that future warfare will shift to informatized warfare and intelligentized warfare. The ideal armed forces for fighting an informatized warfare is a force that builds on informatization and merges land, sea, air, space, cyber, and electromagnetic into an integrated system.[50] Such a force takes the form of joint operations to levels more advanced than what is currently envisioned and will be placed under unified command, eliminating barriers between military services and branches. The targets of attack will be mainly physical targets, and humans will make command and strategic guideline decisions at this stage.

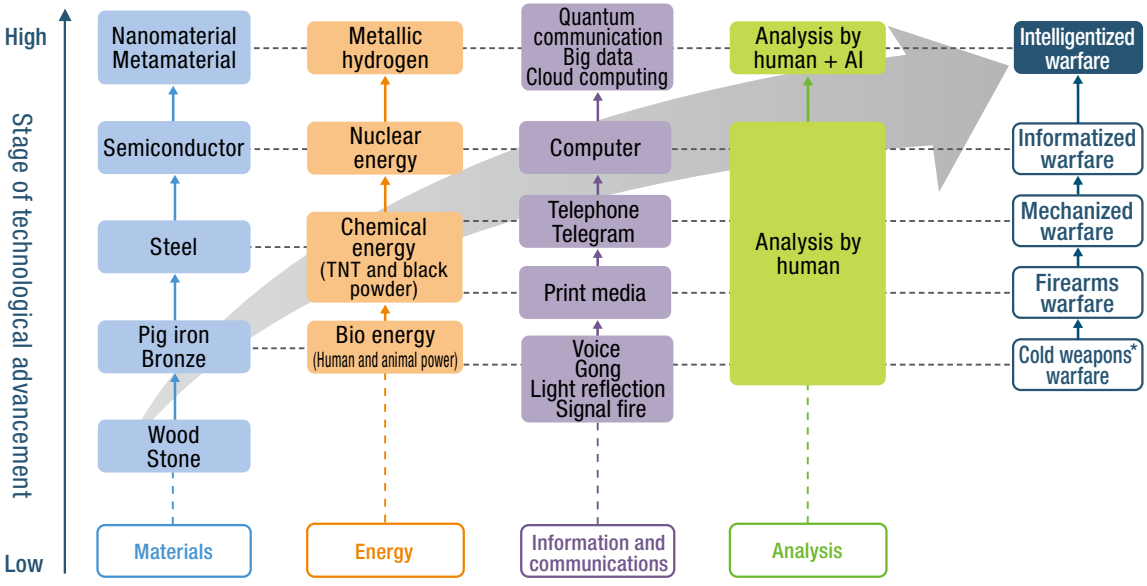
But upon entering the intelligentized warfare phase, equipment with high computing skills will be introduced to make command and strategic guideline decisions. Technologies, such as AI and machine learning, and game theory will be utilized to accurately analyze and determine the opponent's intentions, and this information will be provided to commanders. A command system that essentially integrates humans and machinery will be created. The targets of attack will include nontangible targets in cyber and cognitive spaces. The operational spaces of intelligentized warfare will surpass those of informatized warfare.[51]

Major General Wang Peng, vice chief of staff of the Eastern Theater Command, summarizes the characteristics of intelligentized warfare compared with informatized warfare as follows. Firstly, the focal goal of intelligentized warfare is "intelligence dominance." In informatized warfare, top priority is placed on information dominance to seize the initiative in land, sea, air, space, cyber,

and electromagnetic battlefields; in contrast, in intelligentized warfare, "intelligence dominance" or "mental dominance" is the new contentious domain for seizing the initiative, resulting in competition for superiority in human cognitive speed and cognitive quality. For example, the side with powerful technological capabilities destroys the enemy's cognitive cycle by interfering with and destroying the enemy's sensors and data. Whereas "decapitation operation" is an operation in which special operations forces wage a surprise attack on the enemy's leader in order to damage or paralyze the enemy, "decapitation operation" in intelligentized warfare is a more advanced operation designed to "control the enemy's thought" and achieve maximum cost-effectiveness. A second characteristic of intelligentized warfare is development of autonomous weaponry and equipment. Capabilities similar to human thinking are imparted to weaponry and equipment to autonomously conduct reconnaissance, movement, attack, defense, and more. Such weaponry and equipment autonomously determine the situation based on the target and enemy's circumstances, the battlefield environment, and one's own state, and select the most appropriate action.

Thirdly, intelligentized warfare integrates the operational spaces of land, sea, air, space, cyber, and electromagnetic so that the operational domains can complement each other, which in turn contributes to gaining an advantage on all war fronts. Fourthly, while AI-equipped weaponry are given some authority and thus the battles themselves are unmanned, the battles are not entirely devoid of human involvement. Humans control the battles by: having complete control over the AI-equipped weaponry that are operated; controlling AI weaponry whenever necessary while letting them operate autonomously in principle; and programming AI weaponry to operate freely within

Figure 1.1 Relationship between the Technological Advancement and Evolution of War



Note: War fought mainly with swords and bows and arrows.

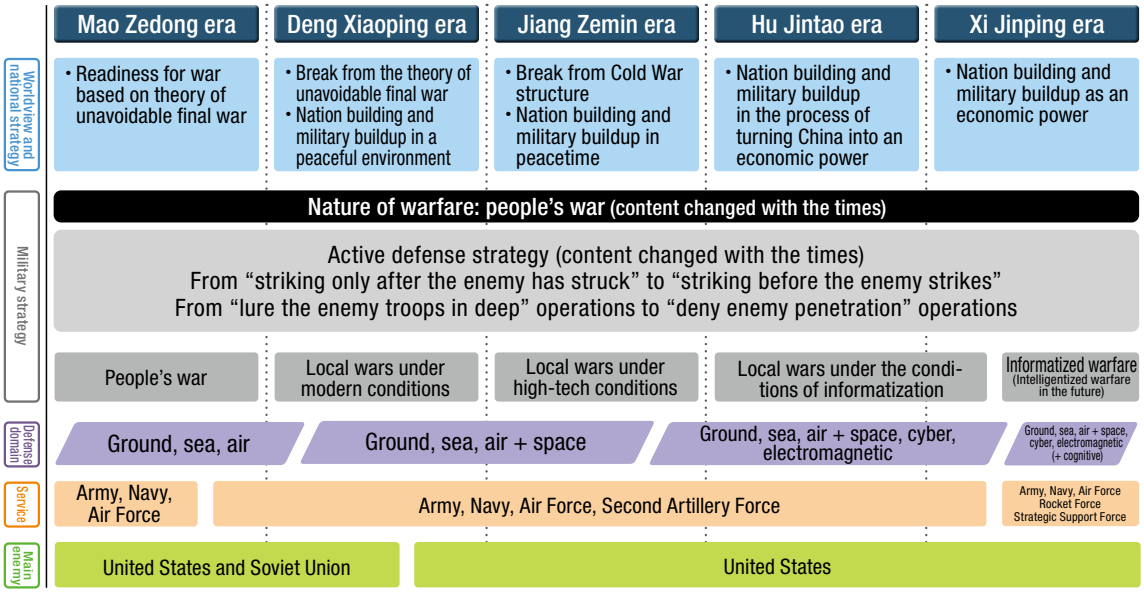
Source: Compiled with additions and alterations by the author, based on 杨益、任辉启 [Yang Yi and Ren Huiqi], 防护工程 [*Defense Engineering*], Vol. 40, No. 6 (2018), p. 66.

the scope of their restricted actions and designated targets. Fifthly, in response to the multidimensionalization of operational spaces as well as offensive and defensive diversification, AI will begin to assist decision-making by commanders. As AI does not get fatigued, does not forget, and has no emotional fluctuation, AI is expected to be able to help commanders make decisions by processing large quantities of data quickly and accurately.[52]

In the process of preparing for informatized warfare, starting with the Hu Jintao administration through the Xi Jinping administration, CMC Chairman Xi Jinping assembled relevant organizations from PLA departments to create the new Strategic Support Force (SSF). Intelligentized warfare emerged out of the PLA's focus on information and use of information, in addition to rapid advances in computers. Albeit this, intelligentized warfare's breadth and depth extend beyond the conventional paradigm, in part because the cognitive domain became a new battlefield as was already mentioned. As discussed in Chapter 2, when informatized warfare moved into full swing, relevant departments from different general departments were reorganized and integrated to create the SSF. If intelligentized warfare increases in importance, the SSF may also be reorganized into a support force for conducting intelligentized warfare efficiently.

Meanwhile, the PLA has been engaged with the development and deployment of conventional types of weaponry and equipment, including aircraft carriers, new fighter models, bombers, airborne early warning and control aircraft, missiles, and vessels. It suggests the PLA continues to recognize the importance of attacking physical targets, even in the post-informatized warfare period, and that no change has been made to its basic principle of warfare, i.e., the strong side wins and the

Figure 1.2 Evolution of China's Military Strategy



Source: Compiled by the author, based on 建国以来毛泽东军事文稿 中卷 [*Mao Zedong's Military Manuscripts since the Founding of the PRC, Vol. II*] (Beijing: 军事科学出版社 [Military Science Publishing House] and 中央文献出版社 [Central Party Literature Press], 2010).

weak side loses.[53] Nevertheless, it is worth paying attention to the PLA's trend toward active use of AI-equipped unmanned weapons amidst its preparations for intelligentized warfare. The shift to unmanned systems has advantages not limited to minimizing loss of human life. For example, the shift enables longer duration activities, a larger radius of action, implementation of attacks involving risks, and the non-requirement of evacuation systems and rescue forces. With regard to unmanned weapons, the U.S. forces already employs unmanned aerial vehicles (UAVs) in actual warfare, the leading examples of which are Global Hawk and Predator. As crew space is unnecessary, UAVs are expected to be easier to design, have better stealth capabilities, have a smaller volume, and a lighter weight. Moreover, as UAVs can be produced at a lower price and in greater quantity than manned aircraft, UAV is a highly cost-effective weapon that can execute saturation attacks against the enemy's high-performance but high-cost targets.[54] Furthermore, turning UAVs into AI will allow for instant parallelization of constantly changing battlefield information as well as selection of the most effective targets of attack and attack methods. China has focused its efforts on UAVs, as was demonstrated at the Zhuhai Airshow held in 2016 where China Electronics Technology Group Corporation (CETC) showcased swarm flying of 67 UAVs. In 2017, CETC conducted a successful test flight of 119 small fixed-wing UAVs, including catapult-assisted takeoff, aerial formation, group dispersion for multiple targets, and reassembly.[55] PLA National University of Defense Technology's College of Intelligence Science and Technology carries out research and tests of UAVs and unmanned vehicles, and is anticipated to aspire to cooperate with entities like CETC to enhance technologies through military-civil fusion.[56]

Column Unrestricted Warfare's High Compatibility with Informatized Warfare and Intelligentized Warfare

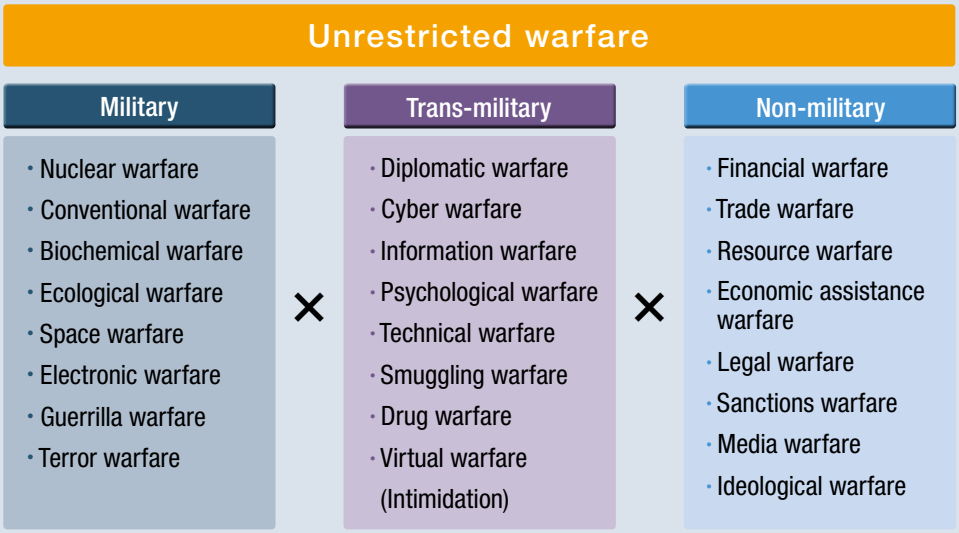
In recent years, analysts have noted that the concepts of security and warfare have expanded noticeably. In China, President Xi Jinping presented the "comprehensive security concept," which places importance on external security, internal security, traditional security, and non-traditional security and is said to cover 11 areas of security, namely, politics, national territory, military, economy, culture, society, science and technology, information, ecology, natural resources, and nuclear.[57] In warfare, the distinction between military and non-military is eroding, and the integrated use of military and non-military means is increasingly becoming the norm. These developments have drawn attention to the concept of unrestricted warfare.

Unrestricted warfare is a term coined by PLA senior colonels Qiao Liang and Wang Xiangsui in 1999 to refer to a new model of warfare and is also the title of their book.[58] As Section 1 discussed, the outbreak of the Gulf War eight years before the publication of *Unrestricted Warfare* had an enormous impact on China. In the Gulf War, bombings and concentration of assets, employing information-based precise enemy searches and high-tech weapons, defeated Iraqi forces relatively quickly. The war was a wakeup call that China, if it was in Iraq's position, was no match for the U.S. forces. As Section 1 stated, China set out the concept of "local wars under high-tech conditions" in order to develop the PLA into an armed force that can be a match for the U.S. forces, and sought to adapt the PLA to new forms of warfare. At the same time, Qiao and Wang, who taught at the PLA National Defense University, conceived that their idea of normal warfare can be replaced with other means of warfare. This notion was borne out by seeing U.S. aircraft carriers sent to waters around the Taiwan Strait and Lee Teng-hui, President of Taiwan, avoid a collapse of the Taiwanese stock market during the Taiwan Strait crisis in 1996. Qiao and Wang proposed ways of fighting that combined military and other fighting methods and collectively called them unrestricted warfare.[59]

Unrestricted warfare refers to ways of fighting advocated by Chinese military personnel and is not considered an official strategic or tactical concept of the PLA. Nevertheless, many similarities with unrestricted warfare-type schemes can be found in China's actual actions, including the "Three Warfares (public opinion, psychological, legal)" and the active use of the naval militia in the South China Sea. Therefore, it can be construed that such actions are based on ideas of unrestricted warfare. In this sense, unrestricted warfare has importance to this day as one of the discourses that have shaped the current trend of China's strategic thought.

According to senior colonels Qiao and Wang, struggles of unrestricted warfare can be divided broadly into military means, trans-military means, and non-military means. Their

Figure 1.3 Unrestricted Warfare



Source: Compiled by the author, based on 乔良、王湘穗 [Qiao Liang and Wang Xiangsui], 超限战 [*Unrestricted Warfare*] (Beijing: 解放军文艺出版社 [PLA Literature and Arts Publishing House], 1999), pp. 156-157.

primary examples are shown in Figure 1.3. Military means are ways of fighting contingencies. The means combined make up military actions. Under the conceptual categories of unrestricted warfare, "decapitation operation" corresponds to terror warfare.

Trans-military means include diplomatic warfare, such as deteriorating an adversary country's diplomatic relations with foreign countries, isolating an adversary country in international organizations, or lodging protests against third countries that take favorable actions toward an adversary country. Another means is cyber warfare, such as stealing information from companies and state agencies via the internet and attacking, destroying, and hijacking websites and servers. Trans-military means also encompass information warfare that spreads numerous fake news stories to interfere with the activities and elections of an adversary country. Psychological warfare effects can be expected from fake news, in that it is designed to lower an adversary country's motivation to resist. Virtual warfare corresponds to enhancement and modernization of equipment and weaponry, strengthening of joint operational capabilities, and display of assets through trainings and exercises.

Non-military means include trade warfare, such as controlling trade to inflict economic damage on an adversary country and make the negotiations favorable to oneself. To conduct trade warfare successfully, there must be a significant economic power disparity between the two sides and one must have functions not easily substitutable by other countries. Related to trade warfare, resource warfare can also be considered non-military means, such as

embargoes on scarce resources and export restrictions on crude oil. Along the same lines is sanctions warfare, which imposes export and import restrictions on strategic supplies. In the economic realm, economic assistance warfare provides assistance to third countries that have friendly relations with an adversary country, with the aim of winning over politicians of third countries or influencing public opinion in third countries favorably to oneself. The provision of material and human assistance to countries struggling with pandemics falls into this category. Legal warfare, such as enacting domestic legislation that legalizes use of non-peaceful means against an adversary country or laws that regulate territorial land and waters, assures the legality of one's actions domestically. Internationally, legal warfare is designed for making claims to foreign ministries and serves as official media advertising. Media warfare includes developing and giving preferential treatment to an adversary country's media that are friendly toward oneself, as well as conducting advertising to strengthen one's position in the international community. Non-military means also cover ideological warfare that implements and advertises policies that give preferential treatment to people and companies in adversary countries, gives preferential treatment to contesting candidates in adversary countries, and advertises one's outstanding or highly moral aspects of political and social systems.

Many of these means cut across multiple domains. An important characteristic of the unrestricted warfare concept is that the choices for means of warfare are close to infinite. There is no reason one has to limit their choice and use of warfare means to armed force and military instruments. Unrestricted warfare enables war goals to be achieved without killing and bloodshed without relying on armed force and the military.[60]

From the late 2000s, alongside modernizing military capabilities, China began to integrate non-military means to adopt a hardline posture to disputes with neighboring countries. The notion of unrestricted warfare, or combining different modes of fighting, offers flexibility and diversity. Unrestricted warfare is fully applicable even amidst the vastly expanding defensive domains of informatized and intelligentized warfares. Though not discussed in this chapter, the methods of the Three Warfares are suitable for informatized warfare and are methods of fighting that are already part of unrestricted warfare. Accordingly, it is expected that China will continue to actively apply unrestricted warfare and the Three Warfares to foreign countries.

With the global outbreak of the coronavirus disease (COVID-19), China engaged in economic assistance warfare, notably mask diplomacy. At the same time, China conducted diplomatic warfare, holding negotiations with foreign governments and having them express appreciation to China. These efforts were advertised domestically through the media and were leveraged to give authority to the Xi Jinping administration. Furthermore, China passed

the National Security Law for Hong Kong in late June 2020 when other countries were occupied with tackling COVID-19 domestically. China's Coast Guard vessels continued to conduct activities in waters surrounding the Senkaku Islands. Further, the fleet of China's aircraft carrier *Liaoning* carried out drills in the Pacific, almost as if to coincide with the forced docking of the U.S. aircraft carrier *USS Theodore Roosevelt* in Guam due to a surge in COVID-19 cases on the carrier. Through the foregoing acts, China has demonstrated that it has not succumbed to the rage of COVID-19. This has elements of both information and psychological warfares.

This page is intentionally left blank

Chapter 2

China's Cyber Strategy

Yatsuzuka Masaaki

1. China's Quest to Improve Cyber Capabilities

(1) The PLA's Pursuit of "Informatization"

Intending to become a "cyber power," the Xi Jinping administration is taking active steps to diffuse information technology across Chinese society. The People's Liberation Army (PLA) is informatizing itself in this context, recognizing the important role cyberspace plays in "informatized warfare." China's cyber strategy has evolved in the course of the PLA's informatization. Informatization refers to incorporating information communications technology (ICT) into the military, connecting military services and units via information networks, enhancing information collection and information transmission capabilities, and improving the military's capabilities through systematization.

The impetus driving the informatization of the PLA is closely related to its recognition of the form of warfare. While some PLA strategists and others noted the shift in the form of warfare toward "informatized warfare" from around the late 1980s, it was not until some years after the end of the Cold War that this perception became widespread, including among the PLA leadership.[1] The PLA leadership was stunned by the 1991 Gulf War, in which reconnaissance satellites and other information communications of the U.S. forces supported ground, sea, and air combat. Studying this war, the PLA leadership recognized that "local wars under high-tech conditions" were the modern form of conflict, and that the PLA needed to mechanize itself mainly through introducing high technology.[2]

Subsequently, the U.S. forces improved its ability to conduct operations utilizing ICT, as demonstrated in wars such as the Kosovo War. In reaction to this, the discourse of the PLA leadership from 1998 through 2000 reflected a change in recognition to: "the essence of high-tech warfare is informatization"; and "informatized warfare" will become the basic form of warfare in the future.[3] At an expanded meeting of the Central Military Commission (CMC) in December 2002, CMC Chairman Jiang Zemin stated that "informatization is at the heart of the new military transformation" and summarized that "the form of modern warfare is shifting from mechanized warfare to informationized warfare." "Building an informationized force and winning the informationized warfare" became a goal of military transformation shared among the PLA.[4] Thus, a CMC meeting in June 2004 adopted a military strategic guideline that stipulated an operational doctrine, force structure, and training for "winning local wars under the conditions of informationization."[5]

Based on this military strategic guideline, trainings tailored to informatized warfare were carried out under the Hu Jintao administration, along with more in-depth studies of military theory.[6] At the PLA-wide military training conference in June 2006, CMC Chairman Hu Jintao indicated his intention to prioritize "systems confrontation," saying, "local wars under the conditions of informationization are confrontations between systems and systems, and their fundamental operational mode is joint operations."[7]

Systems confrontation in informatized warfare considers that achieving "information

dominance" is a core initiative of warfare that impacts all domains and all operational activities and influences the outcome of the war. Major General Qi Shiquan, former Director of the PLA Electronic Engineering Institute, contends that "information dominance" consists of electromagnetic dominance, cyber dominance, and psychological dominance, and that modern warfare from start to finish is a battle to attain "information dominance."[8] Social media and other use of cyberspace shaped public opinion in the "color revolutions" in Eastern Europe in the 2000s, the Arab Spring in the Middle East, and Russia's "annexation" of Crimea in 2014. Drawing on such observations and on electromagnetic/cyber attacks and psychological warfare conducted during a conflict, PLA researchers and others discuss the importance of achieving a wide range of information dominance from peacetime to wartime.[9] Dean Cheng, Senior Research Fellow at The Heritage Foundation, notes that "information dominance" aims to gather, transmit, analyze, assess, and exploit information more quickly and more accurately than one's adversary, and on this basis, shape and influence friendly, adversary, and third-party views and assessments.[10] One of the objectives of the military reforms pursued under the current Xi Jinping administration is improving the PLA's capability to achieve information dominance.

(2) The Missions and Structure of the Strategic Support Force

An entity that is thought to play an important role in achieving information dominance is the Strategic Support Force (SSF) newly established in late 2015 as part of the military reforms.[11] Shortly before the SSF was created, General Gao Jin, who was appointed its first commander, wrote about the transformation of the form of warfare and achieving information dominance in a *PLA Daily* editorial: The form of warfare is in a period of qualitative change from mechanization to informatization. "Under conditions of nuclear deterrence, integrated joint operations (across the) land, sea, air, space, network, electromagnetic (domains) are gradually becoming a reality. The battlefield is expanding from traditional spaces to extremely high, extremely deep, far-reaching physical spaces and virtual spaces and transforming into asymmetric, contactless, and non-linear patterns of operations. Information dominance has become the core of seizing comprehensive control of the battlefield. The mechanism of winning in warfare has changed profoundly."[12]

The problem awareness elaborated here is closely linked to the missions of the SSF. Soon after the force was established, the spokesperson of the Ministry of National Defense of China described the SSF as "a new-type combat force to safeguard national security."[13] Furthermore, China's National Defense White Paper 2019 (hereinafter referred to as "NDWP 2019") states: the SSF is "an important driver for the growth of new combat capabilities"; and "In line with the strategic requirements of integrating existing systems and aligning civil and military endeavors, the PLASSF is seeking to achieve big development strides in key areas and accelerate the integrated development of new-type combat forces."

This information suggests that the basic mission of the SSF is to win informatized warfare

by: (1) providing strategic information support for joint operations, including in the new operational domains of space, cyber, and electromagnetic; (2) achieving information dominance; and (3) endeavoring to convert advanced technologies into military capabilities. Joe McReynolds, research fellow at the Jamestown Foundation, and John Costello at the U.S. Department of Homeland Security identify the following concrete missions of strategic information support: (1) centralizing technical intelligence collection and management; (2) providing strategic intelligence support to theater commands; (3) enabling PLA power projection; (4) supporting strategic defense in the space and nuclear domains; and (5) enabling joint operations.[14] The addition of new missions in NDWP 2019, such as new technology testing, also hints that the missions of the SSF may continue to expand and that it will play a core role in future warfare including intelligentized warfare [*zhinenghua zhanzheng*, 智能化战争].

The SSF is characterized as a "force [*budui*, 部队]" and not a "service [*jun*, 军]." It is under the direct command of the CMC and does not appear to have the status and size of the army, navy, air, and rocket services.[15] Given that the Second Artillery Force [*di'er paobing*, 第二炮兵] was promoted to Rocket Force [*huojianjun*, 火箭军] as a full military service in late 2015, the SSF seems to correspond to an independent military branch, similar to the Second Artillery Force prior to the military reforms.[16]

The SSF was not created from scratch. The functions, personnel, and facilities of the former four general departments (General Staff Department [GSD], General Political Department [GPD], General Logistics Department [GLD], and General Armament Department [GAD]) that existed before the military reforms were transferred to the SSF. It also integrated organizations that had been differentiated by form of operation, such as reconnaissance, attack, and defense.[17] For example,

Table 2.1 Members of the SSF (as of March 2020)

Department	Position	Name	Rank	Notes
–	Commander	李凤彪 [Li Fengbiao]	General	From the paratroops. Member of the 19th CCP Central Committee.
–	Political Commissar	郑卫平 [Zheng Weiping]	General	Member of the 19th CCP Central Committee
–	Deputy Commander	郝卫中 [Hao Weizhong]	Lieutenant General	Has worked at the Taiyuan Satellite Launch Center. Previous Deputy Commander of the Space Systems Department.
Staff Department	Chief of Staff	Unknown	Unknown	饶开勋 [Rao Kaixun] was dismissed in October 2019 for disciplinary violations
Political Work Department	Director	冯建华 [Feng Jianhua]	Lieutenant General	
Discipline Inspection Commission	Director	杨笑祥 [Yang Xiaoxiang]	Lieutenant General	Concurrently serves as Deputy Political Commissar of the SSF
Network Systems Department	Commander	巨乾生 [Ju Qiansheng]	Lieutenant General	Concurrently serves as Deputy Commander of the SSF
	Political Commissar	丁兴农 [Ding Xingnong]	Lieutenant General	
Space Systems Department	Commander	尚宏 [Shang Hong]	Lieutenant General	Has worked at the Jiuquan Satellite Launch Center. Concurrently serves as Deputy Commander of the SSF.
	Political Commissar	康春元 [Kang Chunyuan]	Lieutenant General	

Source: Compiled by the author, based on CCTV, last modified December 12, 2019, http://news.cctv.com/2019/12/12/ARTIgEMinG3D1M386i0D8f4O191212.shtml.

before the military reforms, the GSD Third Department was in charge of intelligence and technical reconnaissance in the cyber domain, the GSD Fourth Department, attack operations such as electronic warfare, and the GSD Fifth Department, information system defense.[18] In contrast to this setup, the SSF assumed the operational duties of these GSD departments, as well as some of the bases and functions of the GAD and GPD, with a view to effectively carrying out integrated reconnaissance, attack, and defense.

The PLA has disclosed little information on SSF personnel and composition. However, based on media reports and previous studies, the SSF leadership can be envisaged as shown in Table 2.1 and the main organizations as shown in Table 2.2. With regard to departments, the SSF is comprised of: the Staff Department, which provides supports for joint operations such as logistics support and training; the Political Work Department, which is believed to be in charge of party governance, political guidance, and the Three Warfares; and the Discipline Inspection Commission, which cracks down on intra-organization corruption. As for operational command departments, it appears that the Network Systems Department (NSD) is in charge of cyber and electronic warfares and the Space Systems Department (SSD) provides supports for space operations (satellite launch, tracking, control, space information support). According to some views, the SSF also has the Equipment Department and the Logistics Department.[19]

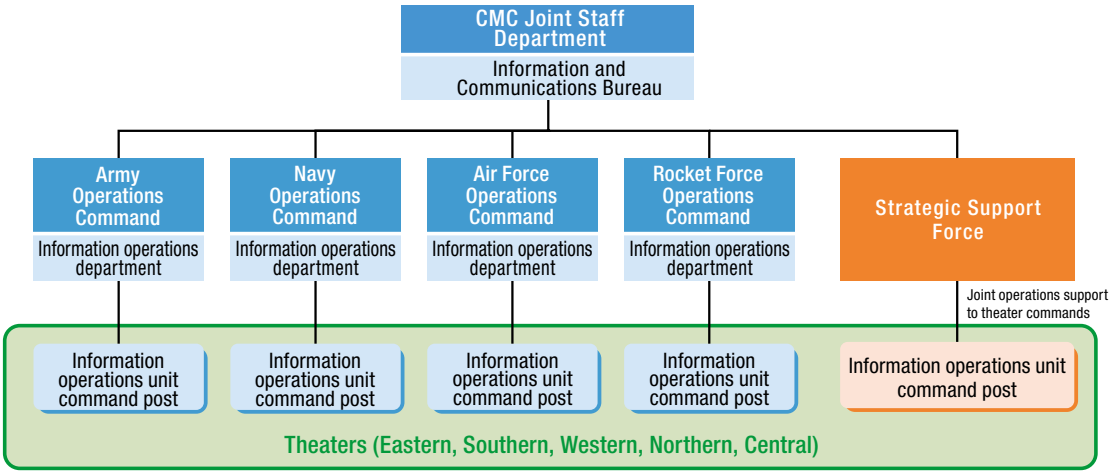
As an outcome of the military reforms of the Xi Jinping administration, the CMC conducts overall management, the five theaters (East, West, South, North, Central) are primarily responsible for military operations as force users, while the services, such as the Army, Navy, Air Force, Rocket Force, SSF, and the Joint Logistic Support Force, are primarily responsible for building forces as force providers [*junwei guanzong*, 军委管总; *zhanqu zhuzhan*, 战区主战; *junzhong zhujian*, 军种主建]. If this decision is abided, the SSF will engage in deploying personnel for space, cyber, and electromagnetic domain operations, procure equipment, and improve military capabilities through training, and will fulfill its role as a force provider that supplies combat capabilities to theaters during operations.

Table 2.2 Key Departments and Roles of the SSF

Key Departments	Roles
Staff Department	Works with the Central Military Commission's Joint Staff Department on supports for joint operations, including logistics support planning and training
Political Work Department	Three Warfares (public opinion, psychological, legal), compliance with party guidance, and organizational management
Discipline Inspection Commission	Combatting corruption inside the organization
Network Systems Department	Reconnaissance, defense, and offense in the cyber and electromagnetic domains; technical reconnaissance
Space Systems Department	Administration of satellite launch centers; satellite launches, tracking, and control; space information support

Source: Compiled by the author, based on John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era* (Washington D.C.: National Defense University Press, 2018), pp. 1-68.

Figure 2.1 Command Organization during Information Operations



Source: Compiled by the author, based on 叶征 [Ye Zheng], 信息作战学教程 [*Lectures on the Science of Information Operations*] (Beijing: 军事科学出版社 [Military Science Publishing House], 2013), p. 134.

Meanwhile, *Lectures on the Science of Information Operations* edited by Ye Zheng, former Director of the Informationized Operations Theory Research Office of the Academy of Military Science, differentiates three levels of information operations command as shown in Figure 2.1. They are: (1) the information operations department of the Joint Operations Command Center; (2) information operations departments of services and branches; and (3) the information operations force command post.[20] If this concept reflects the command composition of the PLA's information operations, the SSF will likely support joint operations under the command of the CMC's Joint Staff Department (JSD) (Information and Communications Bureau) during operations and provide combat capabilities for information operations to the service forces of the theaters engaged in the operations. Analysts note that the SSF will be responsible for strategic national-level operations, whereas services and theaters will be responsible for operational- and tactical-level operations.[21]

At least the following three points can be noted regarding cyber warfare involving the SSF. First, as is evident from the SSF composition, the cyber and electromagnetic domains are closely linked, and it is expected that operations will be conducted by merging the two together. Within the PLA, members including Major General Dai Qingmin, former Director of the GSD Fourth Department, had already advocated concepts such as integrated network and electronic warfare (INEW), which combines cyber and electromagnetic attacks, and integrating soft-kill and hard-kill measures, which combines cyber attacks and conventional firepower. The notion gained traction that cyber warfare can be made more effective by simultaneously conducting kinetic strikes that cause physical damages.[22] The abovementioned *Lectures on the Science of Information Operations* expresses that electronic and cyber warfares can be adapted to information operation missions in battlefields under an integrated command. These opinions are thought to be reflected in making the SSF's NSD responsible for both cyber and electronic warfares.[23]

Cyber warfare is often deemed to be part of information operations. In the PLA's glossary of military terms, information operations are defined as: "integrating modes such as electronic warfare, cyber warfare, and psychological warfare to strike or counter an enemy to interfere with and damage the enemy's information and information systems in cyberspace and electromagnetic space; to influence and weaken the enemy's information acquisition, transmission, processing, utilization, and decision-making capabilities; and to ensure the stable operation of one's own information systems, information security, and correct decision making."[24] "Information warfare" has a broader definition than "information operations" and seemingly refers to a struggle for initiative between two hostile parties involving the use of information technology in the political, economic, science and technology, diplomatic, cultural, military, and other domains.[25]

Secondly, it can be supposed that, in the PLA, the SSF is responsible for the Three Warfares that utilize cyberspace. Jeffrey Engstrom, political scientist at the RAND Corporation, notes that the SSF's Political Work Department manages the Three Warfares and that information operations units are responsible for psychological warfare during wartime.[26] This view is consistent with analysts' observation that the SSF inherited the 311 Base [*311 jidi*, 311基地], known as "Three Warfares Base," from the former GPD.[27] As regards information warfare in peacetime, there are entities including the party's media organizations under the Publicity Department of the Central Committee of the Chinese Communist Party (CCP) and the Ministry of Public Security of the State Council, and it is expected that the Ministry of State Security of the State Council will be chiefly responsible for information warfare through cyberspace in peacetime. It remains a question whether the Three Warfares conducted by the SSF are distinguished from the operations of these organizations or whether they engage in the operations with some overlaps.

Thirdly, the SSF oversees educational institutions, including Information Engineering University and Space Engineering University, as well as research institutes, and appears to have the role of training specialists in the cyber and space domains.[28] With respect to training personnel for cyber warfare, the SSF not only has jurisdiction over Information Engineering University but also has signed framework agreements for strategic cooperation with six universities—University of Science and Technology of China, Shanghai Jiaotong University, Xi'an Jiaotong University, Beijing Institute of Technology, Nanjing University, and Harbin Institute of Technology—and three military enterprises—China Aerospace Science and Technology Corporation (CASC), China Aerospace Science and Industry Corporation (CASIC), and China Electronic Technology Group Corporation (CETC).[29] The SSF is believed to be working with an array of organizations to develop talent who will be responsible for cyber warfare, including academic exchanges with these educational and research institutions, interactions among experts, implementation of specialized educational programs, supplying outstanding talent, and cooperating on educational technology research.

2. The PLA's Recognition of Cyber Warfare

(1) Cyber Operations in Informatized Warfare

Leading examples of state-initiated cyber attacks include those against military facilities, those that halt the functioning of critical infrastructure, those targeting intellectual property of foreign private companies to attain business superiority or promote indigenous industries, and cyber attacks or infiltration and espionage against people's decision-making and democratic systems.[30] In recent years, all of these cyber incidents involving China's military, intelligence agencies, public security authorities, or agents have been increasingly reported. For example, a 2019 report published by the cybersecurity company FireEye detailed about APT41 as one of the Advanced Persistent Threat (APT) groups. APT is a code that the company uses to differentiate groups that conduct cyber attacks. The report notes that APT41 is a Chinese state-sponsored group that carries out such attacks not only for financial motives but also in line with the Chinese government's policy priorities.[31]

In discussing cyber attacks, caution must be paid to the difficultness of identifying source of attack, i.e., the issue of "attribution." Moreover, cyber operational capabilities are never made visible, such as in the form of equipment and weapons, and are kept highly confidential. Accordingly, assessing the situation of China's cyber attacks and cyber operational capabilities entails technical difficulty and uncertainty. In view of these issues, this section attempts to examine the PLA's recognition of cyber warfare by relying on the writings and previous studies of PLA members, and thereby, understand the characteristics of PLA cyber warfare.

As the previous section stated, the PLA is promoting informatization with the goal of "winning local wars under the conditions of informationization." This section first reviews where the PLA places cyber warfare in the context of informatized warfare. According to the 2015 edition of *Science of Military Strategy* (SMS) edited by the National Defense University, military actions in the cyber warfare domain can be classified into four operations: (1) cyber deterrence; (2) reconnaissance and

Table 2.3 Types of Cyber Operations

Cyber Operations	Overview
Cyber deterrence	Dissuading an opponent from conducting a cyber attack by demonstrating one's ability to carry out cyber attacks that could cause catastrophic damages to the enemy's political, military, and economic systems, including C4ISR and transportation/information infrastructure
Cyber reconnaissance and anti-reconnaissance	Stealing military information using malware such as a virus or Trojan horse
Cyber attack	Destroying the enemy's command order system, communications network, or computer system for weapons and equipment using means such as destruction of data by a virus, hacking, and communications interference
Cyber defense	Defense operations to protect against the enemy's reconnaissance, interference, secret theft, and/or destruction

Source: Compiled by the author, based on 肖天亮 [Xiao Tianliang], ed., 战略学 [*Science of Military Strategy*] (Beijing: 国防大学出版社 [NDU Press], 2015), pp. 147-149.

anti-reconnaissance via cyberspace; (3) cyber attack; and (4) cyber defense.[32]

First, as this definition implies, the PLA's information operations that include cyber warfare could be conducted not only in wartime but also in peacetime. As the lines between war and peace are blurred in cyberspace, confrontational acts are taken irrespective of peacetime or wartime.[33] In informatized warfare guidance theory, priority is placed on seizing the initiative in war. To this end, operations in the cyber domain at the war preparation stage, i.e, peacetime, require influencing public opinion in China and abroad by gaining the right to speak via the internet, media, and other mediums, along with weakening the enemy's war command system through military intimidation in the cyber domain.[34] For example, this appears to include cyberspace reconnaissance for gauging the enemy's network vulnerabilities from peacetime, as well as sending false data to the adversary's network to confuse its perceptions.[35]

Secondly, cyber operations may be carried out in a first strike of informatized warfare.[36] In informatized warfare, the basic operational mode is joint operations between military information systems that network the Army, Navy, Air Force, and other services (systems confrontation). In these cases, operations in cyberspace provide vital means of attacking the opponent's command, control, communications, computers, intelligence, surveillance, reconnaissance (C4ISR). In particular, while the PLA sets forth "active defense" as its strategic thought, emphasis is put on preempting the enemy in informatized warfare. From this perspective, offensive cyber warfare has immense value for gaining information dominance.[37] In other words, cyber attacks impede the opponent's chain of command, cause the opponent to lose control of her operational capabilities and operational actions, deprive weapons and equipment of their capabilities and effectiveness, and enable one to seize the initiative in military confrontations. As a result, one can achieve the goals of military actions effectively and meet the conditions for achieving final victory in a war.[38]

Thirdly, informatized warfare emphasizes strict control of the goals of war and prioritizes cyber warfare from the standpoint of controlling escalation.[39] The cost of waging modern warfare is rising; once a war starts, it will likely impede economic growth significantly. Some limits will therefore be set on the goals of war, aimed at preventing the war front from expanding, avoiding the prolongation of war, and keeping the war from turning into an international conflict. The 2011 edition of SMS edited by the National Defense University notes that modern local wars are characterized by "low (medium) strength, high technology" and that many high technologies will be used in local wars.[40] Cyber attacks, depending on their scale, can cause considerable destruction comparable to nuclear weapons. The PLA thus recognizes that, by attaining superiority through cyber warfare and seizing the initiative in war, it can achieve goals without fighting or only with a small conflict.[41]

(2) Aspects of the PLA's Cyber Warfare

As seen above, cyber warfare is intricately linked to controlling the escalation of war. As these issues of war escalation in relation to cyber warfare are concerned, there are at least three points at issue.

The first point is the notion of cyber deterrence frequently referred to by the PLA. In an April 2016 address, President (CCP General Secretary) Xi Jinping stated, "We will strengthen our cybersecurity capability and deterrence [*weishe*, 威慑] capability. The essence of cybersecurity lies in confrontation, and the essence of confrontation lies in the contest between offensive and defensive capabilities." China's deterrence/*weishe* capability is similar to but is a broader concept than deterrence capability in English. Dean Cheng notes that the concept of the Chinese term deterrence/*weishe* embodies both the English terms deterrence (keep an enemy from doing something) and compellence (make an enemy do something).[42] President Zhang Shibo of the PLA's National Defense University puts cyber deterrence within the active defense paradigm, noting: "Simple passive defense gives a chance to cyber attackers; we must therefore maintain active defense in cyberspace and integrate deterrence and defense [*shefang yiti*, 慑防一体] to achieve cyber dominance." President Zhang classifies concrete means of cyber deterrence into: (1) demonstration of cyber attack technology testing; (2) partial disclosure of cyber weapons and equipment through the media; (3) operational exercises in cyberspace; and (4) disclosure of cyber attacks that were conducted.[43] Such stepwise signaling of cyber deterrence will aim to discourage the enemy's cyber attacks as well as control the escalation of war and advance the war in one's favor. Examples of this can already be seen. At China's 70th anniversary military parade in October 2019, information communications and electronic warfare equipment were displayed. Various media organizations have also reported on the status of the technology development and exercises related to cyber weapons. However, there are risks associated with disclosing cyber attacks which are made valuable by their confidentiality, and by extension, there is a question as to how effectively signaling can be conducted. In this regard, there is room for debate on the PLA's concrete methods of cyber deterrence and their effectiveness.

Secondly, China may have its own ideas regarding the criteria and threshold of military attacks in cyberspace. The 2013 edition of SMS states that cyber warfare is low cost, highly efficient, and low risk, making them more prone to occurring than other types of war. In this light, the psychological hurdle of waging cyber warfare may be lower compared to combat involving conventional weapons.[44] For instance, regarding "soft-kill" methods like cyber attacks that do not inflict physical damage to the enemy force's command information system known as C4ISR, analysts have noted that the PLA may treat such methods as defensive countermeasures that do not escalate a war.[45] Meanwhile, from a domestic governance standpoint, the

CCP is especially wary of information circulating on social media and other platforms that is critical of or disadvantageous to the administration, and the PLA sees public opinion manipulation via cyberspace as an important component of information warfare. Hence, the Government of China and the PLA may consider information circulation on social media as cyber attack, depending on the target, scale, and circumstances.[46] "Soft-kill" methods are wide-ranging, including data theft, destruction, and control, and what is considered cyber attack remains a subject of international debate.

The third point pertains to whether or not the PLA conducts cyber attacks against the private sector of other countries. As a guidance theory for informatized warfare, the 2013 edition of SMS notes that what is important in executing a war is not depriving the survivability of the enemy but depriving its military capabilities or compelling the enemy's compromise through such deprivation. In such cases, the main targets of attack are not the enemy's civilians but its military/political central agencies and military command system, or high-tech weapon bases and critical replenishment facilities.[47] These contentions suggest that informatized warfare of the PLA places focus on counter force rather than counter value. On the other hand, as was noted, cyber deterrence includes showcasing cyber attack capabilities against vital transportation and communications infrastructure. In this respect, it cannot be denied that, in peacetime, the PLA (or its agent) conducts low-intensity cyber attacks on a day-to-day basis against the private sector of other countries, notably critical infrastructure companies and the defense industry, including cyber reconnaissance for technology reconnaissance and vulnerability assessment. The U.S. Department of Justice's indictment of five PLA officers in 2014 was a clear demonstration of U.S. government protest against the PLA's cyber attacks on private companies.

The issue is how realistic an option is high-intensity, large-scale cyber attacks on the private sector for the PLA. There is discussion among Chinese national defense experts that, if strategic destruction is inflicted on electronic systems of a specific region, its military operations and tactical activities can be severely impacted. Based on such discussions, some note that the PLA may target critical infrastructure such as electronic systems in addition to military targets.[48] Furthermore, it is noted that, if China's territory is attacked by an enemy, China may conduct a cyber attack on the information system of the opponent's private sector.[49]

(3) The Challenges and Future Direction of China's Cyber Capabilities

In reviewing the outlook for the PLA that aspires to improve cyber warfare capabilities, attention is given to at least the following three challenges and their countermeasures. The first challenge is related to cyber warfare talent. While China produces 15,000 cyber specialists every year, it does not meet the demand for 700,000–1.4 million professionals, creating severe workforce shortages.[50] In addition to personnel shortages, the PLA faces problems including an education-demand gap, unbalanced assignment of personnel, and outflow of talent to the private sector. These problems are said to be especially prominent in the nascent SSF.[51] The Office of the CCP Central Cyberspace

Affairs Commission has already announced that, for ten years starting from 2017, it will designate seven institutions including the SSF's Information Engineering University as cybersecurity model institutions and put efforts into talent training.[52] In response to the government's intention, the private-sector information security firm 360 Enterprise Security Group has established educational and research institutes pertaining to cybersecurity in rapid succession in recent years. Nevertheless, it will likely not be easy to resolve problems such as talent outflow from the military.

The second challenge is related to the development of an "assassin's mace [*sha shou jian*, 杀手锏]" in cyberspace. In short, assassin's mace here refers to a strategic weapon to overcome one's inferiority to the opponent's superior overall assets. The development of an assassin's mace is mentioned also in reference to missile assets and military use of space; however, in regard to cyber warfare in particular, there is recognition within the PLA that an assassin's mace has the potential of enabling China to overcome its inferiority in conventional assets. From this perspective, China, which has inferior military capabilities vis-à-vis the United States, conceives that an assassin's mace for cyber warfare must be developed. According to a biography of Zhang Wannian, former Vice-Chairman of the CMC, in the course of seeing the U.S. and U.K. forces conduct Operation Desert Fox against Iraq in 1998 and the North Atlantic Treaty Organization (NATO) forces utilize high-tech weapons in the Kosovo War in 1999, the PLA leadership shared the recognition that there was an urgent need to develop an assassin's mace for resisting military powers.[53] As this background shows, it appears that the assassin's mace program is closely related to China's deterrence strategy for the United States.[54]

At the symposium on cybersecurity and informatization in April 2016, President Xi Jinping spoke about developing an assassin's mace as a core technology that China should acquire in the cyber field, suggesting that assassin's mace weapons are being developed under the leadership of the current administration.[55] Major General Dai Qingmin, former Director of the GSD Fourth Department, notes that an assassin's mace has strategic, offensive, directional, effective, and menacing elements, albeit their concrete means have not come to light.[56] Given that the PLA is strengthening military capabilities to win intelligentized warfare, which it considers the future form of warfare, an assassin's mace for cyber warfare could be developed by taking into account new technology trends, including artificial intelligence (AI). For example, the China Defense Science and Technology Information Center directly under the CMC Science and Technology Commission notes that further maturation of AI technology may confer breakthrough capabilities to both the offensive and defensive aspects of future cyberspace and bring fundamental changes to cyberspace itself.[57] According to the Central Cyberspace Affairs Commission website, the 360 Enterprise Security Group identifies automatic hole mining technology as an assassin's mace technology for making the first move in cyber offensive and defensive operations.[58] At the same time, Simone Dossi, assistant professor at the University of Milan, who has analyzed the PLA's discourse notes that two requirements must be cleared to develop an assassin's mace: (1) innovation in core technologies such as Operating System (OS); and (2) overall technological sophistication.[59] With core technologies in the

cyber domain remaining immature in China, it seems the PLA has not overcome the challenges of developing an assassin's mace in cyber warfare.

The third challenge is measures for indigenization of core cyber technologies. Having relied on foreign companies for cyber technologies, there is concern about the vulnerability of cybersecurity in China. Notably, as a result of installing foreign-made information devices at the PLA and local government bodies since the 1990s, China gradually became a "cyber colony," which is said to have significantly undermined cybersecurity and led to foreign companies taking the lead in core informatization technologies.[60] Within the PLA, while some advocated for introducing foreign forces' advanced technologies in the informatization process to accelerate informatization of weapons and equipment, others noted that lack of independent innovation capabilities will undermine the PLA's cybersecurity.[61]

Globally, U.S. products currently make up a majority of the facilities and cyber-related software products that are key to internet and information industry supply chains. Furthermore, core technologies are considered to be in the hands of the United States.[62] For example, with regard to core technologies in the disaster tolerance backup industry, China relies on foreign capital including IBM, Hewlett-Packard, and Symantec for over 98% of disaster tolerance backup and recovery systems even as of 2018, according to a report on China's cybersecurity published by the China Center for Information Industry Development.[63]

The lack of indigenization of core technologies in the cyber field is directly linked to the aforementioned challenges of developing an assassin's mace, in addition to China's security vulnerabilities. PLA experts and others fear that U.S. information technology products are installed with special software that gives an advantage to U.S. economic, political, security, and other interests. They are wary about China's domestic critical information infrastructure being placed under U.S. control, especially electricity, financial, telecommunications, and energy networks, exposing China to severe security risks.[64] The 2013 edition of SMS notes that core cyber technologies and authority over the internet are in the hands of other countries, making China inferior in cyber counterattacks.[65] Amidst the PLA's increasing reliance on information technologies owing to informatization, reliance on the United States for core technologies represents a major vulnerability for China. Such concerns over technology dependence are likely behind China's aspiration to increase the indigenization ratio of priority industries, as stated in the Made in China 2025 [*zhongguo zhizao 2025*, 中国制造2025] document which the Government of China released in May 2015 for becoming a "manufacturing power."

As far as the discussion in Chapter 4 goes, some scholars perceive that military-civil fusion in informatization constitutes the most important component of military-civil fusion that is broad in scope.[66] With respect to informatization and military-civil fusion, attention is turned to the idea of "all people concurrently serve as soldiers [*quanmin jianbing*, 全民兼兵]." This is regarded as the social hallmark of future informatized warfare. In peacetime, reserve personnel are assigned to

private-company positions closely tied to the military including internet industries; in wartime, the military secures the necessary personnel from the private sector. This model is thought to achieve savings on military expenditure.[67] With China's abundant outstanding talent in the private sector, remarkable advances have been made in military-civil fusion in the information sector where industries expect to see rapid growth. The CCP leadership established the Central Leading Group for Cybersecurity and Informatization in 2014 and elevated it to Central Cyberspace Affairs Commission in 2018. The Cybersecurity Law also entered into force in 2017. In this way, arrangements are being strengthened for the CCP and the state to provide leadership and management in the cyber field. Fusion between the national defense sector and the private sector requires coordination not only across the military and local governments, but also ministries, industries, and regions. Therefore, CCP's coordinating function will become vital.[68]

3. China's External Activities related to Cybersecurity and the International Reaction

(1) China's Efforts on Cyber Governance

The international issues concerning China's cybersecurity can be divided into two categories: cyberspace governance; and cyber attacks. China's activities in both categories are attracting attention. In particular, differences in vision are becoming more manifest between China and the Western countries that advocate liberal democracy.

The recognition and initiatives on cyber governance are not unified among the major countries, and international rules on cyber governance are still in the development phase. Under such circumstance, the Government of China considers that now is an important time to seize the initiative in shaping international cybersecurity rules. In the National Cyberspace Security Strategy (hereinafter referred to as "NCSS") unveiled in December 2016, the Chinese government expresses the recognition that, "International competition for control of strategic resources in cyberspace, the right to set rules, the occupation of strategic positions for command (e.g., of international standards), and seizing the strategic initiative have continued to intensify."[69]

The Chinese government has its own perception of national sovereignty in cyberspace. NCSS states, "Cyberspace sovereignty is an important part of state sovereignty." While both Western countries and Japan acknowledge sovereignty in cyberspace, they concurrently emphasize that government intervention should be constrained based on their endorsement of freedom of expression. In contrast, the national sovereignty advocated by the Chinese government includes the government's right to regulate content in domestic cyberspace. Thus, it is worthy of note that government authority to intervene in cyberspace differs considerably between China and Western countries. On this account, the Chinese government stresses that cyberspace should be addressed through new treaties

under the recognition that, "As a new frontier, cyberspace needs to be governed by rules and norms of behavior."[70] Underlying this is the perception that applying existing international law to cyberspace will compel protection of human rights in cyberspace, such as freedom of speech and secrecy of communications, making China's censorship and communications interception difficult.[71]

Since the Xi Jinping administration came into power, the Chinese government has established cyber sovereignty in China by passing a series of legislation, including the National Security Law, the Counter-Terrorism Law, and the Cybersecurity Law. Alongside this, the government has shown an active intent to the international community to pursue the development of international rules. China has established international agreements with like-minded countries, including conclusion of an intergovernmental cooperation agreement on information security among the Shanghai Cooperation Organization (SCO) states including Russia. In 2011, China and three other SCO member states proposed the International Code of Conduct for Information Security to the United Nations (UN). In this way, China has sought to form international rules on cyberspace governance. At the same time, with Western countries that have different views than China, the country has advanced dialogue for the creation of cyberspace rules focusing on confidence-building measures. For example, for the compilation of the "Tallinn Manual on the International Law Applicable to Cyber Warfare" led by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Professor Huang Zhixiong at Wuhan University from China participated in the drafting of the "Tallinn Manual 2.0" released in 2017. Despite such developments, however, China and Western countries still have not resolved their differences over neither the issue of national sovereignty in cyberspace, nor the issues surrounding the applicability of existing international law.[72]

In addition to forming international rules, in recent years the Government of China has been preparing to formulate China Standards 2035 [*zhongguo biaozhun 2035*, 中国标准2035], an action plan for unifying and internationalizing domestic standards. Under this plan, China will likely aspire to set standards for international communications technologies and other technologies.[73] From this standpoint, it is noteworthy that China's Ministry of Industry and Information Technology and Chinese communications companies, including Huawei, proposed standardization of new IP addresses at the UN specialized agency, the International Telecommunication Union (ITU).[74] Already appointed to ITU's top position of Secretary-General is Zhao Houlin from China, and countries including the United States and the United Kingdom have expressed concerns over this proposal being taken up for consideration.[75] Some analysts argue that achieving cyber dominance, which is considered one of the key components of information dominance, requires authority over international internet route servers, the right to distribute IP addresses, the right to establish standards, and wide-ranging authority over computer networks including ability to shape public opinion online.[76] From this perspective, the Chinese government's activities to set standards for international communications technologies are consistent with the PLA's stance toward achieving information dominance that was discussed earlier.

On a related note, some contend that bringing information communications infrastructure made in China to developing countries will lead to the proliferation and strengthening of authoritarian regimes. In recent years, the Chinese government and Chinese companies have exported their information communications infrastructure and provided trainings in related technologies to developing countries to help build up their capabilities in public safety and countering terrorism.[77] A Chinese scholar points out that China's own satellite navigation system, the BeiDou Navigation Satellite System (BDS), can protect governments from Western "peaceful evolution [*heping yanbian*, 和平演变] (meaning, attempt at transforming a regime to a democracy)" via cyberspace, and in this regard, that BDS is suitable for the Middle East where there are many authoritarian regimes.[78] Furthermore, if the Chinese government's use of cyber technologies for surveillance and control of the people to contain the coronavirus disease (COVID-19) pandemic in 2020 receives widespread acclaim, China's cyber technologies and governance approaches may find acceptance in developing countries. Attention is being drawn to these developments as an illustration of how China's increasing global presence in the cyber domain has implications for the international community.

(2) China-U.S. Relations concerning Cyberspace

The U.S. government in particular displays wariness of China's increasing cyber warfare capabilities and cyber attacks. Among the cyber issues, the U.S. government is especially dissatisfied with the Chinese government and military agencies' commercial espionage of U.S. companies. At the China-U.S. summit meeting in September 2015, the two countries confirmed agreement that: (1) neither country's government will conduct or support cyber-enabled theft of intellectual property; and (2) they will establish a high-level dialogue mechanism for discussing anti-cyber crime measures that will meet twice a year. Despite this, the United States has continued to have deep-seated suspicions about the agreement's implementation by Chinese authorities. Moreover, China-U.S. high-level dialogue on cyber has not functioned effectively following the inauguration of the Donald Trump administration, and this has contributed to significant loss of momentum in the China-U.S. dialogue on cyberspace.

In the meantime, the PLA's informatization has made progress, and the resumption of cyber attacks originating in China from around 2017 has compounded U.S. frustration and distrust.[79] As China has enacted the Cybersecurity Law and the National Intelligence Law in recent years, scholars have noted that depending on their interpretation they may give the Chinese government legal access to networks developed and maintained by Chinese information communications companies.[80] Indeed, China Telecom hijacked messages between the United States and its allies and sent them to China through routes that deviate from the anticipated simple route. It is said that due to such cyber attacks by China, malicious attackers can enter an organization's network, steal data, add malicious implants, and modify or destroy data.[81]

Coupled with the battle for technological hegemony between China and the United States,

the U.S. government has growing concerns over China's cyber attacks. Cyber is listed as the first threat in the annual *Worldwide Threat Assessment* compiled by the U.S. Senate Select Committee on Intelligence in January 2019. The report names Russia and China as increasing the persistent cyber espionage and cyber attack threat to the U.S. military and critical infrastructure systems.[82] The *National Counterintelligence Strategy* issued in January 2020 by the U.S. National Counterintelligence and Security Center also notes that Russia and China take global actions targeting the United States. The strategy then presents the objectives of their countermeasures: (1) protect the nation's critical infrastructure; (2) reduce threats to key U.S. supply chains; (3) counter the exploitation of the U.S. economy; (4) defend American democracy against foreign influence; and (5) counter foreign intelligence cyber and technical operations.[83] In the midst of the continued outbreak of COVID-19, in May 2020, the U.S. Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security jointly issued a warning to health care, pharmaceutical, and research institutes engaged in the COVID-19 response to protect themselves from Chinese cyber attacks.[84] In response to media reports that such cyber attacks by China target research data and vaccine development status related to COVID-19, the Ministry of Foreign Affairs of China refuted that the reports were rumors and slanders.[85]

Beyond recognizing the threat posed by China, the U.S. government has also begun to take measures against Chinese cyber attacks. One of them is law enforcement by U.S. judicial authorities against China's illegal information theft. In 2014, the U.S. Department of Justice indicted five officers in Unit 61398 of the PLA for espionage against companies by way of cyber attacks. With that, from 2017 to the present, the Department of Justice has successively arrested and indicted Chinese nationals residing in the United States, the Chinese Ministry of State Security, and members of the PLA on charges of technology theft or cyber attack, etc.[86] It is expected that the U.S. government will continue to strengthen its legal measures against China's cyber attacks.

As another countermeasure, the United States has excluded Chinese cyber infrastructure companies from the market. Fearing that its cybersecurity vulnerabilities will increase, the U.S. government has sought to delist communications devices of companies suspected to have ties to the Chinese government's intelligence arm, including ZTE and Huawei, from the U.S. market. In 2014, the United States banned its government agencies from using Huawei products. In 2018, the United States banned companies working with the U.S. government, along with companies working with

such companies, from using products and services of companies like Huawei. In addition to measures on U.S. soil, the government has sought to exclude Chinese companies from the global market. For example, with governments of allies and partners with which confidential information is exchanged, the United States has warned and strengthened information sharing about market entry of Chinese companies that have suspicious investment objectives. Especially with regard to communications infrastructure of the fifth generation mobile communications system (5G), the United States has applied pressure on several allies and partners since around 2018 not to sign a contract with Huawei, notifying them that if they do so, the United States will lower the level of confidential information sharing between their intelligence authorities. While on the one hand some countries have decided not to use the 5G equipment of Chinese companies, on the other hand the U.S. attempts to counter Chinese companies have not necessarily gained widespread support.

Chapter 3

China's Military Use of Space

Fukushima Yasuhito

1. Relationship between Space Policy and National Defense Policy

(1) Long-term Goals of Space Activities and the Military

Since the Xi Jinping administration's establishment, space activities have been considered a means for achieving "the great rejuvenation of the Chinese nation." In 2013, President Xi Jinping (General Secretary of the Chinese Communist Party [CCP]) stated that developing the space program and turning the country into a space power is the space dream, and that the space dream is part of the dream to make China stronger.[1] *China's Space Activities in 2016* (hereinafter referred to as the "2016 Space White Paper"), a white paper published by the State Council Information Office, mentions that to explore the vast cosmos, develop the space industry, and build China into a space power is a dream China has pursued unremittingly.

"Space power [*hangtian qiangguo*, 航天强国]" is a concept unique to China, has a different meaning from "major space country [*hangtian daguo*, 航天大国]," and is not a notion specific to the military. In 2017, Lei Fanpei, Chairman of the board of China Aerospace Science and Technology Corporation (CASC), one of the two major state-owned space enterprises, commented that China is a major space country but has not reached the level of a space power. Chairman Lei noted that by having more than 200 spacecraft in operation and conducting around 30 annual launches by 2020, China will surpass the European Union (EU) and approach the level of a world space power.[2] He added that by 2030 China will surpass Russia and join the ranks of global space powers, and that by 2045 China will partially catch up with the United States and establish itself as a comprehensive space power. China's space activities based on these long-term goals are broad-ranging. The activities focus not only on those oriented primarily toward military purposes but also on raising national prestige, improving the level of science and technology, and stimulating the economy.

Meanwhile, the People's Liberation Army (PLA) plays a core role in China's space activities, making space and military activities inseparable. China's space activities arose out of Mao Zedong's policy on developing "two bombs, one satellite [*liangdan yixing*, 两弹一星]." "Two bombs" refer to the nuclear bomb (initially the atomic bomb; later the atomic bomb and hydrogen bomb) and missile [*daodan*, 导弹]; "one satellite" means an artificial satellite.[3] Pursuant to this policy, the Central Committee of the CCP headed by Mao Zedong established the Fifth Research Academy under the Ministry of National Defense (MND) in 1956 to oversee the development of launch vehicles and missiles.[4] In China, the establishment of the Academy is understood as the beginning of its space programs.[5] Besides, the missile and "one satellite" are closely related. In 1970, China successfully launched its first satellite (Dong Fang Hong 1) using the Long March 1 launch vehicle, which was based on the Dong Feng 4 intermediate range ballistic missile.[6] China's space program achievements listed in the 2016 Space White Paper include not only those related to satellites, crewed spaceflight,

and lunar probe, but also atomic bombs, hydrogen bombs, and missiles. As this makes clear, the country's space programs and military activities are intricately linked.

Furthermore, China started using satellites for military purposes shortly after it launched its first satellite. Specifically, it used recoverable satellites [*Fanhui Shi Weixing* (FSW), 返回式卫星] to conduct reconnaissance of other countries. At the end of its mission, the capsule on the FSW satellite is capable of reentering the atmosphere and is recoverable. Although the maiden launch in 1974 ended in failure, the second attempt in the following year succeeded in launching a satellite and recovering a film capsule.[7] With this, China became the third country in the world to successfully recover a film capsule (the United States and the Soviet Union first succeeded in 1960 and 1962, respectively). Until around 1990, the payload of FSW satellites was mainly optical sensors, and areas of the earth of interest to China were photographed from space.[8]

The Government of China holds peaceful development as one of the principles of space activities. The 2016 Space White Paper states that China always abides by the principle of the use of space for peaceful purposes and opposes the weaponization of and an arms race in space. This is not intended to deny military use of space. Rather, the same white paper goes on to say that an objective of space activities is to meet the demands of national security. Indeed, the Chinese media makes occasional references to the military use of space. For example, according to the CCP's English language newspaper, *China Daily*, when President Xi Jinping visited the Xichang Satellite Launch Center in 2018, he ordered the center to focus on military training and research, enhance satellite launch and combat capabilities, and integrate itself with the PLA's joint operation system.[9]

That said, in many other countries, militaries are also engaged in the entire spectrum of space activities and space is utilized for military purposes; China is not an exception. China's development of its first satellite launch vehicle based on a ballistic missile is the same as its predecessors, notably, the United States and the Soviet Union. Furthermore, it is the international standard interpretation that peaceful uses of space include non-aggressive military uses. As such, it is not peculiar that China uses space for military purposes while advocating its peaceful development.

(2) Space in the Context of the National Defense Policy and PLA Unit Operations

China's space activities from their inception have been closely linked to military activities as described above. However, it was only in the 1990s that the military value of space began to be recognized more widely in the PLA. Though it has not fought a major war since the 1979 Sino-Vietnamese War, China has made observations of other countries' wars to assess the characteristics of modern warfare and has sought to develop military capabilities needed to win such wars. In particular, large-scale U.S. operations since the 1990s offered considerable lessons for the PLA. In 1993, the Central Military Commission (CMC) gave a new focus to winning "local wars under high-tech conditions," and in 2004, the CMC announced its intention to build up military capabilities to

win "local wars under the conditions of informationization."

In parallel with this shift in military strategy, the military value of space began to gain greater appreciation. During the 1991 Gulf War, various satellites were utilized to support the operations of the U.S. forces and other multinational forces, to the extent that the war was dubbed "the first space war." This war is considered to have made the PLA aware of the battleground's expansion to outer space.[10] In addition, through observations of the North Atlantic Treaty Organization's (NATO) air strikes against Yugoslavia in 1999, the PLA appears to have developed a deeper understanding of the role space plays in operations.[11] In 2002, Jiang Zemin, Chairman of the CMC, expressed the view that space will become a new strategic high ground in international military competition.[12] In 2004, Hu Jintao, who replaced Jiang Zemin as Chairman of the CMC, made clear that the PLA must safeguard China's interests in space as part of the PLA's "new historic missions."[13] Also in 2004, the Air Force proposed the "integration of air and space capabilities" to the CMC, and it was formally approved as an Air Force strategy in 2014.[14] In addition, the National Defense White Paper 2015 argued: "The world revolution in military affairs (RMA) is proceeding to a new stage. Long-range, precise, smart, stealthy and unmanned weapons and equipment are becoming increasingly sophisticated. Outer space and cyber space have become new commanding heights in strategic competition among all parties. The form of war is accelerating its evolution to informationization." There is a growing recognition in the PLA that information dominance is key to winning informatized warfare and that space is an inalienable component of information dominance.[15]

Furthermore, the National Defense White Paper 2019 (hereinafter referred to as "NDWP 2019") expressed anew that war is evolving into informatized warfare, and that intelligentized warfare has begun to take tangible form. Intelligentized warfare is defined as "integrated warfare waged in land, sea, air, space, electromagnetic, cyber, and cognitive domains using intelligent weaponry and equipment and their associated operation methods, underpinned by the Internet of Things (IoT) information system."[16] Space continues to be considered an essential domain for executing such warfare.

The strategic guiding thought for military struggle over space is outlined in the 2015 edition of *Science of Military Strategy* published by the National Defense University, namely, that deterrence is the primary means while war is an auxiliary and that the contest for space dominance is at the core of these struggles.[17] Like cyber deterrence, the concept of space deterrence [*kongjian weishe*, 空间威慑] in China consists not only of dissuading an enemy's actions but also compelling an enemy to take certain actions.[18] While the concept of space dominance is similar to space control in the United States, the former is a broader concept that encompasses providing information support from space as well as maintaining one's own space use and denying an adversary's use of space.[19]

As regards space dominance, the PLA has recently begun to place emphasis not only on offense but also defense aspects.[20] China's policy of securing interests in space is not confined to the military. Article 32 of the National Security Law enacted in 2015 enshrines securing China's activities, assets, and other interests in outer space as well as international seabed areas and polar

regions. NDWP 2019 expresses the view that outer space security provides strategic assurance for national and social development and articulates an intention to safeguard space assets.

Ensuring mission assurance to maintain the functions necessary for mission execution is a major challenge for militaries dependent on space use. The PLA recognizes its importance, albeit little information has been made public on how it will do this. The Satellite Navigation Research and Development Center at the National University of Defense Technology directly under the CMC has reportedly succeeded in developing electromagnetic shields for protecting the BeiDou Navigation Satellite System (BDS) from radio interference.[21] Their development was motivated by the existence of states that research interference of positioning signals, raising fears that, unless the problem of radio interference is solved, "weaponry that relies on navigation and positioning, such as China's fighters and missiles, will be unable to fully fulfill its role, leading to decreased combat capability."[22] Moreover, the enhanced variant of the CH-4, a long-endurance unmanned aerial vehicle (UAV), can carry laser-guided munitions on top of satellite-guided munitions, which allows for the execution of strike missions even when jammed.[23] In the future, UAVs may partially substitute communications satellites. CH-T4 developed by CASC is powered by solar energy and can conduct smooth flights even at altitudes of 20 kilometers or higher above sea level where air is thin. CH-T4 can also allegedly remain in flight for many hours without refueling.[24] It is expected that the UAV will be able to fly for several months or longer in the future. CASC plans to have such a drone serve as a "quasi-satellite" and provide communication relays. According to CASC officials, this type of UAV can also be used for intelligence, surveillance and reconnaissance (ISR), early warning, and signal intelligence.[25] These efforts have the potential to improve the PLA's mission assurance.

Furthermore, space-based information support (e.g., reconnaissance, positioning, communications) is anticipated to make PLA operations more efficient and effective. For example, an article in the Japanese edition of the *People's Daily Online* dated February 6, 2013 introduced an MND research report stating that 1,465 fighters equipped with the Global Positioning System (GPS) have combat capability equivalent to 1,714 fighters without GPS, and pointed out that the use of BDS (Chinese version of GPS) will lead to China's military cost savings. The same article cites an expert as saying, "As the construction of BDS proceeds and its coverage expands, BDS will likely double the combat capability and effectiveness of the Chinese military."

Space-based information support has gained importance as the PLA broadens its area of operation. Especially the Navy and Air Force have stepped up activities in open seas as well as in offshore waters. Satellite communications are indispensable for mobile users, such as vessels and aircraft, to communicate with certainty with command headquarters and friendly troops that are out of line-of-sight. Satellite positioning is also essential for accurately knowing one's position in the large expanse of sea. In particular, under present circumstances, wide-area operation of long-endurance UAVs is inconceivable without satellite communications and satellite positioning. In the case of the CH-5 that conducted the first flight in 2015, for example, it has an operable range of up to

250 kilometers via line-of-sight data-link, but it can be extended to 2,000 kilometers if satellite communications are utilized.[26] For the operation of anti-ship ballistic missiles which requires searching for vast areas, it is expected that maritime reconnaissance by satellites, together with over-the-horizon radars and other systems, will provide targeting information.[27] If space-based information support is utilized more actively by the PLA, its operational dependence on space systems will rise, which will increase the necessity of ensuring mission assurance for maintaining space use.

The PLA's emphasis on space is reflected conspicuously in China's military reforms. The Strategic Support Force (SSF) was established in late 2015 coinciding with the elevation of the Second Artillery Force to Rocket Force. The SSF is under the direct command of the CMC. Its purpose is to provide resources that can secure space security alongside cybersecurity.[28] The SSF has the Space Systems Department, which integrates the space-related missions formerly overseen by the General Armament Department and the General Staff Department.[29] These missions are thought to include space launch and support; space telemetry, tracking, and control (TT&C); space information support; space attack; and space defense. Analysts note that the Network Systems Department, which is also under the SSF, has a unit responsible for electronic countermeasures against satellites.[30]

Thus, the PLA recognizes the role of space in modern warfare and has taken steps to integrate space capabilities into unit operations. As already noted, however, the PLA has not experienced a major war in 40 years. The U.S. forces, in contrast, has integrated space capabilities into unit operations while drawing lessons from actual warfare, such as the Gulf War, the air strikes against Yugoslavia, the War in Afghanistan, and the Iraq War. It is difficult to say how effectively the PLA can provide space-based information support for its units on the ground, at sea, and in the air in actual warfare.

2. Situation of Space Activities and Their Military Implications

(1) Operations of Space Systems

As discussed above, China has set a goal to become a comprehensive space power by 2045 and

is pursuing a wide range of space development and utilization. While China has not disclosed its space budget, it is estimated at around US$5.8 billion (2018) according to Euroconsult.[31] This is the second largest after the United States' approximately US$40.9 billion and is larger than Russia's (approximately US$4.1 billion).

Against this backdrop, the number of China-operated satellites has grown steadily. According to the UCS Satellite Database, China is estimated to operate 363 satellites as of the end of March 2020.[32] Of the 2,666 satellites operating worldwide as of the same date, China has the second largest number of operating satellites after the United States' 1,327. China already operates more satellites than Russia (169 satellites). As shown in Table 3.1, China operates an array of satellite types such as those used for earth observation (including weather observation); communications; and positioning, navigation, and timing (PNT). Of these satellites, MND or the PLA is believed to possess or operate the following satellites: 65 earth observation satellites (Gaofen, Ludikancha Weixing, Yaogan); 3 communications satellites (Zhongxing); and 49 PNT satellites (BeiDou for BDS).[33]

Table 3.1 Number of Satellites Operated by China (by Purpose)

Purpose	Number
Earth observation	177
Communications	49
PNT	49
Earth science	2
Space science	15
Technology development	71

Note: "Earth observation" includes "earth observation/technology development" and "earth observation/communications" dual-purpose satellites. "Earth observation," "earth science," and "technology development" include satellites jointly operated with Brazil, France, Germany, or Italy.

Source: Compiled by the author, based on Union of Concerned Scientists, "UCS Satellite Database," last modified April 1, 2020, https://www.ucsusa.org/resources/satellite-database.

As noted earlier, it appears China operated photo reconnaissance satellites from the mid-1970s, but their performance was said to be nowhere near that of the United States and the Soviet Union.[34] Then came the 21st century, which saw dramatic advances in China's operation of earth observation satellites.

Gaofen is the space segment of the China High-resolution Earth Observation System (CHEOS) and is thought to be dual use.[35] Started in 2010, the CHEOS project aims to build a system capable of all-weather, 24-hour global earth observations using a combination of satellites, stratosphere airships, and aircraft by around 2020.[36] Launches of the Gaofen series commenced in 2013. For example, Gaofen-2 launched in 2014 is an optical satellite with a resolution of under 1 meter. Gaofen-3 launched in 2016 is a synthetic aperture radar satellite with a resolution of 1 meter. Gaofen-4 launched in 2015 is China's first optical earth observation satellite placed in the geostationary orbit (GEO) and has a resolution of 50 meters.[37] Earth observation satellites in GEO are globally rare. Ludikancha Weixing is a series of earth observation satellites launched from 2017.[38] They appear to be reconnaissance satellites with electro-optical sensors. The Yaogan satellites have been launched

since 2006.[39] They are believed to be reconnaissance satellites and are considered to consist of optical, radar, and signal intelligence satellites.[40] U.S. defense authorities speculate that Yaogan satellites replicate the U.S. maritime reconnaissance satellites and are used to keep abreast of vessel deployments in the Western Pacific.[41]

Two types of the Zhongxing satellite are used for military communications.[42] One is a satellite series known as Fenhuo. Fenhuo-1 launched in 2000 provided SHF (C-band) and UHF communications and is said to be a satellite for the Qudian, China's first integrated command, control, communications, computers and intelligence (C4I) system.[43] The other is a satellite series called Shentong, which began to be sent into space in 2003, and is said to provide communications in SHF (Ku-band) to users on the ground.[44]

Started in 1994, the BDS project has proceeded based on a three-step development strategy.[45] In the first step (BDS-1), two satellites were launched in 2000, and the system began providing pilot services in China. A third satellite was launched in 2003. In the second step (BDS-2), the launches of 14 satellites were completed in 2012, and the system began providing services in the Asia-Pacific. In the third step (BDS-3), the system began providing services worldwide by the end of 2018.[46] The BDS-3 consists of 30 satellites, and the launches of all satellites were completed in 2020.[47]

It has been announced that BDS has both civil and military signals.[48] The PLA likely seeks to shift from GPS to BDS to use with the satellite positioning system.[49] While GPS is a U.S. military-operated system, anyone can utilize its civil signals and they are used globally. To prevent an adversary's use of GPS, the United States announced that it will jam civil signals in the relevant region in an emergency.[50] For this reason, the PLA needs PNT services which can replace GPS and ensure stable access even in an emergency. PLA units have already begun using BDS for, for example, ammunition guidance, vessel and aircraft navigation, and location determination by soldiers.

A BDS feature not available on GPS is a function that notifies users' location to other users. This function is reputed for enabling a commander to have real-time information on the movements of his/her troops and for significantly increasing the combat capabilities of individual soldiers.[51] The function was utilized to maintain control over the numerous participants in the military parade, which celebrated the 70th anniversary of China's victory in the war against Japan.[52] Another feature of BDS not available on GPS is text messaging. Since short text messages can be sent from BDS terminals, PLA units are said to be utilizing this function as a complementary way of communications during exercises.[53]

In addition, observers repeatedly point to the PLA's ongoing development of early warning satellites.[54] China is developing a missile defense system, and early warning satellites that can detect ballistic missile launches quicker than radars on mainland China will play a critical role in establishing an interception posture. According to the U.S. Department of Defense, China's nuclear forces may aspire to secure a launch on warning posture (where China can immediately launch a ballistic missile upon receiving warning of an adversary's ballistic missile launch), and if so, early warning satellites may support this posture in the future.[55]

It is unclear which satellites China actually uses for military purposes and to what extent. Military use cannot be determined solely from whether or not a satellite was developed for military purposes. "Military use" applies not only to satellites that have been developed and launched at the military's request but also to other satellites if they are used by the military. Military use of services provided by satellites possessed and operated by non-military actors (civil satellites and commercial satellites) has become common internationally. As discussed later, China places importance on military-civil fusion in the space domain. In this light, it needs to be kept in mind that an overall improvement in space activities could strengthen China's military capabilities in the space domain.

In 2017, for instance, China announced that for the first time in the world it achieved intercontinental quantum key distribution using the Quantum Science Satellite Mozi, and that through this satellite China transmitted encrypted data and conducted a video communication.[56] China plans to start operating satellite-based, global quantum-encrypted communications by 2030.[57] The PLA's use of such capability will make its communications far more secure. It has also been found that, entering the 2010s, China has conducted rendezvous and proximity operation (RPO) tests repeatedly.[58] RPO constitutes the technical foundation of space-based anti-satellite (ASAT) weapons. Moreover, if satellites can be repaired with RPO capability in the future, this will translate into increased mission assurance.

In examining the situation of China's space activities and their military implications, one needs to consider capabilities pertaining to space access and space situational awareness (SSA). China has a range of satellite launch vehicles and has maintained a high launch frequency. The flagship Long March series have evolved from the first generation (e.g., Long March 1, 2) to the second generation (e.g., Long March 2C, 2D, 2E, 3), the third generation (e.g., Long March 2F, 3A, 4), and the fourth generation (e.g., Long March 5, 6, 7, 11).[59] These launch vehicles can be classified into small (e.g., Long March 6, 11), medium (e.g., Long March 2, 3A, 4, 7), and large (e.g., Long March 5).[60]

The Long March 5, first launched in 2016, is a heavy-lift launch vehicle used for the construction of a Chinese space station. It is China's largest launch vehicle and has a launch capacity nearly equivalent to that of the United States' Delta IV Heavy. Launches of the Long March 5 were suspended following the failed launch in 2017 but resumed in late 2019.[61] By around 2028, China aims to begin launching the Long March 9 comparable to the Saturn V, which the United States used for the crewed Apollo lunar probe program.[62] The Long March 9 launch vehicle is being considered for use in crewed exploration of the moon and beyond.

The Long March 11 is the only solid propellant rocket of the Long March series, which are predominantly liquid-propellant rockets.[63] The Long March 11 is designed for rapid satellite launch in an emergency and can be carried on a transporter-erector-launcher (TEL). The Long March 11 reportedly can complete preparation within 24 hours of receiving a launch order and can be launched daily. In 2015, it was launched successfully for the first time carrying four small satellites.

Other launch vehicles capable of sending small satellites into space at low cost and in a short time include the Kuaizhou series, which are also solid propellant rockets.[64] The 2016 Space White Paper assesses that successful launches of the Kuaizhou 1 and the Kuaizhou 2 (a satellite carried on the Kuaizhou 1) have improved China's emergency response capabilities in space. Kuaizhou 1 can also lift off from a TEL. Factories capable of producing 20 Kuaizhou launch vehicles a year (the Kuaizhou 1A and the new Kuaizhou 11) are slated to start operations by the end of 2020.[65]

Using a variety of launch vehicles, China conducted more launches than any other country in the world in 2018 for the first time (39 launches, including one failure) and again in 2019 (34 launches, including two failures).[66] China's goal of approaching the level of global space powers by operating more than 200 spacecraft and carrying out around 30 launches annually, as indicated by CASC Chairman Lei Fanpei in 2017, was achieved earlier than the 2020 target year.

China has four rocket launch sites. Three (Jiuquan, Taiyuan, Xichang) are located inland, and the remaining site (Wenchang) is on the coast. Wenchang is a new launch site capable of launching Long March 5 and has conducted launches since 2016.

China has sought to diversify its launch methods. In 2019, it successfully launched satellites from a sea-based platform using the Long March 11.[67] A sea-based platform has the advantage of offering flexibility to choose the launch position.[68] In addition, studies of the reusable space transportation system between the earth and low-earth orbit are under way. China Aerospace Science and Industry Corporation (CASIC), a state-owned space enterprise comparable to CASC, is implementing the Tengyun Project and aims to conduct the first flight of a space plane by 2030.[69]

China thus has a number of methods at its disposal to carry out frequent satellite launches. Therefore, by global standards, the country has one of the highest abilities to launch additional satellites in response to changes in the situation. If a satellite breaks down for any reason, China will likely be able to launch an alternative satellite to reconstitute the satellite constellation relatively quickly.

The foundation of the space activities elaborated above is SSA. Without SSA capability, it is not possible for satellite operators to determine where their satellites are flying, whether they will not collide with other satellites or space debris, and at what timing a rocket can be launched to avoid collision with satellites and space debris. For this reason, China has been putting efforts into enhancing SSA. The China National Space Administration, which oversees civil use of space and international cooperation, established the Space Debris Observation and Data Application Center in 2015.[70] The Center's responsibility includes developing systems that observe space debris and near-earth objects, performing the actual tracking and observations, addressing emergency situations, and engaging in international cooperation. According to the 2016 Space White Paper, China has improved the monitoring of and early warning against space debris, and such activities have been put into regular operation to ensure the safe operation of spacecraft. The white paper notes that in the next five years, China will continue to develop the space debris basic database and advance the development of space debris monitoring facilities, the early warning and emergency response platform, and the online service system.

NDWP 2019 also sets out the government's plans to strengthen SSA. SSA serves as the foundation for not only the safe operation of satellites but also achievement of space dominance. SSA provides information needed for China to conduct targeting when interfering with the space use of an adversary and is essential for detecting interference with China's own space use.

(2) Development of Counterspace Capabilities

China not only operates space systems to provide information support for operations on land, sea, and air, but is also developing capabilities to disrupt other countries' use of space. The counterspace capabilities being developed by China can be broadly divided according to target of attack: ASAT weapons, which attack satellites in orbit; and electronic countermeasure systems, which attack links connecting satellites and earth stations (control facilities and user terminals).

While it is said that China's development of dedicated weapons for ASAT can be traced back to 1970, test launches gathered pace only from the mid-2000s.[71] In 2007, China destroyed an old Chinese weather satellite in low Earth orbit (LEO) using an ASAT weapon. This test is thought to have used basically a derivative of the DF-21C medium-range ballistic missile (known as SC-19 among the U.S. intelligence community).[72] This type is called a direct-ascent ASAT, which is launched from a platform such as a TEL and reaches the target satellite on a ballistic trajectory. As a result of this successful test, China became the third nation after the Soviet Union and the United States to demonstrate destructive anti-satellite capability in orbit.

Although China admitted to performing an ASAT test only once in 2007,[73] it has since then repeatedly carried out SC-19 test launches not involving satellite destruction. It is believed that China has already completed operational deployment of ASAT weapons targeting LEO satellites (likely SC-19) and that it is conducting training.[74] Analysts note that the SSF is responsible for training units

that operate these weapons.[75] Furthermore, it is deemed that in 2013, China carried out a test launch of a new direct-ascent ASAT missile (called DN-2 in media reports).[76] According to the analysis of U.S. defense authorities, its range may cover GEO.[77] China also reportedly conducted test launches of its third direct-ascent ASAT missile (called DN-3 in media reports) in the latter half of the 2010s,[78] but some observers note that these missiles may be a mid-course missile defense system.[79]

In addition to direct-ascent ASATs, a report published by the U.S. Defense Intelligence Agency (DIA) in 2019 assesses that China is developing capabilities to inspect and repair satellites in orbit, some of which are capable of functioning as weapons.[80] The report does not go so far as to explain how China may utilize these capabilities as weapons. In general terms, however, DIA states that the following methods could be utilized for satellite-to-satellite attacks: kinetic kill vehicles; radiofrequency jammers; lasers; chemical sprayers; high-power microwaves; and robotic mechanisms.[81]

China could deploy a laser weapon targeting sensors on LEO satellites by 2020.[82] Also, DIA notes that, from the mid-to-late 2020s, China may deploy higher power laser weapons that can attack non-optical satellites.[83]

As regards electronic countermeasure systems, China is thought to have jamming capabilities against GPS and satellite communications.[84] The PLA's electronic warfare units carry out routine training to conduct jamming against GPS signals alongside communications and radar systems.[85] On Mischief Reef of the Spratly Islands, China has reportedly deployed mobile jammers targeted at GPS and other global navigation satellite systems.[86] The U.S. forces has revealed that it monitors jamming against communications satellites while its aircraft carriers sail through the South China Sea.[87] DIA analyzes that China continues to develop jamming capabilities against satellite-borne synthetic aperture radars.[88]

Additionally, China may have cyber attack capabilities against space systems. In 2007 and 2008, U.S. civil use earth observation satellites were reportedly under Chinese cyber attacks via ground stations.[89] Furthermore, the PLA is considering attacks against satellite TT&C facilities and launch sites.[90] Such attacks do not require dedicated weapons and can be carried out with ballistic missiles, cruise missiles, or special forces, for example.

The focus of attention should be on when and how the PLA will utilize its multiple counter-space capabilities. One cannot discount the possibility that preemptive attacks in the space domain lie within the purview of the PLA, given that its military strategy emphasizes the preemptive attack element as part of "active defense." In that case, the question of which means of interference the PLA will actually utilize also deserves attention. Will the means be limited to electronic countermeasure systems against the links? If the PLA were to attack satellites, will it be limited to reversible means, such as lasers for dazzling sensors on satellites? Or will the PLA employ non-reversible means like destructive ASATs for preemptive attacks?

In particular, how does the PLA perceive the risk of secondary damage to its satellites caused by space debris produced by the destruction of satellites? In the case of an armed conflict between

China and the United States, will the PLA actually destroy satellites, judging that the United States loses more than China from the destruction of satellites and its secondary damages? China's reliance on space is expected to keep increasing. In this context, the questions of when and how destructive ASAT weapons should be used will become even more critical issues for the PLA.

(3) Military-Civil Fusion in Space Activities

China regards the development and use of space as a key area of the military-civil fusion strategy. President Xi Jinping has urged the SSF to focus on integration of military and civilian development.[91] Advancement of military-civil fusion in space activities may lead to strengthening China's use of space for military purposes.

In China, emerging space enterprises have rapidly boosted their technological capabilities with government and military support. State-owned enterprises have traditionally developed and manufactured Chinese satellites and launch vehicles. Specifically, they are the two enterprises under the State Administration of Science, Technology and Industry for National Defense (SASTIND): CASC and CASIC. These two trace their origin to the Fifth Research Academy of MND.[92]

To this day CASC and CASIC remain leading players in the Chinese space industry. However, there have been noteworthy changes in the last five years. In 2014, the Government of China decided to open the space sector to private capitals. At a State Council executive meeting in the same year, Premier Li Keqiang officially encouraged private capital investment in the space industry.[93] This gave impetus to the establishment of numerous emerging space enterprises in China.

Emerging space enterprises that have set themselves apart from traditional space enterprises have been established globally since the 2000s, led by the United States, and have increased their presence especially since the 2010s. These enterprises have come to be called "New Space" as opposed to "Old Space" (e.g., Boeing, Lockheed Martin).[94] Representative examples include SpaceX founded by Elon Musk and Blue Origin established by Jeff Bezos in the early 2000s. In particular, SpaceX has had significant influence on space business trends, not only driving down prices of satellite launch services but also planning the provision of an internet service enabled by a constellation of thousands to tens of thousands of satellites.

Emerging space enterprises in China can be dubbed the Chinese version of New Space. As of the end of 2018, 141 aerospace enterprises have been registered in China, consisting of 36 satellite manufacturing enterprises; 22 launch vehicle manufacturing enterprises; 39 satellite operation enterprises; and 44 satellite applications enterprises.[95]

For example, Beijing Commsat Technology Development established in 2015 aims to launch 72 IoT satellites into LEO by 2022.[96] Galaxy Space founded in the following year, 2016, has a scheme to provide high-speed global communications by launching up to 1,000 5G satellites into LEO.[97] Galaxy Space launched a technology verification satellite in January 2020.[98] Beijing Interstellar Glory Space Technology (iSpace), also founded in 2016, became the first Chinese private rocket

company to successfully launch satellites with an independently developed rocket in July 2019.[99] The solid propellant rocket Hyperbola-1 developed by iSpace was launched from Jiuquan Satellite Launch Center administered by the SSF.[100]

Private companies are rapidly improving their technological capabilities against the backdrop of the military-civil fusion strategy pursued by the Chinese government. Technologies are being transferred to these companies to promote innovation in dual-use technology.[101] Following its successful launch, iSpace expressed its appreciation to CASC, CASIC, SASTIND, and the CMC Equipment Development Department for their support.[102] At the top of its "About Us" webpage, One Space Technology (One Space) founded in 2015 states that President Xi Jinping elevated military-civil fusion to national strategic level in 2015.[103] In an interview with the foreign media, One Space noted that China already has mature space technologies and that the job of private companies is to apply the military's aerospace technologies to private-sector launch vehicles.[104]

In June 2019, SASTIND and the CMC Equipment Development Department jointly created and released rules on manufacturing, test flights, and launches of commercial rockets.[105] The rules explain the significance of commercial rocket development in the context of increasing China's space power and international competitiveness, coupled with potentially lowering the development costs of the space sector.[106] The specific rules include the need for commercial rocket companies to obtain SASTIND's prior permission for research and manufacturing and to give prior notice to relevant departments when actually beginning research and manufacturing.[107] The published rules also contain a provision encouraging companies to make maximum use of national resources for technology research, manufacturing equipment and facilities, and launch sites.[108]

In December 2019, the China Commercial Space Alliance was launched by entities including the China Space Foundation, China Volant Industry (CASIC subsidiary), China Great Wall Industry Corporation (CASC subsidiary), and Chinese Academy of Sciences Holdings.[109] The Alliance plans to support member organizations through such activities as providing information under the guidance of the China National Space Administration.

The coronavirus disease (COVID-19) pandemic has forced delays in China's private-sector space activities in the first half of 2020 and has slowed fundraising.[110] However, as the National Development and Reform Commission added satellite internet to the list of "new infrastructure development" in April 2020, investments in this sector have begun to gather pace.[111]

At present, China's private space firms are in their early stages, and it appears premature for the military to use technologies or services that the companies developed. Nonetheless, the Chinese version of New Space has grown at an extraordinary pace, supported by the government and the military under the military-civil fusion strategy. The future is expected to herald an era in which the military adopts the technologies developed by the private sector and uses its services.

3. International Relations over the Space Domain

(1) Relations with the United States

China sees the United States as the world's No. 1 space power and as the ultimate goal of Chinese space programs. As was already discussed, observations of U.S. combat operations in the 1990s and thereafter made the PLA realize that space plays a key role in modern warfare. Analysts suggest that the U.S. Strategic Command served as the model for creating the SSF that integrated space and cyber forces into a single organization.[112] Meanwhile, China is wary of U.S. military activities in the space domain. NDWP 2019 indicates China's recognition that the United States has improved its capabilities in the space domain and is undermining global strategic stability.

Likewise, the United States has become strongly cautious about China's stepped-up activities in space. In particular, U.S. military space activities since the 2000s cannot be discussed without mentioning China. China's destructive ASAT test in 2007 was a major wakeup call to the entire U.S. forces.[113] China's test firing of a new ASAT weapon in 2013 gave the United States impetus to conducting the Space Strategic Portfolio Review, and since then, has been preparing itself for a war in space.[114]

The Donald Trump administration inaugurated in 2017 labeled China as a strategic competitor and maintains vigilance of the space domain. In a 2018 address, Vice President Mike Pence, alongside mentioning Russia's activities, remarked that China was developing ASAT weapons and that in 2015, China created a separate military organization to oversee and prioritize its warfighting capabilities in space (likely in reference to the SSF).[115] Vice President Pence went on to express the view that U.S. adversaries have already transformed space into a warfighting domain. Based on this recognition, in late February 2019, the Trump administration submitted a bill to Congress to create the Space Force. The National Defense Authorization Act for fiscal year 2020, which contains provisions on creating the Space Force, was passed in late 2019, establishing the Space Force as the sixth branch of the armed services following the Army, Navy, Air Force, Marine Corps, and Coast Guard.

The Space Force flag unveiled at the White House (May 15, 2020) (Photo by: Shealah Craighead, White House)

In his regular press conference on February 28, 2020, a spokesperson for the Chinese MND criticized that it was the United States which has been weaponizing space, and that as was well known, the United States, in

pursuit of space hegemony, has created the Space Force, spent significant funds on enhancing space combat readiness, and unilaterally initiated an arms race in space.[116] He went on to state that the U.S. accusation against China was an excuse for the United States to strengthen its military capabilities. In addition, the *PLA Daily* dated April 9, 2020 sounded alert over the U.S. Space Force's deployment of Counter Communications System Block 10.2, and expressed concern that other countries may follow the United States in acquiring or preemptively utilizing similar weapons.

Moreover, the moon and surrounding area are beginning to become a new area of competition between the United States and China. China launched the Chang'e 4 lunar probe in 2018 and became the first country in the world to successfully soft-land it on the moon's far side in 2019. To secure communications with Chang'e 4, the Queqiao relay satellite was placed in orbit around Lagrange point (EML2).[117] With Chinese activities in cislunar space (outer space between the earth and the moon) starting to become normal, U.S. defense authorities have raised concerns that U.S. satellites in GEO may suffer surprise attacks from the moon side.[118] U.S. defense authorities therefore have begun examining capabilities to collect information on activities in cislunar space.[119]

While the United States and China are increasingly wary of each other, there remains room for expanding cooperation between the two countries. Currently, the U.S. military notifies China if an artificial object is found approaching a Chinese satellite.[120] This is because if a Chinese satellite is destroyed due to collision with an artificial object and causes space debris, there is risk of secondary damage to satellites used by the United States. As was noted, China already operates the second highest number of satellites in the world. Furthermore, the growth of the Chinese version of New Space is expected to further increase the number of China-operated satellites. China's safe operation of satellites is thus a vital issue for the United States. The two countries have a shared interest in securing stable use of space. From this perspective, future U.S.-China discussions on matters such as international rule-making, SSA sharing, and space traffic management are worthy of attention.

(2) Relations with Other Countries

The United States is not the only country wary of China's increasing military space activities. India conducted its first destructive ASAT test in 2019. The Ministry of External Affairs of India expresses the view that the capability achieved through the test will serve as deterrence against threats to India's space assets.[121] Although the ministry states that the test was not directed at any specific country, it is believed that the test was carried out with China in mind.[122]

On the surface, China's reaction to the test was restrained. Asked about the test at a regular press conference, an MND spokesperson merely stated that China takes notice of related reports and hopes all countries can take real actions to protect lasting peace and stability in space.[123] However, with counterspace capabilities becoming more widespread around the world, the PLA will have to put further efforts into not only offense but also defense aspects of space dominance.

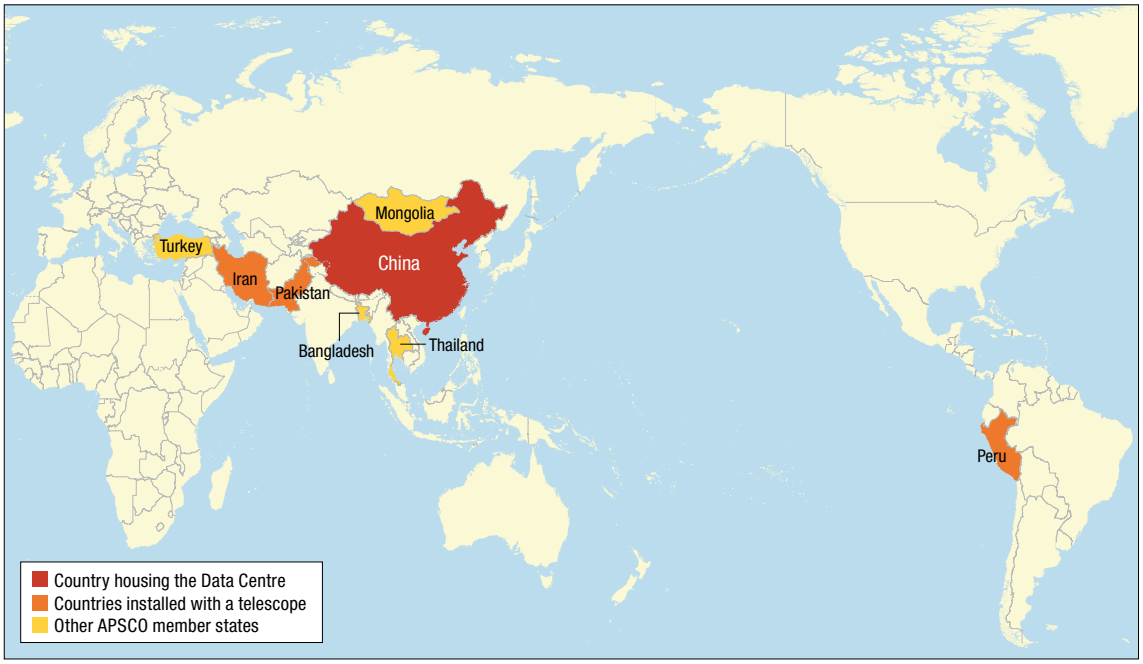
While there are countries that seek to counter China, a number of nations are also eager to

work with China in space activities and China is enthusiastic about pursuing such cooperation. Its most important partner is Russia. In 2008, China and Russia proposed the Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects (PPWT) at the Conference on Disarmament (CD). In 2014, the two countries jointly submitted a new PPWT draft to CD. Behind the China-Russia PPWT proposal is likely an intention to keep the United States from deploying missile interception systems into space.[124] Furthermore, China is advancing cooperation with Russia on satellite positioning, as the latter operates the Glonass satellite positioning system. The political leaders of the two countries have prioritized such cooperation since 2012, and in 2015, China and Russia concluded an agreement on securing BDS-Glonass compatibility (meaning each other's signals will not cause interference) and interoperability (meaning each other's signals can be used on their respective terminals).[125] An article in *Global Times* (dated September 3, 2019), an English-language newspaper published by the *People's Daily*, suggested that synergistic effects between BDS and Glonass will offset GPS dominance in satellite positioning. In addition, in 2019, President Vladimir Putin announced that Russia was providing assistance for China's creation of a missile warning system.[126] Although the details of the cooperation have not been made public, the question of whether it will be related to China's development and future operation of early-warning satellites deserves attention.[127]

China also actively works with other countries through the Asia-Pacific Space Cooperation Organization (APSCO). APSCO is an intergovernmental organization founded in 2008 under China's leadership and is headquartered in Beijing. Its eight member states are China, Bangladesh, Iran, Mongolia, Pakistan, Peru, Thailand, and Turkey. Egypt, Indonesia, and Mexico are associate member, signatory state, and observer state, respectively. In particular, SSA cooperation may have security implications among APSCO's wide-ranging areas of cooperation. In 2011, APSCO initiated a project known as the Asia-Pacific Ground-Based Space Object Observation System (APOSOS).[128] Its main objective is to create a network observing objects in orbit (initially in LEO) using optical telescopes of member states and provide collision avoidance and early warning services that are necessary for member states to operate space assets. As shown in Figure 3.1, in 2015, telescopes were installed in Pakistan and Peru, and the APOSOS Data Centre was established in Beijing. In 2016, a telescope was installed in Iran as well. APSCO plans to install larger-diameter telescopes in all member states, enable observation of objects as small as 10 centimeters in LEO, and allow for the tracking of objects in medium Earth orbit and GEO and near-earth objects. As already stated, SSA is the foundation of all kinds of space activities, and data collected by APOSOS could be utilized as a basis of PLA space operations.

Moreover, China has established TT&C facilities across the globe and has already begun operating facilities in Pakistan, Namibia, Kenya, Australia, Chile, Brazil, Argentina, and Sweden.[129] The facility in Kiruna, Sweden is a data reception station for earth observation satellites that China installed overseas for the first time in 2016.[130] With this facility now being operational, it is said that

Figure 3.1 APOSOS' Observation Network



Source: Compiled by the author, based on Asia-Pacific Space Cooperation Organization, "Ground-Based Space Object Observation Network," accessed July 21, 2020, http://www.apsco.int/html/comp1/content/APOSOS/2019-03-01/59-261-1.shtml.

China can acquire satellite images of any place on earth within two hours.[131]

China has a long-term vision to build "a community of common destiny in outer space" and is asking countries for their cooperation.[132] Additionally, China is undertaking a project to construct a Space Information Corridor that will provide satellite-based communications, earth observation, and positioning services to the One Belt, One Road members.[133] As China moves along the path toward becoming a comprehensive space power, attention must be paid to whether the country will develop into a new hub for space cooperation and what implications it will have for national security in the world.

Chapter 4

China's Military-Civil Fusion Strategy

Iwamoto Hiroshi and Yatsuzuka Masaaki

1. Historical Development of Military-Civil Relations in China

(1) Military-Civil Relations Prior to the Era of Reform and Opening Up

Under the Xi Jinping administration, the modernization of military capabilities in China has been advanced through a policy of military-civil fusion (MCF). This MCF strategy, simply put, aims to strengthen military capabilities and promote the nation by tying together the military and socio-economy. Specifically, China utilizes the market economy principle to advance modernization of the military in a wide range of fields, including goods, technologies, industries, and human resources development. The "military" in military-civil fusion refers to the military force itself and the munitions companies in charge of the production and research of weapons and equipment, while the "civil" refers to non-military entities such as state-owned enterprises, private companies, educational institutions, and research institutes.[1] The two main means of promoting MCF are "eliminating barriers to defense conversion" [*jun zhuan min*, 军转民] and "civilian participation in the defense industries" [*min can jun*, 民参军]. "Eliminating barriers to defense conversion" refers to encouraging efficient modernization and market revitalization by outsourcing the production of military supplies to private companies and other civilian entities and transferring the outcomes of military research to civilian products. In contrast, "civilian participation in the defense industries" refers to the participation of private companies and others in the production and research of military supplies with the approval of the authorities. This section examines the development of military-civil relations in modern China in order to understand the ideas and directions underlying the MCF strategy of the Xi Jinping administration.

The Chinese Communist Party (CCP) has always emphasized military-civil relations in order to govern society. Looking at the history of China in the 20th century, the exercise of military capabilities has enabled the CCP's governance, as exemplified by the phrase "Political power grows out of the barrel of a gun," stated by Mao Zedong during an emergency meeting of the CCP Central Committee in August 1927.[2] In fact, the role of the People's Liberation Army (PLA) was essential in the process of the CCP's violent implementation of the agrarian revolution across China. As the CCP expanded the regions under its control, revolution by the CCP was made possible by their use of the military to mobilize and requisition various resources such as land, food, and human resources that existed in Chinese society. In 1942, in a meeting of top officials of the Shaan-Gan-Ning Border Region during the war against Japan, Mao Zedong presented the principle of "giving consideration to both the military and civilians" [*junmin jiangu*, 军民兼顾], which aimed to develop the economy and guarantee supply by having the military participate in production activities.[3] The history of using the military to enhance social governance and production capacity during the communist revolution has been a large factor behind the CCP's consistent emphasis on military-civil relations

even after the founding of the People's Republic of China (PRC).

Production activities by the military were continued even after the founding of the PRC in 1949. The Chinese People's Political Consultative Conference decided to permit the military to systematically participate in agricultural and industrial production to the extent that this did not interfere with its military missions.[4] In the context of the severe fiscal situation of the country's founding period, it was decided that the PLA should be responsible for some production tasks. It was permitted to participate in agriculture, livestock farming, fishing, water projects, handicrafts, construction work, industry and transportation, but it was prohibited from participating in commerce on the grounds that it would lead to corruption. In his instructions concerning the military's participation in production activities, Mao Zedong gave a positive appraisal of the military's production activities, saying that "participation by the People's Liberation Army in production is not temporary; it is based on the perspective of long-term construction."[5]

After a period of continuous warfare, including the war against Japan, the Chinese Civil War, and the Korean War, from the mid-1950s, China began to place priority on nation-building, and the CCP began to aim to balance both economic construction and national defense buildup. In his 1956 speech "On the Ten Major Relationships" in which he discussed the problems in the construction of socialism in China, Mao Zedong raised the importance of economic construction, asserting that only by further expediting the development of economic construction could China achieve further progress in its national defense buildup. Furthermore, more specifically, Mao indicated that the costs pertaining to the military, which had climbed to 30% of the state budget during the period of the First Five-Year Plan (1953–1957), should be reduced to around 20% during the period of the Second Five-Year Plan (1958–1962), in order to raise more funds which could be used to open more factories and manufacture more equipment. In response to Mao Zedong's policy, in 1957 the State Council's Second Ministry of Machine Building, which was in charge of arms production, presented a 16-character policy for national defense industries, namely, "civil-military integration [*junmin jiehe*, 军民结合], integration of peace and war [*pingzhan jiehe*, 平战结合], giving precedence to the military [*yijun weizhu*, 以军为主], and supporting the military in the civil sector [*yimin yangjun*, 以民养军]."[6]

However, due to confrontations with the two superpowers of the United States and the Soviet Union and tensions in domestic politics, the achievement of both economic construction and national defense buildup did not proceed as initially envisaged. From the mid-1960s, the "third front" [*sanxian jianshe*, 三线建设] movement progressed, and priority was given to investing economic resources into heavy industries and national defense industries.[7] In this process, the PLA became bloated, and in the early stages of the Cultural Revolution the number of military personnel reached 6.6 million, and the national defense budget climbed to 26% of the national budget.[8] Furthermore, the PLA continued its production activities in society even during the Cultural Revolution period. The revised constitution of 1975 also stipulates that "the Chinese People's Liberation Army is at all times a fighting

force, and simultaneously a working force and a production force."

(2) Military-Civil Relations in the Era of Reform and Opening Up

After the death of Mao Zedong, China under Deng Xiaoping changed direction to a reform and opening-up policy that placed more importance on economic construction than on national defense buildup, resulting in changes in military-civil relations. After the Third Plenary Session of the 11th Central Committee of the CCP, and based on his analysis of the situation that "peace and development are the main issues currently and large-scale war will not occur in the short term," Deng Xiaoping revised the relationship between economic construction and national defense buildup by stating: "It is necessary to place importance on economic construction and ensure that national defense buildup is subservient to economic construction. If this is not done, the national defense buildup will also be wasted."[9] Furthermore, Deng Xiaoping made it clear that the disproportionate focus on military construction should be rectified; for example, in January 1982, he aimed to correct course by giving instructions to revise the 16-character policy pertaining to national defense industries ("civil-military integration, integration of peace and war, giving precedence to the military, and supporting the military in the civil sector") by changing the expression "giving precedence to the military" [*yijun weizhu*, 以军为主] to "giving priority to military goods" [*junpin youxian*, 军品优先].[10]

In accordance with this policy, the trend of "eliminating barriers to defense conversion" strengthened, and excess facilities and human resources possessed by the PLA were transferred to the private sector. At the same time, while reducing military expenditure and the number of PLA personnel, China encouraged business undertakings by the PLA in order to avoid the social anxiety brought about by such "rearranging" of the military.[11] In the context of this trend, production projects undertaken by the PLA expanded its range of activities beyond traditional agriculture and infrastructure construction to include private-sector businesses such as the management of companies and hotels. As a result of this, it is reported that the percentage of the total production by national defense industry companies accounted for by civilian products, which was 8.2% in 1979, rose to 70% in 1989.[12] On the other hand, the rapid deepening of involvement in economic activities by the PLA in response to the shift to a market economy also led to widespread business-related fraud and corruption in the PLA.[13]

The Gulf War had a significant impact on China's military-civil relations. This is because the Jiang Zemin administration, in the face of public distrust of the party and the military after the Tiananmen Square Incident, was compelled to mobilize private-sector science and technology into the military in order to respond to the changing forms of warfare caused by the revolution in military affairs (RMA). In 1993, the PLA made it its military strategy to win "local wars under high-tech conditions," and consequently, in 1995, it presented the policy "strengthening the military through science and technology" [*keji qiangjun*, 科技强军], which changed its course toward "two fundamental changes" that advanced (1) a shift from quantity to quality, and (2) a shift from a

manpower-intensive approach to a science and technology-intensive approach.[14] Under this policy, the aim was to encourage collaboration between the scientific research and production systems of the military and civil sectors. Military-civil relations under Jiang Zemin, who clarified a policy of incorporating capitalists into the CCP in his theory of "the three represents," can be characterized by the concept of "locating military potential in civilian capabilities" [*yujun yumin*, 寓军于民].[15] In October 2000, the Fifth Plenary Session of the 15th Central Committee of the CCP proposed "construction of a new type of structure for science, technology and industry for national defense adapted for national defense buildup and the demands of the market economy."[16] In other words, the trend of "civilian participation in the defense industries," in which the innovations of the private sector are incorporated in munitions in order to develop military and civil dual-use technologies had emerged.

Entering the 21st century, the PLA, perceiving that the form of warfare was transitioning to "informatized warfare," was pressed to incorporate the outcomes of the development of state-of-the-art technology, including information technology, into its military technology. Against this background, the Hu Jintao administration began to newly advocate for "military-civil fusion" (MCF) at an expanded meeting of the Central Military Commission (CMC) in December 2005. Previous "civil-military integration" and "locating military potential in civilian capabilities" policies had focused on reorganizing national defense authorities and raising their technical levels. In contrast, MCF, while basically inheriting these approaches, responds to the growth of general-purpose military and civil dual-use technologies by aiming to bring private-sector capital across a broader range of fields, including the economy, science and technology, education, and human resources, into munitions.[17] In fact, the National Defense Mobilization Law promulgated in 2010 provides for support and assistance from the public sector for organizations, such as those that develop advanced military and civil dual-use technologies, and this can be seen as a legal measure to attract the private sector.

As can be understood from the above, to date the CCP has consistently and actively deployed the military in the private sector for the purpose of governance under the ideology of the "people's war." The National Defense White Paper 2019 (hereinafter referred to as "NDWP 2019") also uses the expression "China's national defense is the responsibility of all Chinese people," calling for the involvement of all citizens in national defense. On the other hand, the fact that military-civil relations changed in each era must not be overlooked. In the 1980s, as China was incorporating a market economy, the movement to "eliminate barriers to defense conversion," which shifted bloated and high-cost military functions to the private sector, moved into high gear, and in the 1990s, in response to the shift to high-tech warfare, the movement for "civilian participation in the defense industries," which encouraged the diversion of cutting-edge technologies in the private sector for military use, gained momentum. These ideas underlying the foundation of China and the trends that define military-civil relations formed in each era are regulating the direction of the MCF strategy of the Xi Jinping administration.

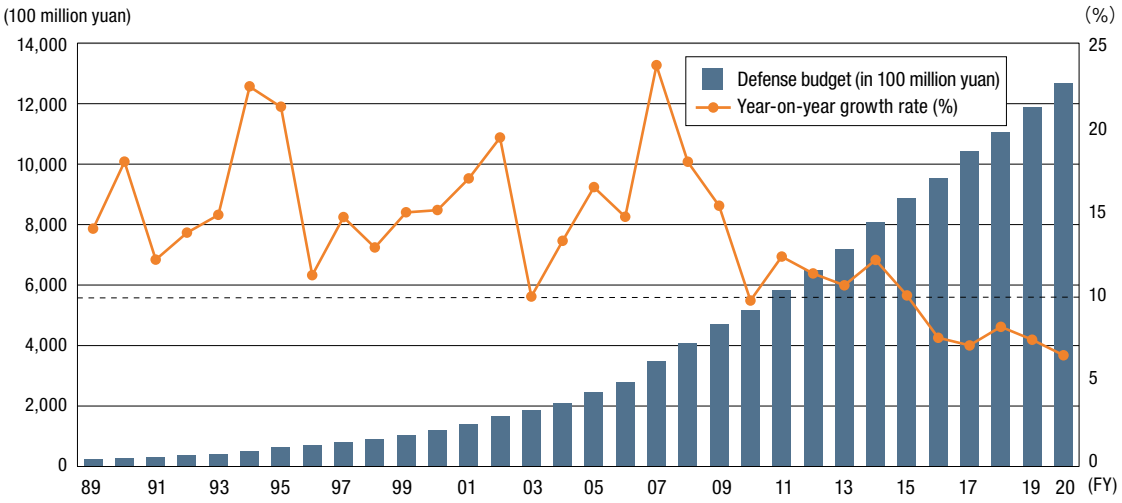
2. Military-Civil Fusion Strategy in the Xi Jinping Administration

(1) Background

The Xi Jinping administration, while inheriting the "development of a military-civil fusion approach" begun in the era of the Hu Jintao administration, aims to shift from "initial fusion" to "deep fusion."[18] After Xi Jinping became General Secretary of the CCP, he made it clear during the plenary session of the PLA delegation at the first session of the 12th National People's Congress that he would aim for "military-civil fusion-style development" and announced at the National People's Congress in March 2015 that MCF would be upgraded to a national strategy.[19] Furthermore, he has clarified his emphasis on MCF at the 19th National Congress of the CCP in October 2017, for example, by revising the Party Constitution to explicitly state "military-civilian integration strategy."

When considering the direction of MCF by the Xi Jinping administration, it is necessary to grasp the following two background facts. First is the fact that the Chinese economy has already shifted from high growth to an era of low growth. As shown in Figure 4.1, in the context of a "new normal" in which the growth rate of national defense expenditure is slowing down financially, streamlining national defense buildup projects in particular is required to achieve both economic construction and national defense buildup. The idea of MCF is to aim to improve efficiency in response to the situation in which resource constraints conflict with the demands of modernizing the military.[20] It is reported that in this context there is also a proposal that "military-civil fusion" should be added as a fiscal budget item.[21] Professor Jiang Luming of PLA National Defense University warns that "China's economic development has entered a new normal, fiscal revenue growth has entered an adjustment period, and the resource conditions that can be invested into national defense have become strained," while on the other hand, "pressure on national defense and security is constantly growing."[22] Moreover, this kind of warning is related to a sense of crisis regarding a decline in national power. According to Professor Jiang, "the rise of a great power is established on the harmonization of the economy and the military, and the decline of a great power occurs when long-term harmonization of the economy and the military cannot be achieved."[23] As the economic growth rate shows a trend of decline due to a shrinking labor force and other factors, the Chinese government is expecting to reduce the economic burden of the national defense buildup

Figure 4.1 Changes in China's Announced Defense Budget



Source: Ministry of Defense of Japan, *Defense of Japan 2020* (Tokyo: Ministry of Defense of Japan, 2020), p. 60.

by outsourcing low-efficiency and high-cost elements burdening the military to the private sector. The Chinese government has been announcing its growth targets for the economy at the National People's Congress held every year, but in 2020, it did not announce the targets on the grounds that the situation going forward is unclear due to the coronavirus disease (COVID-19) pandemic. On the other hand, the national defense budget increased 6.6% compared to 2019. For the time being, harmonization between the military and the economy is difficult, and the outlook is unclear.

Secondly, there are changes in the form of warfare.[24] NDWP 2019 states that "War is evolving in form towards informationized warfare, and intelligent warfare is on the horizon," and that in the process of the transition to intelligentized warfare, "Driven by the new round of technological and industrial revolution, the application of cutting-edge technologies such as artificial intelligence (AI), quantum information, big data, cloud computing and the Internet of Things is gathering pace in the military field." In order to apply these highly-versatile cutting-edge technologies to the military field, it will be important to build a structure of "civilian participation in the defense industries" to flexibly divert to military use the technological innovations of a broader range of the private sector, including start-up companies and research institutes that conduct research on the latest technologies.

Against this background, the United States has become increasingly concerned about China's growing presence in new domains through its policy of MCF, and confrontations between the United States and China are spilling over into a wide range of fields. President Xi Jinping has presented a goal of realizing the "Chinese Dream," namely, "the great rejuvenation of the Chinese nation," and on the military front he has proposed constructing world-class forces by the middle of this century. The announcement of these ambitious goals has prompted concerns in the United States and other countries and has led to the tightening of trade and investment restrictions against China by the United States, as discussed in the next section. The MCF strategy, which encourages a shift to indigenization of the national defense industry based around independent development of

core technologies, can be seen as a measure that aims to sustainably strengthen military capabilities even in the event of a prolonged U.S.-China confrontation. In October 2018, when friction between the two countries intensified, President Xi Jinping stated that "the foundation of the struggle of the Chinese people is regeneration by their own efforts, and the path for China to climb high in global science and technology is independent innovation," and instructed that core technologies be shifted to indigenous production.[25] This policy direction is also reflected in a range of industrial promotion policies, such as Made in China 2025 [*zhongguo zhizao2025*, 中国制造2025], which is discussed below.

(2) Military-Civil Fusion Policy System

In advancing the MCF strategy, the Chinese government presented the development of systems in three areas in its 13th Five-Year Plan (2016–2020): "management system"; "operational system"; and "policy system."[26] Of these, key areas of focus in MCF are presented in the development of the policy system. Below examines the system development situation in these three fields, beginning with the details of the policy system in order to discuss China's purpose in advancing policy related to MCF.

The industrial development policy is one policy system in the MCF strategy. The report at the 19th National Congress of the CCP held in October 2017 stated that "the modernization of our national defense and our military will be basically realized by 2035, and our people's military will have been fully built up into world-class forces by the mid-21st century," thereby setting new goals in the form of bringing forward previously-set goals. On the other hand, NDWP 2019 presents the assessment: "Greater efforts have to be invested in military modernization to meet national security

Table 4.1 Priority Areas of Science, Technology, and Industry for National Defense Indicated by the State Council

Space	● Major projects including large carrier rockets, nuclear power facilities, deep-space exploration, in-orbit servicing, and maintenance systems ● Yaogan [遥感] data policy; sharing of satellite resources and data between the military and civilian sectors ● Research on construction of launch sites and measuring systems
Cyber	● Building communications satellites and other communications infrastructure ● Improving cybersecurity as well as electromagnetic management technology and equipment ● Promoting the space-terrestrial integration information network project ● Establishing and constructing testing grounds for military electronic intelligence; researching and producing weapons and equipment and contributing them to the civil sector
Maritime	● Coordinating testing needs of military and civilian sectors and testing facilities in the ocean and accelerating construction of deep/far sea testing sites ● Improving technologies for underwater measurements, data transmission, and security; enhancing comprehensive detection capabilities in the ocean ● Promoting construction of deep-sea stations, nuclear power offshore platforms, and deep ocean monitoring and measuring equipment ● Actively developing high-performance icebreakers, polar icebreaking research vessels, polar rescue vessels, polar semi-submersible transport vessels, polar resource exploration vessels, and core parts and materials for use in polar regions; and supporting major projects in the ocean

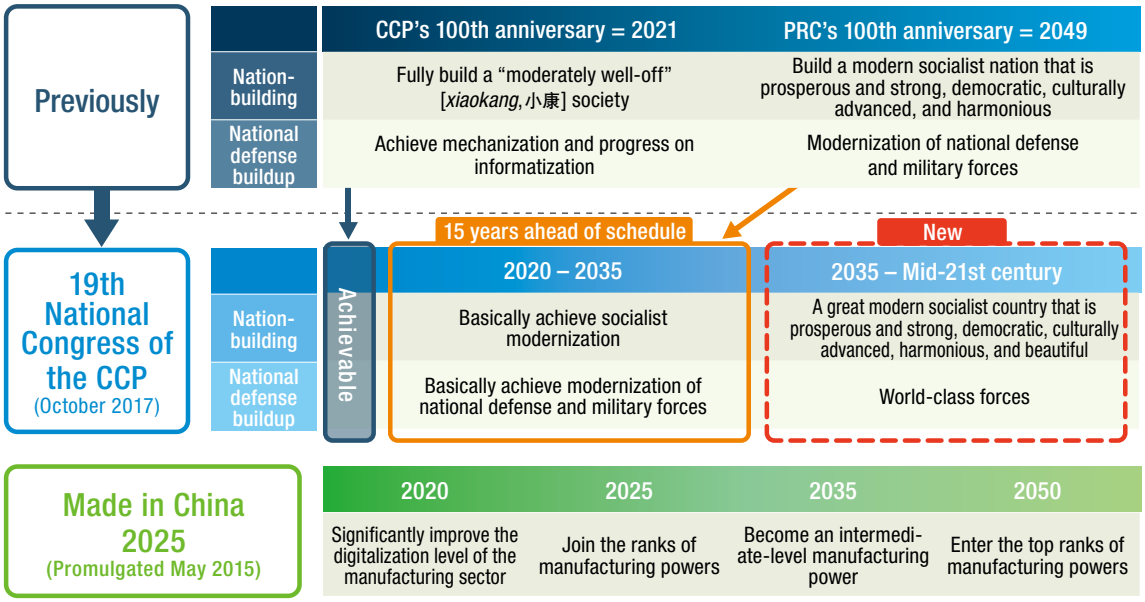
Source: Compiled by the author, based on Central People's Government of the People's Republic of China, last modified December 4, 2017, http://www.gov.cn/zhengce/content/2017-12/04/content_5244373.htm.

demands. The PLA still lags far behind the world's leading militaries." This perception of the current situation has become a major motivator for advancing MCF. In the statement on MCF of science, technology and industry for national defense released by the State Council in December 2017, technologies in the space, cyber, and maritime domains are identified as priority areas, as shown in Table 4.1.[27]

Furthermore, similar perceptions are held not only from a military perspective, but also from the wider perspective of the manufacturing sector. Made in China 2025, the platform for China to become a "manufacturing power" [*zhizao qiangguo*, 制造强国], states that China's manufacturing sector "is large but not strong" and "greatly lags in innovation, efficiency of resource utilization, industrial structure, degree of digitalization, and quality," and indicates the necessity of a change in production methods. The assessment published by the U.S.-China Economic and Security Review Commission of the United States in 2017 also states that while China is superior to the United States with regard to some of the latest technologies, such as supercomputers and commercial unmanned drones, it remains inferior to the United States in the fields of biotechnology, nanotechnology, and collaborative robots, and the science and technology fields in which China has established its superiority globally are still limited.[28]

As shown in Figure 4.2, Made in China 2025 sets the goals of turning China into a manufacturing power by 2025, reaching an intermediate level among world manufacturing powers by 2035, and consolidating its position as a manufacturing powerhouse and entering the top ranks of the world's manufacturing powers with its overall capabilities by 2049, the centennial of the founding of the PRC. This vision presents the perception that in addition to MCF, building a manufacturing

Figure 4.2 China's Goals for Becoming a Great Power



Sources: Compiled by the author, based on 人民日报 [*People's Daily*], November 18, 2012, May 20, 2015, and October 28, 2017.

Table 4.2 Ten Key Priority Industry Sectors

New information technology
High-end numerically controlled machine tools and robots
Aerospace equipment
Ocean engineering equipment and high-end vessels
High-end rail transportation equipment
Energy-saving cars and new energy cars
Electrical equipment
Farming machines
New materials
Bio-medicine and high-end medical equipment

Source: Compiled by the author, based on "国务院关于印发《中国制造2025》的通知 [Notice of the State Council on Issuing the 'Made in China 2025' Plan]," Central People's Government of the People's Republic of China website, May 19, 2015.

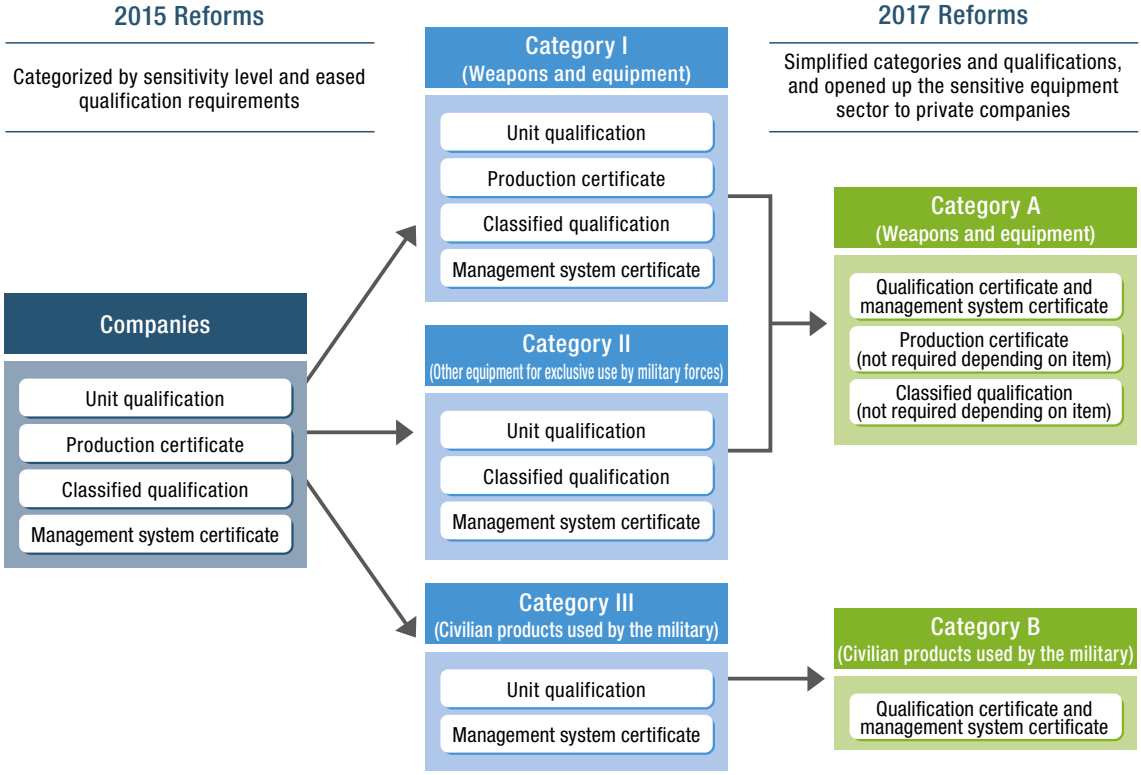
sector that has international growth potential will lead to improving the nation's overall strength, and consequently, contribute to national security. It can thus be inferred that this vision is closely related to the policy direction of MCF and to national goals. Furthermore, Made in China 2025 stipulates as its goals that 40% of "essential spare parts and key materials" will "have domestic sources" by 2020 and 70% by 2025. Professor Marukawa Tomoo at the University of Tokyo indicates the possibility that having domestic sources does not simply mean a shift to indigenous production involving foreign capital, but also includes the meaning of a shift to indigenous production by Chinese enterprises.[29] As stated above, it can be concluded that the national security perspective of aiming for the independence of the national defense industry and reducing vulnerabilities by shifting to indigenous production of core technologies is reflected in this. Note that Made in China 2025 presents the ten fields shown in Table 4.2 as strategic priorities.

In addition to industry promotion measures, encouragement of the introduction of technologies from abroad is important in the MCF strategy. Elsa B. Kania, Adjunct Senior Fellow of the Center for a New American Security, points out that the lack of talent and core technologies that China is facing is motivating Chinese enterprises to invest in foreign countries and bring in technologies and talent.[30] The Thousand Talents Plan [*qianren jihua*, 千人计划] decided by the Central Committee of the CCP in December 2008 is one of the talent acquisition policies aimed at introducing technologies. This plan is called the "overseas high-level talent introduction plan" and it aims to achieve innovation by bringing outstanding scientists and leaders back home to China, or inviting them to work in China, in state priority projects.[31] As of 2018, ten years after this Thousand Talents Plan was started, more than 6,000 people have been hired in a range of fields including AI, integrated electronics, quantum communications, integrated circuits, the biomedical field, and dual-use technologies made with advanced materials, and significantly more talent than in the initial hiring plan have moved their base to China.[32] On the other hand, the percentage of international students who reside in the United States for the long term after earning their doctorate is nearly 90% for Chinese students, whereas the average for the citizens of other countries is 70%. In this regard, the effectiveness of the talent acquisition policies employed by the Chinese government is still open to debate.[33]

Furthermore, as part of the development of systems, the removal of barriers to entry is also

being advanced in order to encourage "civilian participation in the defense industries." Firstly, the system of permits has been simplified in order to encourage "civilian participation in the defense industries." Originally, four military industry permits [*jungong sizheng*, 军工四证] were established around 2005 for private-sector entry into the munitions industry. The four military industry permits are: (1) the Equipment Manufacturing Unit Qualification, which is mandatory for manufacturing contractor organizations that directly conclude purchase contracts for weapons and equipment with the PLA; (2) the Weapons and Equipment Research and Production Certificate, which is mandatory for organizations participating in scientific research or manufacturing activities in the area of weapons and equipment; (3) the Weapons and Equipment Research and Production Unit Classified Qualification Permit, for which acquisition is mandatory for organizations participating in scientific research or manufacturing activities in the area of weapons and equipment pertaining to state secrets; and (4) the Weapons and Equipment Quality Management System Certificate, which certifies that an organization has the capacity to undertake missions related to the research, development, or manufacturing of weapons and equipment.[34] Reforms of this system were implemented in 2015 and 2017 under the Xi Jinping administration.[35] The motivation for reforming the four military industry permits was to reduce the burden of the administrative procedures for acquiring qualification certifications while

Figure 4.3 Reforms of the Four Military Industry Permits



Source: Compiled by the author, based on Kazama Takehiko, "Chugoku no Gijutsu Kakutoku Senryaku—Gunmin Yugo no Katsuyo to Kanren Seisaku (2) [China's Technology Acquisition Strategy: Use of Military-Civil Fusion and Related Policies (2)]," *CISTEC Journal*, No. 181 (May 2019), pp. 310-312.

encouraging entry into the fields of research, development, and manufacturing of sensitive weapons and equipment, which had not been permitted for private companies previously.[36] The series of simplifications of the four military industry permits can be summarized as shown in Figure 4.3. These reforms have allowed private companies to enter the field of research, development, and manufacturing of highly sensitive weapons and equipment, which had only been permitted for state-owned enterprises previously.[37] Partly due to the effect of these simplifications, as of March 2016, more than 1,000 private companies have already acquired the Weapons and Equipment Research and Production Certificate, and it is reported that this is an increase of 127% from when the 11th Five-Year Plan (2006–2010) ended.[38]

In addition, a range of subsidy systems are being put in place for private companies conducting research into military technologies. It is reported that applications for "model area construction" were made from approximately 30 regions across China by about March 2018, based on the Plan for Construction of a State Military-Civil Fusion Novel Model Area adopted in March 2018 by the Central Commission for Military-Civil Fusion Development.[39] This model area is expected to attract and grant subsidies to companies entering the munitions industry, and enable sharing of large-scale research facilities.[40]

(3) Military-Civil Fusion Management System

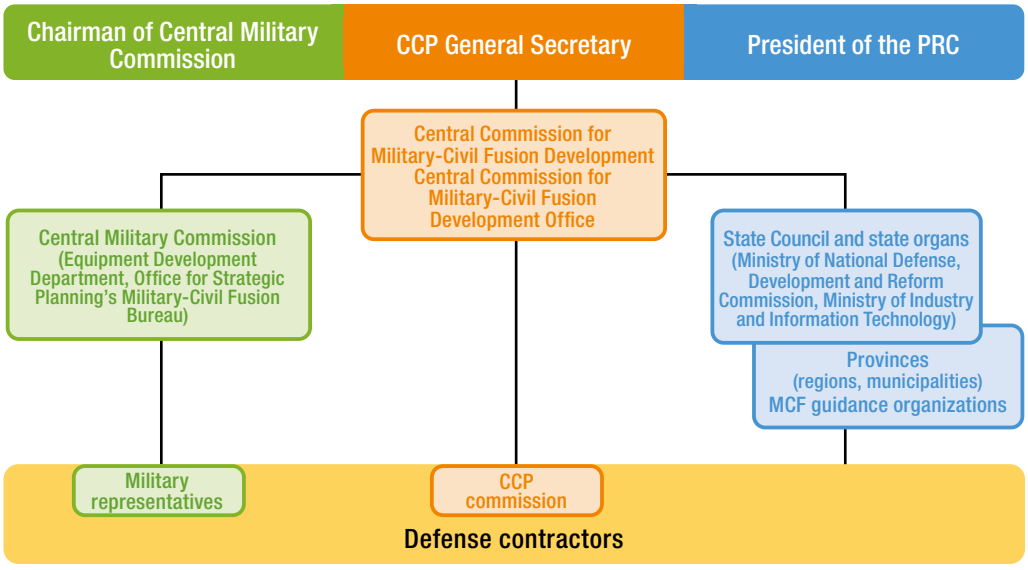
Party, military, and state organizations shown in Figure 4.4 are being developed in order to carry out measures pertaining to MCF effectively. In the party, the Central Commission for Military-Civil Fusion Development chaired by General Secretary Xi Jinping was inaugurated in January 2017. It is highly significant that General Secretary Xi himself, who is consolidating authority, is serving as chair. This commission is a party organization that decides and coordinates policies pertaining to MCF, and provides uniform guidance for the MCF strategy.[41] As a background to the founding of this commission, it has been pointed out that the lack of a coordinating organization for MCF in the era of the Hu Jintao administration meant that various policies were either not executed at the bureaucratic and local government levels, or were implemented in a fragmented way, meaning they lacked effectiveness.[42] The Department of MCF Promotion in the Ministry of Industry and Information Technology (MIIT) of the State Council is believed to have been previously responsible for the coordination operations pertaining to MCF, but the authority of the department, which is no more than an administrative division, was too limited to coordinate MCF, which has a scope that extends to the military and society.[43] In contrast, the Central Commission for Military-Civil Fusion Development

is chaired by General Secretary Xi Jinping, is comprised of a large number of relevant leaders straddling the state and military, and has quite a strong authority. For example, in addition to the CMC Vice-Chairmen, the top uniformed officer of the PLA, the inclusion among the constituent members of the chair of the National Development and Reform Commission, responsible for the economic plan in the State Council, and the Minister of Finance, who is in charge of fiscal matters, is thought to have enabled investment of flexible and large-scale state budgets into militarily important new technology development projects under long-term plans.

In the military, the Military-Civil Fusion Bureau was established in the Office for Strategic Planning of the CMC in 2016. This bureau carries out its duties together with related departments and commissions such as the National Development and Reform Commission, and is said to be the driving force behind "civilian participation in the defense industries," while the State Administration for Science, Technology and Industry for National Defense (SASTIND), discussed below, is the force behind "eliminating barriers to defense conversion."[44] Furthermore, it is thought that the organization promoting development of the latest weapons is the Science and Technology Commission in the CMC.[45] It has been pointed out that this organization was modeled after the Defense Advanced Research Projects Agency (DARPA) of the United States, and it is thought to be in charge of funds procurement, matters pertaining to resources, and the implementation of projects. In addition, military representative offices have been established at each level as "representatives" of the PLA in defense contractors and other entities, and are responsible for implementing contracts, monitoring quality control, receiving products, and even liaising with the military.[46]

SASTIND under MIIT is one of the competent institutions in the state apparatus. Furthermore, MIIT's Department of MCF Promotion is thought to carry out coordination pertaining to MCF in

Figure 4.4 Organizational Relationship Chart of MCF



Source: Compiled by the author, based on 军事大辞海（上） [*Military Dictionary (Vol. I)*] (Beijing: 长城出版社 [Chang Cheng Publication], 2000), p. 1239.

the administrative division. MIIT's website lists the duties of the Department of MCF Promotion as including promotion of the fusion and development of the military economy and the regional economies and promotion of industrialization of civil-military integration, and additionally mentions operations pertaining to disseminating military and civil dual-use technologies and establishing military and civil standards. SASTIND inside the ministry is also believed to be responsible for supervision of national defense company policy. Because the field of MCF is wide-ranging and not limited to the industrial sector, the National Development and Reform Commission is involved in a cross-sectoral manner, and each division is believed to have established its own department pertaining to MCF to implement operations within the scope of the administration under its respective jurisdiction.

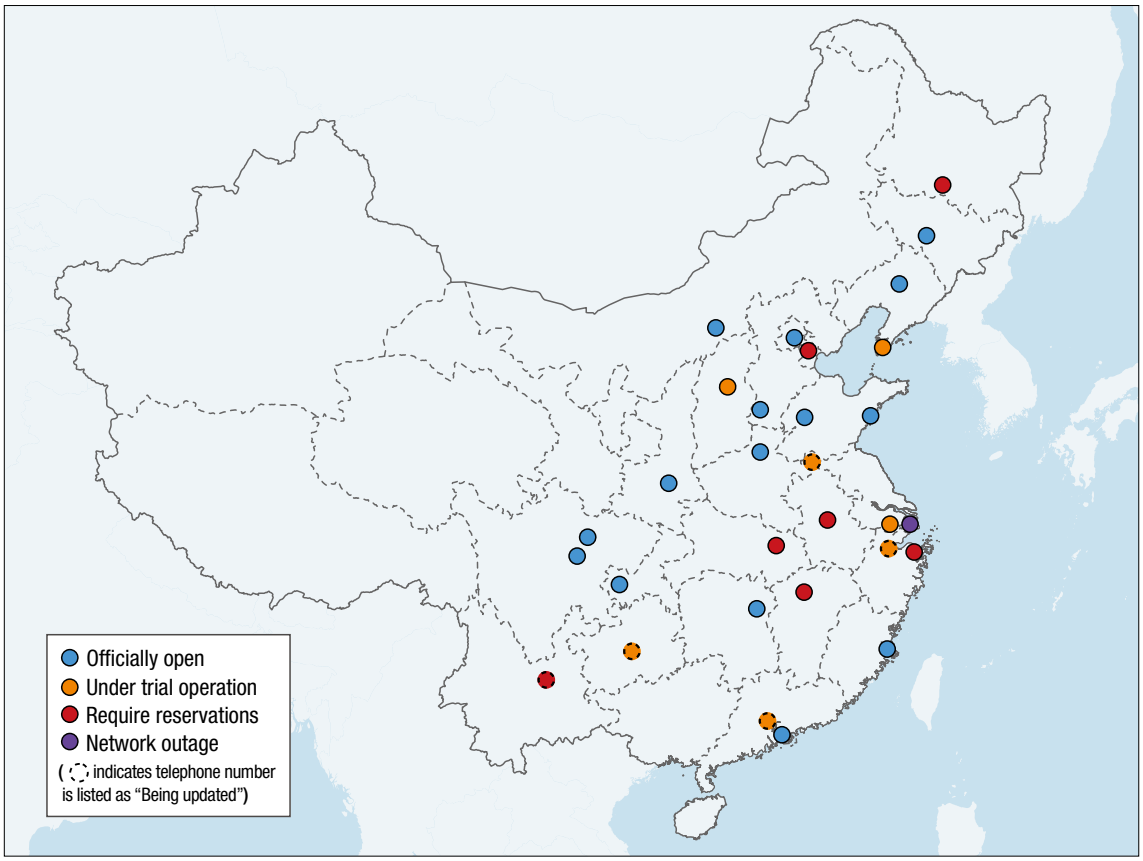
Local governments are also advancing measures to promote MCF. For example, as of 2018, it is reported that 20 provincial governments have already announced MCF development plans, and guidance organizations pertaining to MCF have been established inside 23 provincial and municipal governments.[47] Meanwhile, party committees for MCF development have been established for nearly every provincial grade and are providing guidance in each region pertaining to MCF. When COVID-19 started to spread in China, each region's Department of the People's Armed Force took the lead in responding with measures to control the pandemic. However, it has been confirmed that in addition to considering guidelines for the resumption of operations by companies involved in MCF, the MCF development committees in each region responded in diverse ways, such as by establishing central leading groups to stop the spread of the virus, engaging in donation activities in each region, and supporting other regions, indicating that they are attempting to fulfill their role as party organizations.[48]

Therefore, it is thought that the overall planning, coordination, and execution process pertaining to MCF is structured with the party's Central Commission for Military-Civil Fusion Development at the top establishing the overall plan, the Military-Civil Fusion Bureau of the CMC's Office for Strategic Planning and the Science and Technology Commission coordinating on the military side, and MIIT's Department of MCF Promotion and SASTIND coordinating on the government side. In addition, it appears that coordination institutions pertaining to MCF have been established in each local government, and they are executing the MCF policy established at the central government level. Furthermore, structures for implementing MCF measures have also been developed in the private sector by establishing "representatives" of the party and military, such as party committees and military representatives, in each company.

(4) Military-Civil Fusion Operational System

To advance MCF in a concrete manner, building an operational system that efficiently links the military and civil sectors is important. This operational system aims to establish information exchange and information sharing systems for the military and local governments by clarifying regulations and bringing transparency to the procurement process.[49] Specifically, the All-Army Weapons and

Figure 4.5 Distribution of the "Nationwide Centers" related to MCF



Source: Compiled by the author, based on All-Army Weapons and Equipment Procurement Information Network, accessed July 22, 2020, http://www.weain.mil.cn/ (figure as of March 31, 2020).

Equipment Procurement Information Network website, a platform for information on munitions industry entry for private companies, was set up by the CMC Equipment Development Department.[50] While many daily tender notices are posted on this site, as shown in Figure 4.5, the distribution of the "nationwide centers" established in each region is skewed toward urban areas and coastal regions, with few centers in the western region. Furthermore, of the 30 telephone numbers listed for inquiries from each region, 15 are "officially open," seven are "under trial operation," seven "require reservations," and one is experiencing "network outage," suggesting that these platforms are being operated while still under construction. Note that on the smartphone version of this site, "sub-centers" are also displayed in the western areas. Such discrepancies in an initiative positioned as a "national strategy" are a factor behind the lack of transparency in the measures by China.

Furthermore, until now SASTIND has been publishing a variety of "lists encouraging the diversion of military-use technologies to private sector use" and "lists recommending participation in military technologies and products by the private sector," in other words, lists for "eliminating barriers to defense conversion" and "civilian participation in the defense industries," in order to carry out matching of the military and civil sectors appropriately.[51] The lists regarding civilian

participation in the defense industries require regional subordinate organizations and others to gather information and select advanced technologies possessed by companies and entities in each region, based on the priority items. These types of measures can be positioned as a part of the policy to strengthen military capabilities while also holding down national defense expenditure by outsourcing high-cost military supplies to the private sector to produce high-quality, dual-use products at a low cost. The main fields presented in the lists of FY2018 include satellites, electromagnetic waves, surveillance, cybersecurity, cloud computing, IT, unmanned equipment, and simulators.[52] The lists for FY2019 could not be confirmed on the SASTIND website, but according to some local government websites and other sources, it seems that they list advanced materials, cutting-edge equipment, the field of electronic information, energy and power technologies, and environmental protection technologies. It can be inferred that these are the directions of military technology development on which China is placing importance. Furthermore, exhibitions of the high-tech outcomes of MCF development have been held actively in recent years by the Central Commission for Military-Civil Fusion Development and the CMC Equipment Development Department.[53]

Certain outcomes in specific projects based on the construction of these operational systems

Table 4.3 Ten Major Outcomes of MCF Identified by the Xinhua News Agency

Item	Description
Tianhe-2	Ranked the world's fastest supercomputer for six consecutive times
Laser gyro	Can be applied to the Long March launch vehicles
BeiDou	Navigation system
Gaofen-2	Earth observation satellite
Hualong-1	Nuclear reactor
Demolition equipment for civilian use and demolition integration platform	Applicable to infrastructure construction and ore mining
Unmanned aerial vehicle	Can be used for distribution in civilian sectors as well as for military purposes
Intelligent robot	Can be applied to lethal autonomous weapons systems (LAWS)
Driverless vehicle	Applicable to military vehicles
Caterpillar-tracked small unmanned platform	Firearm-mounted, night reconnaissance function

Source: Compiled by the author, based on 新华网 [*Xinhuanet*], last modified October 23, 2015, http://www.xinhuanet.com//mil/2015-10/23/c_128348509.htm.

for MCF have been confirmed. For example, Wang Changhai, the Party Committee Secretary for the Dalian Shipbuilding Industry, has revealed that a high level of MCF was achieved in building China's first indigenous aircraft carrier *Shandong*. According to him, under the MCF strategy, of the 532 companies including military engineering companies involved in the production or building of major facilities and parts, 412 were state-owned enterprises, private companies, or research institutes, which means that the MCF rate (the ratio of civil sector) reached 77%.[54] Furthermore, the Xinhua News Agency site introduces ten major outcomes of MCF in science and technology fields (Table 4.3).[55]

(5) Challenges Faced by Military-Civil Fusion

The MCF strategy of the Xi Jinping administration is facing a variety of challenges because it is in a period of transition from the elementary stage to deep fusion. For example, the PLA National Defense University's PLA NDU National Defense Economics Research Center raises the policy problems of (1) differences in perceptions in the national defense sector and other sectors, (2) the lack of uniformity in top-down structures and their subordinate collaborative structures, (3) structural problems that do not allow for appropriate supply and demand allocation in the military and civil sectors, and (4) policy problems such as inadequate policy and laws.[56]

Concerning the "unified leadership" repeatedly emphasized by President Xi Jinping, the launch of the Central Commission for Military-Civil Fusion Development and the Military-Civil Fusion Bureau are said to have largely completed the building of the structural aspects related to MCF.[57] On the other hand, however, a lack of uniformity in planning and guidance and the confusion of authority have been pointed out, which tell the story of deep-rooted problems at the operational level.[58] In fact, the lack of collaboration between military authorities and local governments is an oft-noted problem. For example, Professor Jiang Luming at the PLA National Defense University points out that the current collaboration structure of the military authorities and local governments has a clear tendency to be "fragmented," and there is a phenomenon of each acting on its own within the two systems of the military and local governments.[59] These kinds of problems are said to increase dysfunction and arrogations in MCF policy. At the regional level as well, discrepancies in the intentions of the military and regional companies caused by inadequate communication between the two parties have been pointed out, requiring further development of systems.[60]

Another problem is the lack of systematic legislation pertaining to MCF. Regarding legal norms pertaining to MCF, multiple regulations and ordinances from the CMC have already been issued, and while they are actually functioning in areas such as the market entry of military-related organizations, procurement, and equipment management, there lacks strong binding laws promulgated by the National People's Congress.[61] It has been pointed out that the vested interests of the central government, local governments, and military are a factor behind the delay in establishing such laws, and the delay in the revision of laws pertaining to classification of rights has also been

noted.

In addition, the fundamental contradiction of employing the market-economy principle in a planned economy has been pointed out. Under the current legal structure, it is legally guaranteed that defense contractors will make profits commensurate with the costs they incur, creating a structural problem of not bringing about cost reductions and efficiency improvements. It is reported that due to the closed nature of defense contractors, cost management is not thoroughly implemented, and there has been no movement toward legal revisions.[62]

In September 2018, in the legislative program of the Standing Committee of the National People's Congress, legislation pertaining to MCF was classified into a group of laws soon to be established; furthermore, at the second session of the Central Commission for Military-Civil Fusion Development in October of the same year, an opinion concerning construction of a legal framework for MCF development was adopted, and it appears that it is close to becoming law.[63] Meanwhile, the National Defense Mobilization Law, brought into force in 2010, is said to have taken nearly 30 years to be enacted.[64] President Xi Jinping is thought to be utilizing the Central Commission for Military-Civil Fusion Development, which has strong authority, to rapidly advance the establishment of laws in order to avoid this kind of situation. Whether or not a law pertaining to MCF is established quickly can be seen as an indicator of the political skills of President Xi.

3. The International Community's Reaction to the Military-Civil Fusion Strategy

(1) Concerns regarding Technology Transfer due to Military-Civil Fusion

As was already seen, China's MCF strategy is predicated on the technological innovation of private companies and the introduction of technologies from abroad. In particular, concerning the latter, China is using a variety of means to attempt to acquire advanced weapons and equipment, related technologies, and the talent of foreign countries, in order to compensate for its shortage of research talent and lags in specific core technology fields.[65]

The U.S. government has long been wary of technology leakage to China, but as stated in Chapter 2, since the inauguration of the Donald Trump administration, the United States' sense of crisis has grown and it has started taking hardline countermeasures. The United States is taking actual measures to regulate military technologies and weapons transactions with the PLA as well. For example, in September 2018, it barred the CMC Equipment Development Department and its leadership from applying for permission to export to the United States and from using the U.S. financial system on the grounds that it had violated sanctions on Russia, and in addition, added it to the specially designated list of the U.S. Department of the Treasury, which prevents it from doing business with the United States.

However, one of the difficulties in responding to China's MCF is the need to cast a net of surveillance not only over the activities of the military authorities, but also over economic and scientific exchanges in the private sector, which are difficult to understand in relation to security. In particular, many state-of-the-art technologies are dual-use technologies, and many cases in which they have circumvented conventional regulations are now being seen. For example, the report published by the Center for Advanced Defense Studies (C4ADS) in the United States in September 2019 introduces a case of technology leakage pertaining to the development of an electromagnetic catapult which would lead to a large improvement in the payload of the J-15 carrier-based aircraft in China's development of an indigenous aircraft carrier.[66] According to that report, in 2008, China South Rail Times Electric, a subsidiary company of a state-owned enterprise in the railroad car manufacturing field, obtained power semiconductor device (IGBT) technologies by acquiring beneficial ownership of Dynex Semiconductor in the United Kingdom. Subsequently, through its affiliates, Times Electric provided IGBT technical assistance in the process of researching and developing the ships and equipment of the Chinese navy, and this is reported to have contributed to the development of the railgun and electromagnetic catapult on China's aircraft carrier.

There are a variety of patterns to such cases in which overseas private-sector technologies leak into military technologies in a form that is difficult to ascertain. For example, leakages can occur via attracting the research and development facilities of foreign companies into the country, technology transfer through technical cooperation with and acquisition of said companies, information theft and technology transfer through international students and researchers, information theft through industrial spying activities conducted by intelligence agencies, and so on.[67] These kinds of inconspicuous cases of technology leakage based on MCF force Western countries to reconsider their security and economic relations with China and encourage initiatives for new trade restrictions. In fact, the Thousand Talents Plan, which is deemed to be a talent acquisition policy for technology introduction, is viewed in the United States as a threat to intellectual property and as technology infringement. In January 2020, the Chair of the Department of Chemistry and Chemical Biology at Harvard University was indicted by the U.S. Department of Justice on charges of giving a false explanation to the U.S. government regarding his participation in the Thousand Talents Plan.[68]

The National Defense Mobilization Law and the National Intelligence Law—domestic laws of China—provide the legal basis for the above transfer of military technologies from abroad to China through the private sector. The National Defense Mobilization Law provides that "all organizations and citizens have the obligation to accept the requisitioning of civil resources under the law," and foreign companies are said to be subject to this law as well.[69] The National Intelligence Law provides that "all organizations and citizens shall support and cooperate with state intelligence activities," which is a factor inviting concerns about information leakages and other problems.

(2) Strengthening of Investment Regulations in the West

Regarding trade and investment control, to date the U.S. government has implemented export controls to ensure that cutting-edge technologies such as communications equipment do not leak to hostile countries, based on the list of restricted items issued by the Department of Commerce. Conventionally, export control policies focused on individual handled commodities, end users, and end uses, and as the means of doing this, the authorities categorized the commodities into civil-use and military-use commodities before implementing end user verification. However, China's MCF strategy raised concerns among the national defense authorities of the United States that their conventional export control policy had been invalidated because the strategy made it difficult to distinguish between private and military companies.[70]

These concerns of the United States led to the National Defense Authorization Act for fiscal year 2019, which was established on August 13, 2018 to strengthen export controls and investment regulations. One of the important institutional changes contained in this Act was the strengthening of the authority of the Committee on Foreign Investment in the United States (CFIUS).[71] As a result of this Act, the scope of the transactions reviewed by CFIUS was expanded from transactions leading to control of U.S. companies by foreign companies, such as mergers, acquisitions, and takeovers, to also include investments by foreign companies in companies that handle information which could have an impact on critical infrastructure, critical technologies, or security, even if the transaction in question does not necessarily involve the acquisition of enough shares to enable control of a U.S. company. Furthermore, under the Export Control Reform Act (ECRA) established in August 2018, 14 emerging technologies and foundational technologies that could have an impact on the security of the United States were newly subjected to export restrictions. Due to this, permission became necessary also for exports and re-exports of emerging technologies from the United States to embargoed countries, domestic transfers in embargoed countries, and deemed exports (the taking out of technologies, knowledge, and software).

These measures have not only led to more cases of companies involved in illegal exporting, but have also placed more of China's MCF companies and state project companies on the Entity List under U.S. export control regulations, based on the discretionary judgment that they are "contrary to the security interests of the United States."[72] The strengthening of these export controls and trade restrictions can be seen as measures taken in response to technology transfers that were difficult to catch using conventional measures.

The positions of the European countries differ depending on their economic situation and their degree of economic dependence on China, but looking at the developments in Europe overall, concerns about the risk of technology transfers through investment and company takeovers by China are gradually getting stronger. These concerns were triggered by the case of KUKA, an industrial robot manufacturer in Germany that was acquired by China's Midea Group in August 2016.

This case not only meant that highly-versatile military and civil dual-use technologies, namely,

the robot technologies that are a priority area in Made in China 2025, were transferred to China, it also made an impression on each country regarding the growing influence of China in Europe, which increased the sense of caution in Europe about China's investments in Europe. The European Commission of the European Union (EU) published a document titled "EU-China – A strategic outlook" in March 2019, which positions China as becoming a "strategic competitor" in trade and investment relations, and proposes that more equal and mutually beneficial trade and investment relationships should be realized, pointing to the protectionist policies in Made in China 2025.[73]

Against the background of this growing sense of caution over China's economic advancement, in March 2019, the Council of the EU approved a draft regulation pertaining to the screening of foreign direct investments. With this, the EU began to implement strict screenings of inbound foreign direct investments, including of company acquisitions, from the perspectives of national security and public order. However, since 14 member countries of the EU have already introduced screening systems for foreign direct investments, screening by the EU primarily focuses on information sharing to determine the pros and cons of an investment, and the final judgment about a proposed investment is left to each EU member. Therefore, the effectiveness of the EU's screening system is considered to be limited compared to the screening system in the United States.

China's MCF strategy, combined with the rapid growth of China's military capabilities and the expansion of its military presence overseas, is raising alarm in the West. China's proposed MCF strategy, together with its ambitious industrial development policies such as Made in China 2025, have made Western countries recognize a need for countermeasures linking the economy and security, and have led them to strengthen trade and investment regulations. The setback in research, human resource, and technology exchanges brought about by the strengthening of investment regulations in Western countries may pose a major challenge to China's policy of opening up to the outside world, which was predicated on the development of economic relations with countries. Going forward, the focus will be on what impact these challenges will have on the direction of China's MCF strategy.

This page is intentionally left blank

Conclusions

Yatsuzuka Masaaki

Conclusions

As society transitions to a market economy under the reform and opening-up policy, China has given priority to promoting science and technology (S&T) that drive this transition and sought to translate S&T achievements into military capabilities. China's military capability enhancements in the new era are characterized by an emphasis on new security domains and a greater ability to mobilize resources in society based on expectations for S&T. Under the policy of "strengthening the military through S&T [*keji qiangjun*, 科技强军]," the People's Liberation Army (PLA) on the one hand has striven to improve its long-distance force projection and precision strike capabilities in the respective domains of the Army, Navy, Air Force, and Rocket Force. On the other hand, it has attached importance to new security domains, such as space, cyber, electromagnetic, and artificial intelligence (AI), as key fields for influencing the fate of future warfare. The PLA aims to "overtake [militarily developed countries] at the bend" by making concentrated investments in state-of-the-art technologies in priority military domains and deepening military-civil fusion. It hopes to achieve superiority in these fields and thereby overturn its inferiority in overall military capabilities.

The emphasis on S&T for enhancing military capabilities became more manifest in the PLA from the post-Cold War era, a time when the presence of the United States as a superpower created a relatively stable world. Stunned by the modern warfare conducted by the United States and other forces in the Gulf War, the Kosovo War, and the Iraq War, the PLA leadership attempted to adapt to new forms of warfare in the process of setting the direction for building its military force. While the rapid global rise of China's S&T in the last few years has been impressive, the incorporation of S&T achievements into the military has been a steady process lasting some 30 years. This effort enabled the PLA to cement China's status as a major military power in 2021, when the Chinese Communist Party marked the 100th anniversary of its founding. The Xi Jinping administration has set ambitious goals to further establish China as a global power by the next centenary in 2049, marking the 100th anniversary of the founding of the People's Republic of China. It aims to match the United States in overall military capabilities by, for example, turning the PLA into world-class forces and becoming a cyber power, a space power, and a manufacturing power in the respective fields covered in this report.

The chapters in this report provided analyses for understanding China's military strategy in the new era and its implications for the international security environment. While "active defense" as a military strategic concept has been consistently advocated by the PLA, its content has evolved reflecting changes in China's national power, the international environment, and industry structure, as well as advances in military technology. Mao Zedong's active defense gave weight to the tenet of "striking only after the enemy has struck," i.e., luring the enemy into one's territory and then making a counterattack. On the other hand, Deng Xiaoping and subsequent leaders gradually

stressed offensive actions of active defense. This shift was propelled by the PLA's strategic level responses to local wars, such as territorial disputes. Namely, improvements in medium- and long-range precision strike capabilities and the accelerated tempo of operations elevated the importance of preemptive attacks in warfare. Considering that such trends are forecasted to further gain traction in intelligentized warfare [*zhinenghua zhanzheng*, 智能化战争], active defense is expected to take on a more offensive nature in the military strategy in the new era. At the same time, it should be taken into account that, as it prepares for these wars, the PLA has proposed warfare methods combining a variety of domains such as "unrestricted warfare."

In the decade following the end of the Cold War, the PLA came to recognize that achieving information dominance, especially in cyberspace, was vital in modern warfare. Accordingly, the PLA has promoted its informatization and honed its cyber strategy. In particular, in order to achieve information dominance in informatized warfare, the PLA places importance on information warfare in peacetime, cyber operations for information theft, and the means of preemptive attack that use cyber in the initial stage of war. Meanwhile, further reliance on information as well as efforts to introduce foreign capital in the information sector in the transition to a market economy have created vulnerabilities in the PLA. To overcome these issues, the PLA is anticipated to press ahead with fostering independent development capabilities and training talent for establishing innovative technologies in the cyber field.

In the space domain, the PLA gives weight to securing space dominance by maintaining its use of space, denying use of space by adversaries, and providing information support from space. If space information support is stepped up, PLA's operations will become more dependent on space systems, making it further necessary to ensure mission assurance for maintaining space use. Against this backdrop, the PLA has steadily increased the number of satellites that can be used for military purposes, its space access capabilities, and its space situational awareness capabilities. It also develops capabilities for interfering with an opponent's use of space through anti-satellite (ASAT) weapons, electronic jammers, and other means. In this manner, the PLA has improved its overall capabilities for achieving space dominance.

China's military strategy for the cyber and space domains is closely tied to China's deterrence against the United States. The PLA aspires to ultimately match the United States in overall military capabilities. Until then, as is stated in its military strategy, the PLA will likely boost strategic weapons and assets in new security domains to achieve partial superiority in order to secure deterrence. As part of this, the PLA will build up its interference and strike capabilities to prevent the United States' military use of both the cyber and space domains. Deterrence against the United States is very much reflected in the PLA's persistent development of ASAT weapons and an "assassin's mace" in the cyber domain. The PLA is expected to continue to augment such assets to heighten the cost the United States has to bear in intervening in local wars.

The Government of China, which prioritizes the role of S&T in the military, has established

the "military-civil fusion strategy" as a national strategy. Under this strategy, the government makes concentrated investments in S&T in new security domains, facilitates military use of advanced technologies, and promotes indigenization of core technologies. The Xi Jinping administration established the Central Commission for Military-Civil Fusion Development, a CCP organ that has been given powerful authority. Under the commission, the administration aims to build a management system through which organizations of the state, military, and society cooperate with each other for executing military-civil fusion policies. In addition, a review of the policy system has been under way, including reform of the system of four military industry permits, in order to encourage a broader range of private companies to enter the arms industry. These measures have already produced certain outcomes including in weapons development. Military-civil fusion efforts place particular emphasis on the cyber, space, and maritime domains, and it cannot be overlooked that emerging companies cooperating with the government and the military in these areas are rapidly improving their technological capabilities.

However, China's military strategy itself entails a certain type of dilemma. The PLA's informatization of the military system and increased reliance on space assets in military operations have created vulnerabilities that accrue from attacks on these systems. Furthermore, the PLA fears that such vulnerabilities will have fatal consequences because of partial reliance on U.S. and other foreign companies for core technologies in relevant fields. These fears have factored into an ambitious quest for indigenization. China has made a rapid rise in S&T, but it is still in the developing stage. Especially with regard to talent and specific core technologies, it is essential that China continues to make strides through exchanges with Western countries. In other words, China is caught in a dilemma between rapid indigenization for eliminating security vulnerabilities and its opening-up policy needed for the development of the country. Moreover, as elaborated below, China's increasingly offensive military strategy has sparked concerns among neighboring and Western countries and appears to have raised the costs of achieving China's political goals.

Then, how will China's military strategy in the new era affect international affairs and Japan's security environment? First, it may give China a greater voice in creating international norms in new security domains. China participates actively in meetings about international rules in space, cyber, and other domains. Chinese efforts have the potential to drive forward the formation of international norms, as China acts not alone but in concert with Russia and emerging countries in international organizations such as the United Nations. However, as seen, the international norms that China aims to establish involve issues that conflict with Japanese and Western views. While the formation of stable international norms in new security domains will contribute to the stabilization of the international community, if unilateral military activities continue without consensus they may lead to the disruption of international order.

Secondly, the enhancement of China's military capabilities in new security domains has fueled international competition over core technologies and technological infrastructure, along with

strengthening trade and investment regulations in various countries. In response, China aims to independently develop core technologies for overcoming its security vulnerabilities. Toward this goal, China promotes military-civil fusion at home, while endeavoring to introduce foreign technologies through Chinese firms' active investments and technological exchanges. These two efforts have raised security concerns among the international community, especially the West, which have led to the strengthening of Western trade and investment regulations and, at the United States' initiative, removal of Chinese information technology equipment from the international market. If China's military-civil fusion proceeds without transparency, it could further precipitate the demand for security-oriented policy measures for private-sector trade and technological exchanges with China.

Thirdly, China's moves to use advanced technologies for military purposes have given rise to a new security situation in neighboring countries including Japan. The PLA has expanded its operational domains in parallel with the rise of its military capability, and is reinforcing the offensive element of active defense. As it prepares for intelligentized warfare in this context, the PLA will likely test operate new technologies. In May 2017, a small Chinese drone flew over Japanese territorial waters around the Senkaku Islands. In April 2018, a Chinese aircraft that appears to be a reconnaissance drone flew in Japan's air defense identification zone on the north side of the Senkaku Islands. These new incidents utilizing drones occurred in Japan's surrounding waters and airspace. Provocative actions by drones not only place a burden on the receiving end but can also cause misunderstanding and unforeseen situations. If such drones are intelligentized through the use of AI and begin to be operated in waters and airspace in Japan's periphery, it will make on-site responses more complicated. Japan will be compelled to respond to such new situations.

Even more importantly, if China pursues a military strategy in the new era that places considerable weight on a strategy against the United States, an international order defined by U.S.-China rivalry will likely remain in the medium- to long-term. Toward its major goal of forming world-class forces commensurate with the U.S. forces in the next 30 years, the PLA is working to strengthen military capabilities with an eye on the long-term U.S.-China rivalry, as can be observed from the PLA's moves to indigenize military technologies. Fulfilling the "Chinese Dream" of "the great rejuvenation of the Chinese nation" seems to include resolving the disputes with neighboring countries in a manner consistent with China's wishes. It is projected that the enhancement of the PLA's military capabilities, which are becoming more offensive to achieve such goals, will lead to raising the United States' cost of intervening in local wars and will have significant implications for the security of the East Asian region, including the U.S. ally, Japan.

In light of the above, it is important for Japan to enhance its own defense posture while continuing to deepen relations with the United States in order to improve the deterrence and response capabilities of the Japan-U.S. alliance. Looking ahead to the medium- and long-term trends of military technology, Japan needs to enhance its defense posture upon holding strategic discussions for acquiring superiority in new security domains, such as space, cyber, electromagnetic, and advanced

technologies including AI. Japan's own efforts in these areas, needless to say, will contribute to improving the deterrence and response capabilities of the Japan-U.S. alliance. At the same time, Japan should seek to maintain and strengthen a stable international security environment by having strategic dialogues with China through bilateral and multilateral frameworks.

Introduction

1 中国国防报 [*China National Defense Daily*], October 19, 2017.

2 解放军报 [*PLA Daily*], May 3, 2018.

3 解放军报 [*PLA Daily*], November 6, 2018.

4 国务院新闻办公室 [The State Council Information Office of the People's Republic of China], last modified July 24, 2019, http://www.scio.gov.cn/xwfbh/xwbfbh/wqfbh/39595/41105/zy41109/Document/1660290/1660290.htm.

5 中共中央文献研究室 [CCP Central Literature Research Office], ed., 习近平关于科技创新论述摘编 [*Excerpts of Xi Jinping's Remarks on Scientific and Technology Innovation*] (Beijing: 中央文献出版社 [Central Party Literature Press], 2016), p. 25, 28.

Chapter 1

1 The time period listed for Mao Zedong corresponds to the period from the establishment of the Chinese Communist Party (CCP) Army to Mao's death; for Deng Xiaoping, the period beginning from the year of Mao's death for convenience sake; and for other leaders, the years they were Chairman of the CCP Central Military Commission (CMC).

2 M. Taylor Fravel, *Active Defense: China's Military Strategy since 1949* (Princeton: Princeton University Press, 2019), p. 30.

3 寿晓松 [Shou Xiaosong], ed., 邓小平军事思想新论 [*New Theory of Deng Xiaoping Military Thought*] (Beijing: 军事科学出版社 [Military Science Publishing House], 2007), p. 170.

4 The military force under the guidance of the CCP (CCP Army) was officially named the Chinese People's Liberation Army (PLA) by the PLA Declaration of October 10, 1947. To avoid complexity, this chapter uses the term "CCP Army" to refer to the military from the establishment of the Chinese Red Army to October 10, 1947 and the term "PLA" to refer to the military from this date onwards.

5 Murai Tomohide and Momma Rira, eds., *Senryakuron Taikei 7 Mo Takuto* [*Outline of Strategic Theories 7: Mao Zedong*] (Tokyo: Fuyoshobo, 2004), p. 53.

6 李德义 [Li Deyi], 当代军事理论与实践的思考 [*Contemporary Military Theory and Practical Thinking*] (Beijing: 军事科学出版社 [Military Science Publishing House], 2012), pp. 160-161.

7 毛泽东文集 第6卷 [*Collected Works of Mao Zedong, Vol. VI*] (Beijing: 人民出版社 [People's Publishing House], 1999), p. 392.

8 建国以来毛泽东军事文稿 中卷 [*Mao Zedong's Military Manuscripts since the Founding of the PRC, Vol. II*] (Beijing: 军事科学出版社 [Military Science Publishing House] and 中央文献出版社 [Central Party Literature Press], 2010), pp. 268-269.

9 Li, *Contemporary Military Theory and Practical Thinking*, p. 161.

10 Ibid.

11 邓小平军事文集 第3卷 [*Collection of Deng Xiaoping's Military Works, Vol. III*] (Beijing: 军事科学出版社 [Military Science Publishing House] and 中央文献出版社 [Central Party Literature Press], 2004), p. 273.

12 Saito Makoto, "Chugoku Sekkyoku Bogyo Gunji Senryaku no Hensen [Transitions in China's Active Defense Military Strategy]," *NIDS Journal of Defense and Security*, Vol. 13, No. 3 (2011), p. 33.

13 臧跃军 [Zang Yuejun], "邓小平新时期军队建设思想概述 [Outline of Deng Xiaoping's Thought on Army Building in the New Period]," 新时期国防和军队建设研究 [*Study of Defense and Army Building in the New Period*] (Beijing: 军事科学出版社 [Military Science Publishing House], 1994), pp. 7-8.

14 Andrew J. Nathan and Andrew Scobell, *China's Search for Security* (New York: Columbia University Press, 2012), p. 281.

15 刘继贤 [Liu Jixian], 国防与军队建设 [*Defense and Army Building*] (Beijing: 中国大百科全书出版社 [Encyclopedia of China Publishing House], 2011), p. 49.

16 人民日报 [*People's Daily*], November 24, 1984.

17 张玉良 [Zhang Yuliang], ed., 战役学 [*The Science of Campaigns*] (Beijing: 国防大学出版社 [NDU Press], 2006), p. 4.

18 Saito, "Chugoku Sekkyoku Bogyo Gunji Senryaku no Hensen," pp. 33-34.

19 Nathan and Scobell, *China's Search for Security*, p. 281.

20 *Collection of Deng Xiaoping's Military Works, Vol. III*, p. 177.

21 蒋顺学 [Jiang Shunxue], "新时期国防建设军队建设的理论指南 [Theoretical Guide on Defense and Army Building in the New Period]," 邓小平新时期国防建设军队建设理论研究 [*Deng Xiaoping's Theoretical Study of Defense and Army Building in the New Period*] (Beijing: 军事科学出版社 [Military Science Publishing House], 1992), p. 28.

22 解放军报 [*PLA Daily*], December 12, 1995.

23 光明日报 [*Guangming Daily*], July 12, 2017.

24 Takeda Junichi, *Jinmin Kaihogun* [*People's Liberation Army*] (Tokyo: Business-sha, 2008), p. 52.

25 解放军报 [*PLA Daily*], April 27, 1995.

26 Hiramatsu Shigeo, *Ko Takumin to Chugokugun* [*Jiang Zemin and the Chinese Military*] (Tokyo: Keiso Shobo, 1999), pp. 35-37.

27 王学东 [Wang Xuedong], 傅全有传　下册 [*Fu Quanyou's Biography, Vol. II*] (Beijing: 解放军出版社 [People's Liberation Army Publishing House], 2015), pp. 413-414.

28 Asano Ryo, "Gunji Dokutorin no Henyo to Tenkai [Transformation and Development of the Military Doctrine]," *Chugoku wo meguru Anzenhosho* [*China's Security*] (Kyoto: Minerva Shobo, 2007), pp. 260-271.

29 胡锦涛文选　第2卷 [*Selected Works of Hu Jintao, Vol. II*] (Beijing: 人民出版社 [People's Publishing House], 2016), pp. 600-601.

30 蔡和顺 [Cai Heshun], "从中共军事战略思维演变论其陆军未来发展 [The Future Development of the Army Discussed Based on Changes in the Military Strategic Thinking of the Chinese Communist Party]," 国防大学陆军指挥参谋学院学术检讨会论文集104年度 [*Collection of Academic Papers of the 104th School Year of the Army Command and Staff College, National Defense University*] (Taoyuan: Army Command and Staff College, National Defense University, 2015), pp. 3-4.

31 李亞明、陈泰吾 [Li Yaming and Chen Taiwu], 中共军事改革的深层结构 [*The Deep Structure of the Military Reforms of the Chinese Communist Party*] (Taipei: Political Warfare College, National Defense University, 2012), p. 107.

32 Asano, "Gunji Dokutorin no Henyo to Tenkai," p. 264.

33 胡锦涛文选　第3卷 [*Selected Works of Hu Jintao, Vol. III*] (Beijing: 人民出版社 [People's Publishing House], 2016), pp. 40-41.

34 十八大以来重要文献选编(上) [*Selected Important Documents since the 18th Party Congress, Vol. I*] (Beijing: 中央文献出版社 [Central Party Literature Press], 2014), p. 33.

35 马平 [Ma Ping], ed., 连合作战研究 [*Joint Operations Research*] (Beijing: 国防大学出版社 [NDU Press], 2013), p. 242.

36 肖天亮 [Xiao Tianliang], ed., 战略学 [*Science of Military Strategy*] (Beijing: 国防大学出版社 [NDU Press], 2015), pp. 164-166.

37 Ibid., pp. 166-169.

38 军事科学院军事战略研究部 [Department of War Theory and Strategic Research, PLA Academy of Military Science], ed., 战略学 [*The Science of Military Strategy*] (Beijing: 军事科学出版社 [Military Science Publishing House], 2013), pp. 91-92.

39 中国人民解放军军语 [*Glossary of the Chinese People's Liberation Army*] (Beijing: 军事科学出版社 [Military Science

Publishing House], 2011), p. 48.

40 Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare* (Santa Monica: RAND Corporation, 2018), pp. 10-11.

41 伍仁和 [Wu Renhe], 信息化战争论 [*Theory of Informatized Warfare*] (Beijing: 军事科学出版社 [Military Science Publishing House], 2004), p. 128.

42 Ibid., p. 86.

43 Ibid., p. 126.

44 Ibid., pp. 142-144.

45 十九大以来重要文献选编(上) [*Selected Important Documents since the 19th Party Congress, Vol. I*] (Beijing: 中央文献出版社 [Central Party Literature Press], 2019), p. 38.

46 解放军报 [*PLA Daily*], November 6, 2018.

47 庞宏亮 [Pang Hongliang], 21世纪战争演变与构想—智能化战争 [*Changes and Concept of 21st Century Warfare: Intelligentized Warfare*] (Shanghai: 上海社会科学院出版社 [Shanghai Academy of Social Sciences Press], 2018), p. 28.

48 戴凤秀 [Dai Fengxiu], ed., 信息化国防動员概论 [*Introduction to Informatized Defense Mobilization*] (Beijing: 军事科学出版社 [Military Science Publishing House], 2004), p. 43.

49 *Selected Important Documents since the 19th Party Congress, Vol. I*, pp. 37-38.

50 姜铁军 [Jiang Tiejun], ed., 党的国防和军队改革思想研究 [*Study of the Party's Thought on National Defense and Army Reform*] (Beijing: 军事科学出版社 [Military Science Publishing House], 2015), p. 184.

51 杨益、任辉启 [Yang Yi and Ren Huiqi], "智能化战争条件下国防工程建设构想 [Conception of National Defense Engineering Construction under the Condition of Intelligentized Warfare]," 防护工程 [*Defense Engineering*], Vol. 40, No. 6 (2018), pp. 66-67.

52 王鹏 [Wang Peng], "把握智能化战争特点规律 [Understanding the Principles of the Characteristics of Intelligentized Warfare]," 国防科技 [*National Defense Technology*], Vol. 40, No. 1 (2019), pp. 1-2.

53 解放军报 [*PLA Daily*], January 14, 2020.

54 解放军报 [*PLA Daily*], April 30, 2019.

55 新华网 [*Xinhuanet*], June 10, 2017.

56 解放军报 [*PLA Daily*], December 5, 2017.

57 人民日报 [*People's Daily*], April 16, 2014.

58 乔良、王湘穗 [Qiao Liang and Wang Xiangsui], 超限战 [*Unrestricted Warfare*] (Beijing: 解放军文艺出版社 [PLA Literature and Arts Publishing House], 1999), p. 6.

59 乔良、王湘穗 [Qiao Liang and Wang Xiangsui], 超限战与反超限战 [*Unrestricted Warfare and Anti-Unrestricted Warfare*] (Wuhan: 长江出版传媒 [Changjiang Publishing & Media] and 长江文艺出版社 [Changjiang Literature and Arts Publishing House], 2016), p. 174.

60 Qiao and Wang, *Unrestricted Warfare*, p. 54.

Chapter 2

1 For example, 解放军报 [*PLA Daily*], November 7, 1995.

2 解放军报 [*PLA Daily*], August 6, 1993.

3 江泽民文选　第3卷 [*Selected Works of Jiang Zemin, Vol. III*] (Beijing: 人民出版社 [People's Publishing House], 2006), p. 584.

4 丁宝文 [Ding Baowen] et al., 新时期党的军事指导理论研究 [*Theoretical Study of the Party's Military Guidance in the New Period*] (Beijing: 国防大学出版社 [NDU Press], 2013), pp. 246-257.

5 M. Taylor Fravel, *Active Defense: China's Military Strategy since 1949* (Princeton: Princeton University Press, 2019), pp. 218-219.

6 Ding et al., *Theoretical Study of the Party's Military Guidance in the New Period*, pp. 98-100.

7 中华人民共和国驻美利坚合众国大使馆 [Embassy of the People's Republic of China in the United States of America], last modified June 27, 2006, http://www.china-embassy.org/chn/xw/t260256.htm.

8 解放军报 [*PLA Daily*], October 9, 2002.

9 For example, 肖天亮 [Xiao Tianliang], ed., 战略学 [*Science of Military Strategy*] (Beijing: 国防大学出版社 [NDU Press], 2015), pp. 143-144; 中国军网 [*China Military Net*], last modified August 22, 2018, http://www.81.cn/jsjz/2018-08/22/content_9260460.htm.

10 Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Santa Barbara: Praeger, 2017), pp. 15-16.

11 For a detailed analysis of the structure and missions of the SSF, see: John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era* (Washington D.C.: National Defense University Press, 2018), pp. 1-68; Elsa B. Kania and John Costello, "Seizing the Commanding Heights: The PLA Strategic Support Force in Chinese Military Power," *Journal of Strategic Studies*, published electronically (May 12, 2020). This chapter draws heavily on these studies.

12 解放军报 [*PLA Daily*], November 2, 2015, quoted in Kania and Costello, "Seizing the Commanding Heights," p. 4.

13 人民网 [*People's Daily Online*], last modified January 2, 2016, http://military.people.com.cn/n1/2016/0102/c1011-28004573.html.

14 Costello and McReynolds, *China's Strategic Support Force*, p. 36.

15 Kevin L. Pollpeter et al., *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations* (Santa Monica: RAND Corporation, 2017), pp. 21-22.

16 According to the PLA's glossary of military terms, "services" and "forces, troops, or unit" are differentiated. "Services" is defined as basic categories into which military components are classified based on their key operational domains and main means of warfighting, while on the other hand, "forces, troops, or unit" is defined as: (1) a group responsible for operations and assurance missions or a larger unit; and (2) a part of the armed forces, such as the Beijing garrison forces, artillery, and Air Force unit. 中国人民解放军军语 [*Glossary of the Chinese People's Liberation Army*] (Beijing: 军事科学出版社 [Military Science Publishing House], 2011), p. 332.

17 Costello and McReynolds, *China's Strategic Support Force*, pp. 11-12.

18 Mark A. Stokes et al., *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, Project 2049, 2011.

19 Costello and McReynolds, *China's Strategic Support Force*, p. 13.

20 叶征 [Ye Zheng], 信息作战学教程 [*Lectures on the Science of Information Operations*] (Beijing: 军事科学出版社 [Military Science Publishing House], 2013), pp. 132-135.

21 Costello and McReynolds, *China's Strategic Support Force*, p. 31.

22 解放军报 [*PLA Daily*], July 1, 2003; 林颖佑 [Lin Ying-yu], "中国近期网路作为探讨 [Discussion on Recent China Cyber Operations]," 台湾国际研究季刊 [*Taiwan International Studies Quarterly*], Vol. 12, No. 3 (2016), p. 59.

23 Ye, *Lectures on the Science of Information Operations*, p. 29.

24 *Glossary of the Chinese People's Liberation Army*, p. 259.

25 Ye, *Lectures on the Science of Information Operations*, p. 3.

26 Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare* (Santa Monica: RAND Corporation, 2018), pp. 34-35, 41.

27 Costello and McReynolds, *China's Strategic Support Force*, p. 17.

28 Pollpeter et al., *The Creation of the PLA Strategic Support Force*, p. 23.

29 国防部 [Ministry of National Defense of the People's Republic of China], last modified July 12, 2017, http://www.mod.gov.cn/power/2017-07/12/content_4785370.htm.

30 See Kawaguchi Takahisa, "Kokka ni yoru Saibaa Kogeki kara no Sekyuriti [Security against Cyber Attacks from States]," *Synodos*, March 18, 2020.

31 FireEye, "Double Dragon: APT41, a Dual Espionage and Cyber Crime Operation," 2019. According to FireEye, hacker groups based in China are APT41 along with APT1, 3, 10, 12, 16, 17, 18, 19, 30, and 40.

32 Xiao, *Science of Military Strategy*, pp. 147-149.

33 Ibid., p. 145.

34 军事科学院军事战略研究部 [Department of War Theory and Strategic Research, PLA Academy of Military Science], ed., 战略学 [*The Science of Military Strategy*] (Beijing: 军事科学出版社 [Military Science Publishing House], 2013), pp. 129-131.

35 Bryan Krekel et al., *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, March 7, 2012, p. 41.

36 Simone Dossi, "On the Asymmetric Advantages of Cyberwarfare," *Journal of Strategic Studies*, Vol. 43, No. 2 (2020), p. 14.

37 Kevin Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," in *China and Cybersecurity* (New York: Oxford University Press), 2015, pp. 141-142.

38 PLA Academy of Military Science, *The Science of Military Strategy*, p. 189.

39 Ibid., pp. 122-133.

40 王文荣 [Wang Wenrong], ed., 战略学 [*Science of Military Strategy*] (Beijing: 国防大学出版社 [NDU Press], 2011), p. 252.

41 PLA Academy of Military Science, *The Science of Military Strategy*, p. 191.

42 Cheng, *Cyber Dragon*, p. 151.

43 张仕波 [Zhang Shibo], 战争新高地 [*New Highland of War*] (Beijing: 国防大学出版社 [NDU Press], 2016), pp. 67, 84-85.

44 PLA Academy of Military Science, *The Science of Military Strategy*, pp. 190-191.

45 Joe McReynolds and Peter Mattis, "Electronic Warfare and the Renaissance of Chinese Information Operation," in *China's Evolving Military Strategy* (Washington D.C.: The Jamestown Foundation, 2017), pp. 183-184.

46 The 2015 edition of *Science of Military Strategy* expresses wariness over the circulation of criticisms of the administration on social media and other platforms.

47 PLA Academy of Military Science, *The Science of Military Strategy*, p. 124.

48 战晓苏 [Zhan Xiaosu], "加强网络国防建设战略运筹需要强化的六种意识 [On the Six Elements of Awareness that Should be Strengthened in Order to Reinforce the Strategic Planning for Cyber National Defense Construction]," 国防科技 [*Guofang Keji*], Vol. 34, No. 6 (2013), p. 71; Dossi, "On the Asymmetric Advantages of Cyberwarfare," p. 16.

49 Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," pp. 152-153.

50 翁健 [Weng Jian] et al., "网络空间安全人材培养探讨 [Discussion on the Cultivation of Cyber Security Talents]," 网络与信息安全学报 [*Chinese Journal of Network and Information Security*], Vol. 5, No. 3 (2019), p. 45.

51 李明海 [Li Minghai], "网络信息体系军民融合战略的思考 [Thoughts on the Military-Civil Fusion Strategy of the Network Information System]," 网络传播 [*Internet Communication*] (August 2018), p. 81; 戴清民 [Dai Qingmin], 求道一无形之境 [*Seeking a Path at an Invisible Border*] (Beijing: 解放军出版社 [People's Liberation Army Publishing House], 2009), pp. 276-279.

52 中国电子信息产业发展研究院 [China Center for Information Industry Development], ed., 2017-2018年中国网络安

全发展一蓝皮书 [*Blue Book of China's Cyber Security Development 2017–2018*] (Beijing: 人民出版社 [People's Publishing House], 2018), p. 38.

53 《张万年传》写作组 ["Biography of Zhang Wannian" Writing Group], ed., 张万年传 下 [*Biography of Zhang Wannian, Vol. II*] (Beijing: 解放军出版社 [People's Liberation Army Publishing House], 2011), pp. 164-174.

54 Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," p. 149.

55 中共中央网络安全和信息化委员会办公室 [Office of the CCP Central Cyberspace Affairs Commission], last modified April 25, 2016, http://www.cac.gov.cn/2016-04/25/c_1118731366.htm.

56 戴清民 [Dai Qingmin], "论军队信息化建设与时信息战建设 [Informatization Buildup in the Military Forces and the Development of Information Warfare in Line with the Times]," 论中国军事变革 [*On China's Military Reform*] (Beijing: 新华出版社 (Xinhua Publishing House), 2003), p. 77.

57 中国国防科技信息中心 [China Defense Science and Technology Information Center], 国防科技发展报告 总合卷 [*National Defense Science and Technology Development Report, Comprehensive Volume*] (Beijing: 国防工业出版社 [National Defense Industry Press], 2017), p. 119.

58 中共中央网络安全和信息化委员会办公室 [Office of the CCP Central Cyberspace Affairs Commission], last modified November 6, 2018, http://www.cac.gov.cn/2018-11/06/c_1123672716.htm.

59 Dossi, "On the Asymmetric Advantages of Cyberwarfare," pp. 17-18.

60 钱学森智库 [Qian Xuesen Think Tank] et al., eds., 2017 网信军民融合发展报告 [*2017 Report on Military-Civil Fusion Development in Cyberspace*] (Beijing: 北京理工大学出版社 [Beijing Institute of Technology Press], 2018), p. 52.

61 解放军报 [*PLA Daily*], December 10, 2002; 解放军报 [*PLA Daily*], February 13, 2007.

62 翟贤军 [Zai Xianjun] et al., 网络空间安全战略问题研究 [*Study of the Issue of Cyberspace Security Strategy*] (Beijing: 人民出版社 [People's Publishing House], 2018), p. 164.

63 China Center for Information Industry Development, *Blue Book of China's Cyber Security Development 2017–2018*, p. 190.

64 Zai et al., *Study of the Issue of Cyberspace Security Strategy*, p. 164; 叶征 [Ye Zheng], "我国网络空间的主要威吓和基本对策 [Main Threats and Basic Countermeasures in China's Cyberspace]," 信息安全 [*Information Security*], November 2015, p. 32.

65 PLA Academy of Military Science, *The Science of Military Strategy*, p. 195.

66 冯亮、朱林 [Feng Liang and Zhu Lin], 中国信息化军民融合发展 [*Military-Civil Fusion Development related to China's Informatization*] (Beijing: 社会科学文献出版社 [Social Sciences Academic Press], 2014), p. 14.

67 Ibid., p. 66; 于川信 [Yu Chuanxin], ed., 军民融合战略发展论 [*Military-Civil Fusion Strategy Development Theory*] (Beijing: 军事科学出版社 [Military Science Publishing House], 2014), p. 300.

68 姜鲁鸣 [Jiang Luming] et al., 军民融合发展战略探论 [*On the Military-Civil Fusion Development Strategy*] (Beijing: 人民出版社 [People's Publishing House], 2017), pp. 47-48.

69 国家互联信息办公室 [Cyberspace Administration of China], "国家网络空间安全战略 [National Cyberspace Security Strategy]," December 27, 2016.

70 外交部、国家互联信息办公室 [Ministry of Foreign Affairs and Cyberspace Administration of China of the People's Republic of China], "International Strategy of Cooperation on Cyberspace," March 1, 2017.

71 Tsuchiya Motohiro, *Saibaa Sekyuriti to Kokusai Seiji* [*Cybersecurity and International Relations*] (Tokyo: Chikura Publishing, 2015), pp. 157-158.

72 Harada Yu, "Fukuzatsuka suru Saibaa Kihan Purosesu no Doko [Developments in the Increasingly Complex Cyber Norms Processes]," *NIDS Commentary*, No. 118 (June 2, 2020).

73 中华人民共和国中央人民政府 [Central People's Government of the People's Republic of China], last modified January 11, 2018, http://www.gov.cn/xinwen/2018-01/11/content_5255443.htm.

74 中国电子网 [*21ic China Electronics Network*], last modified March 30, 2020, https://www.21ic.com/article/701570.

html.

75 *Financial Times*, March 28, 2020.

76 Zai et al., *Study of the Issue of Cyberspace Security Strategy*, p. 153.

77 Danielle Cave et al., "Mapping China's Tech Giants," Australian Strategic Policy Institute, April 2019.

78 孙德刚 [Sun Degang], "中国北斗卫星导航系统在阿拉伯世界推广的前景 [Prospects for the Promotion of China's BeiDou Navigation Satellite System in the Arab World]," 中东地区发展报告 [*Reports on Middle East Development*] (Beijing: 时事出版社 [Current Affairs Press], 2016), pp. 52-53.

79 FireEye, "M-TRENDS 2019: Special Report" (Milpitas: FireEye, 2019), pp. 29-30.

80 David E. Sanger, *Saibaa Kanzen Heiki* [*The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*], trans. Takatori Yoshihiko (Tokyo: Asahi Shimbun Publishing, 2019), p. 424.

81 Chris C. Demchak and Yuval Shavitt, "China's Maxim – Leave No Access Point Unexploited," *Military Cyber Affairs*, Vol. 3, No. 1 (2018), p. 4.

82 Senate Select Committee on Intelligence, *Worldwide Threat Assessment of the US Intelligence Community*, January 29, 2019, p. 5.

83 National Counterintelligence and Security Center, *National Counterintelligence Strategy of the United States of America 2020–2022*, January 7, 2020.

84 CISA, last modified May 13, 2020, https://www.cisa.gov/news/2020/05/13/fbi-and-cisa-warn-against-chinese-targeting-covid-19-research-organizations.

85 中国外交部 [Ministry of Foreign Affairs of the People's Republic of China], last modified May 11, 2020, https://www.fmprc.gov.cn/web/wjdt_674879/fyrbt_674889/t1777931.shtml.

86 Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019* (Washington D.C.: U.S. Department of Defense, May 2019), pp. 103-104.

Chapter 3

1 *Xinhua*, April 24, 2017.

2 人民网 [*People's Daily Online*] (Japanese edition), October 19, 2017.

3 CCTV, accessed July 21, 2020, http://tv.cctv.com/2012/12/10/VIDA1355151248768183.shtml.

4 Shu-Hsien Liao, "Will China Become a Military Space Superpower?" *Space Policy*, Vol. 21, No. 3 (2005), p. 205.

5 *Xinhua*, October 10, 2016.

6 Brian Harvey, *China in Space* (New York: Springer, 2013), p. 40.

7 Tsujino Teruhisa, "Chugoku no Uchu Kaihatsu Jijo (Sono 10) Kaishushiki Eisei [The Space Development Situation of China (Part 10): Recoverable Satellites]," *Chugoku Kagaku Gijutsu Geppo* [*China Science and Technology Monthly Report*], No. 79 (May 2013).

8 Ibid.

9 *China Daily*, February 13, 2018.

10 Yatsuzuka Masaaki, "Gunji Senryaku kara miru Chugoku no Uchu Kaihatsu Riyo [China's Development and Use of Space as Seen from its Military Strategy]," *Toa* [*East Asia*], No. 625 (July 2019), p. 21.

11 Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Santa Barbara: Praeger, 2017), p. 157.

12 Yatsuzuka, "Gunji Senryaku kara miru Chugoku no Uchu Kaihatsu Riyo," pp. 21-22.

13 Cheng, *Cyber Dragon*, p. 157.

14 Yamaguchi Shinji, "Revising Its Strategic Posture and Expanding Capabilities—The PLAAF," *NIDS China*

Security Report 2016 (Tokyo: NIDS, 2016), pp. 22-24.

15 Cheng, *Cyber Dragon*, p. 164.

16 解放军报 [*PLA Daily*], November 6, 2018.

17 肖天亮 [Xiao Tianliang], ed., 战略学 [*Science of Military Strategy*] (Beijing: 国防大学出版社 [NDU Press], 2015), p. 141.

18 Cheng, *Cyber Dragon*, p. 165.

19 Ibid., p. 163.

20 Yatsuzuka, "Gunji Senryaku kara miru Chugoku no Uchu Kaihatsu Riyo," p. 22.

21 人民网 [*People's Daily Online*] (Japanese edition), February 6, 2013.

22 Ibid.

23 *Global Times*, February 13, 2018.

24 Ibid.; *Xinhua*, June 13, 2017.

25 Kelvin Wong, "Solar-Electric Cai Hong UAV Conducts Stratospheric Flight," *Jane's International Defence Review*, June 26, 2017.

26 Kelvin Wong, "Heavily Armed CASC CH-5 UAV Makes Public Debut," *Jane's International Defence Review*, November 7, 2016.

27 Office of the Secretary of Defense (OSD), *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019* (Washington D.C.: U.S. Department of Defense (DOD), May 2019), p. 47.

28 *Xinhua*, August 29, 2016.

29 John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," in *Chairman Xi Remakes the PLA* (Washington D.C.: National Defense University Press, 2019), p. 455.

30 U.S.-China Economic and Security Review Commission, "Prepared Statement of Mark A. Stokes before the U.S.-China Economic and Security Review Commission, Hearing on 'China in Space: A Strategic Competition?'" April 25, 2019, p. 4.

31 Simon Seminari, "Op-Ed: Global Government Space Budgets Continues Multiyear Rebound," *SpaceNews*, November 24, 2019.

32 Union of Concerned Scientists, last modified April 1, 2020, https://www.ucsusa.org/resources/satellite-database.

33 Ibid.

34 Liao, "Will China Become a Military Space Superpower?" p. 209.

35 GlobalSecurity.org, accessed July 21, 2020, https://www.globalsecurity.org/space/world/china/cheos.htm.

36 *People's Daily Online*, March 16, 2012.

37 The State Council, The People's Republic of China, *Full Text of White Paper on China's Space Activities in 2016*, December 28, 2016.

38 Rui C. Barbosa, "Long March 2D Launches LKW-4," *NASASpaceFlight.com*, March 17, 2018.

39 Harvey, *China in Space*, p. 210.

40 *Gbtimes*, October 9, 2018.

41 Tate Nurkin, "Catching Up: China's Space Programme Marches On," *Jane's Defence Weekly*, July 30, 2015.

42 Harvey, *China in Space*, pp. 146-147.

43 GlobalSecurity.org, accessed July 21, 2020, https://www.globalsecurity.org/space/world/china/fh-1.htm.

44 Rui C. Barbosa, "China Launches Shen Tong-1 Military Satellite via Long March-3A," *NASASpaceFlight.com*, November 24, 2010.

45 The State Council Information Office, The People's Republic of China, "China's BeiDou Navigation Satellite System," June 2016, p. 5.

46 *Xinhua*, December 27, 2018.

47 *Xinhua*, June 23, 2020.

48 人民网 [*People's Daily Online*] (Japanese edition), February 6, 2013.

49 Kevin N. McCauley, "Putting Precision in Operations: The Beidou Satellite Navigation System," *China Brief*, Vol. 14, No. 16 (2014), p. 11.

50 GPS.GOV, last modified October 2001, https://www.gps.gov/systems/gps/modernization/sa/faq/#on.

51 人民网 [*People's Daily Online*] (Japanese edition), February 6, 2013.

52 *Xinhua*, September 1, 2015.

53 McCauley, "Putting Precision in Operations," p. 11.

54 *Kyodo News*, July 24, 2013; OSD, *Military and Security Developments Involving the People's Republic of China 2019*, p. 67.

55 OSD, *Military and Security Developments Involving the People's Republic of China 2019*, p. 67.

56 人民网 [*People's Daily Online*] (Japanese edition), January 22, 2018.

57 OSD, *Military and Security Developments Involving the People's Republic of China 2019*, p. 101.

58 Brian Weeden and Victoria Samson, eds., *Global Counterspace Capabilities* (Washington D.C.: Secure World Foundation, April 2020), pp. 1-2, 1-8.

59 鲁宇 [Lu Yu], "Chugoku Kyaria Roketto Gijutsu no Hatten (Sono 1) [Development of Chinese Carrier Rocket Technology (Part 1)]," *Chugoku Kagaku Gijutsu Geppo*, No. 142 (August 2018).

60 Ibid.

61 *Xinhua*, December 28, 2019.

62 中国运载火箭技术研究院新闻中心 [China Academy of Launch Vehicle Technology News Center], last modified November 6, 2018, http://www.calt.com/n482/n498/c14640/content.html.

63 中国运载火箭技术研究院新闻中心 [China Academy of Launch Vehicle Technology News Center], last modified May 12, 2016, http://www.calt.com/n482/n498/c4962/content.html.

64 *Xinhua*, August 31, 2019.

65 *China Daily*, April 27, 2020.

66 Tsujino Teruhisa, "Teiten Kansoku Shiriizu Chugoku no Uchu Kaihatsu Doko (Sono 6) [Fixed Point Observation Series: Chinese Space Development Trends (Part 6)]," *Chugoku Kagaku Gijutsu Geppo*, No. 148 (February 2019); Tsujino Teruhisa, "Teiten Kansoku Shiriizu Chugoku no Uchu Kaihatsu Doko (Sono 10) [Fixed Point Observation Series: Chinese Space Development Trends (Part 10)]," *Chugoku Kagaku Gijutsu Geppo*, No. 160 (February 2020).

67 *Xinhuanet*, June 5, 2019.

68 Ibid.

69 人民网 [*People's Daily Online*] (Japanese edition), March 8, 2018; *Global Times*, October 23, 2019.

70 人民网 [*People's Daily Online*] (Japanese edition), June 12, 2015.

71 Weeden and Samson, *Global Counterspace Capabilities*, p. 1-9.

72 Ibid., p. 1-10.

73 *The Guardian*, January 23, 2007.

74 National Air and Space Intelligence Agency, U.S. Air Force, *Competing in Space* (Wright-Patterson AFB: U.S. Air Force, December 2018), p. 21; Defense Intelligence Agency (DIA), *Challenges to Security in Space* (Washington D.C.: U.S. DOD, January 2019), p. 20; Weeden and Samson, *Global Counterspace Capabilities*, p. 1-13.

75 Todd Harrison et al., *Space Threat Assessment 2020* (Washington D.C.: Center for Strategic and International Studies (CSIS), March 2020), p. 10.

76 Bill Gertz, "China Conducts Test of New Anti-Satellite Missile," *The Washington Free Beacon*, May 14, 2013.
77 OSD, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2015* (Washington D.C.: U.S. DOD, May 2015), p. 14.
78 Bill Gertz, "China ASAT Test Part of Growing Space War Threat," *The Washington Free Beacon*, February 23, 2018.
79 Weeden and Samson, *Global Counterspace Capabilities*, pp. 1-13, 1-14.
80 DIA, *Challenges to Security in Space*, p. 21.
81 Ibid., p. 10.
82 Bill Gertz, "Satellite Photos Show Chinese Anti-Satellite Laser Base," *The Washington Free Beacon*, April 1, 2019.
83 DIA, *Challenges to Security in Space*, p. 20.
84 Weeden and Samson, *Global Counterspace Capabilities*, p. 1-15.
85 OSD, *Military and Security Developments Involving the People's Republic of China 2019*, p. 64.
86 Weeden and Samson, *Global Counterspace Capabilities*, p. 1-16.
87 NHK, June 23, 2019.
88 DIA, *Challenges to Security in Space*, p. 20.
89 *The Guardian*, October 27, 2011.
90 Cheng, *Cyber Dragon*, p. 161.
91 *Xinhua*, August 29, 2016.
92 China Aerospace Science and Technology Corporation, accessed July 21, 2020, http://english.spacechina.com/n16421/n17138/n382513/index.html; China Aerospace Science and Industry Corporation, accessed July 21, 2020, http://www.cccme.org.cn/shop/tools043/introduction.aspx.
93 Jean Deville, "China's New Space: A Deep Dive into the World's Fastest Growing Commercial Space Industry," The China Aerospace Blog, December 12, 2018.
94 *The Washington Post*, November 23, 2013.
95 中新网 [*Chinanews*], December 11, 2019.
96 *China Daily*, December 7, 2018.
97 Galaxy Space, accessed July 21, 2020, http://www.yinhe.ht/solutionEn.html.
98 Andrew Jones, "China Launches Yinhe-1 Commercial Low Earth Orbit 5G Satellite," *SpaceNews*, January 16, 2020.
99 iSpace, accessed July 21, 2020, http://www.i-space.com.cn/index.php?m=content&c=index&a=lists&catid=2; Andrew Jones, "Chinese iSpace Achieves Orbit with Historic Private Sector Launch," *SpaceNews*, July 25, 2019.
100 Jones, "Chinese iSpace Achieves Orbit with Historic Private Sector Launch."
101 Ibid.
102 Ibid.
103 One Space, accessed July 21, 2020, http://www.onespacechina.com/en/about/.
104 Andrew Jones, "Landspace of China to Launch First Rocket in Q4 2018," *SpaceNews*, August 2, 2018.
105 *People's Daily Online*, June 12, 2019.
106 *South China Morning Post*, June 12, 2019.
107 *Global Times*, June 11, 2019.
108 Ibid.
109 中新网 [*Chinanews*], December 11, 2019.
110 Blaine Curcio, "China's Space Industry in the Time of COVID-19," *Satellite Markets & Research*, June 1, 2020.

111 Ibid.; 北京九天微星科技发展有限公司 [Beijing Commsat Technology Development Co., Ltd.], last modified May 14, 2020, http://www.commsat.cn/news/read/124.html.

112 Costello and McReynolds, "China's Strategic Support Force," pp. 442-443.

113 "Transcript of '60 Minutes' Air Force Space Command Segment," *SpaceNews*, April 26, 2015.

114 Theresa Hitchens and Joan Johnson-Freese, "Toward a New National Security Space Strategy," *Atlantic Council Strategy Paper*, No. 5 (Washington D.C.: Atlantic Council, June 2016), p. 3.

115 The White House, last modified August 9, 2018, https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-future-u-s-military-space/.

116 *China Military Online*, March 1, 2020.

117 人民网 [*People's Daily Online*] (Japanese edition), May 21, 2018.

118 Patrick Tucker, "China's Moon Missions Could Threaten US Satellites: Pentagon," *Defense One*, October 16, 2018.

119 Sandra Erwin, "Air Force Eyeing Technology to Monitor Space Traffic near the Moon," *SpaceNews*, April 14, 2020.

120 Colin Clark, "China Reaches Out to US for Space Data: Air Force Space Commander," *Breaking Defense*, December 8, 2014.

121 Ministry of External Affairs, Government of India, last modified March 27, 2019, https://www.mea.gov.in/press-releases.htm?dtl/31179/Frequently_Asked_Questions_on_Mission_Shakti_Indias_AntiSatellite_Missile_test_conducted_on_27_March_2019.

122 Ashley J. Tellis, "India's ASAT Test: An Incomplete Success," Carnegie Endowment for International Peace, April 15, 2019.

123 *China Military Online*, March 28, 2019.

124 Aoki Setsuko, "Uchu Gabanansu no Genzai: Kadai to Kanosei [Space Governance Now: Challenges and Possibilities]," *Kokusai Mondai* [*International Affairs*], No. 684 (September 2019), p. 18.

125 BeiDou Navigation Satellite System, last modified November 7, 2018, http://en.beidou.gov.cn/SPECIALCOLUMN/201811/t20181115_16596.html; *Xinhua*, December 27, 2018.

126 *TASS*, October 4, 2019.

127 Dmitry Stefanovich, "Russia to Help China Develop an Early Warning System," *The Diplomat*, October 25, 2019.

128 Asia-Pacific Space Cooperation Organization, accessed July 21, 2020, http://www.apsco.int/html/comp1/content/APOSOS/2019-03-01/59-261-1.shtml.

129 Elsa B. Kania, "China's Strategic Situational Awareness Capabilities," CSIS, Spring 2019, p. 11.

130 The Institute of Remote Sensing and Digital Earth, Chinese Academy of Sciences, accessed July 21, 2020, http://english.radi.cas.cn/RD/crssgs/; *China Daily*, December 16, 2016.

131 *China Daily*, December 16, 2016.

132 人民网 [*People's Daily Online*] (Japanese edition), June 22, 2018.

133 人民网 [*People's Daily Online*] (Japanese edition), September 14, 2017.

Chapter 4

1 中国共产党网 [*News of the Communist Party of China Net*], January 16, 2018; 温莉 [Wen Li], "新时代军工企业军民两用技术发展探析 [Analysis of the Development of Military and Civil Dual-Use Technologies in the Military Industry in the New Era]," 科技资讯 [*Science & Technology Information*], No. 26 (2019), p. 252.

2 人民日报 [*People's Daily*], August 18, 1984.

3 毛泽东军事文集 第2卷 [*Collection of Mao Zedong's Military Works, Vol. II*] (Beijing: 军事科学出版社 [Military Science Publishing House] and 中央文献出版社 [Central Party Literature Press], 1993), pp. 689-695.

4 人民日报 [*People's Daily*], September 30, 1949.

5 人民日报 [*People's Daily*], December 6, 1949.

6 孙力、王鸾 [Sun Li and Wang Ying], "军民融合战略的历史演进及内在逻辑 [The Historical Evolution and Internal Logic of the Military-Civil Fusion Strategy]," 中国浦东幹部学院学报 [*Journal of China Executive Leadership Academy Pudong*], March 2018, p. 70.

7 The "third front" movement refers to large-scale construction projects that sought to disperse the locations of strategic equipment and military facilities to China's interior in preparation for war. The "first front" was coastal areas, the "second front" central areas, and the "third front" remote inland areas.

8 The calculations are based on, among other sources: Department of Comprehensive Statistics of the National Economy, National Bureau of Statistics of the People's Republic of China, ed., 新中国五十五年统计资料汇编 [*China Compendium of Statistics 1949–2004*] (Beijing: 中国统计出版社 [China Statistics Press], 2005); and materials compiled by the Department of Comprehensive Statistics, Ministry of Finance of the People's Republic of China.

9 邓小平军事文集 第3卷 [*Collection of Deng Xiaoping's Military Works, Vol. III*] (Beijing: 军事科学出版社 [Military Science Publishing House] and 中央文献出版社 [Central Party Literature Press], 2004), p. 195.

10 姜鲁鸣 [Jiang Luming] et al., 军民融合发展战略探论 [*On the Military-Civil Fusion Development Strategy*] (Beijing: 人民出版社 [People's Publishing House], 2017), p. 7.

11 Its background is discussed in detail in Anami Yusuke, *Chugoku wa Naze Gunkaku wo Tsuzukerunoka* [*Why Does China Continue to Expand the Military?*] (Tokyo: Shinchosha, 2017).

12 孙力、王鸾 [Sun Li and Wang Ying], 新时代军民融合发展战略研究 [*Study of the Military-Civil Fusion Development Strategy in the New Era*] (Beijing: 人民出版社 [People's Publishing House], 2019), p. 28.

13 Komagata Tetsuya, "Kaihogun Bijinesu to Kokubokogyo (Gunmin Tenkan Gunmin Kenyo) [The PLA's Businesses and National Defense Industry (Military to Civil Conversion and Military-Civil Dual Use)]," *Chugoku wo meguru Anzenhosho* [*China's Security*] (Kyoto: Minerva Shobo, 2007), p. 350.

14 Sun and Wang, *Study of the Military-Civil Fusion Development Strategy in the New Era*, p. 30.

15 "The three represents" is the concept that the CCP represents: (1) demands for the development of China's advanced social productive forces; (2) the forward orientation of China's advanced culture; and (3) the fundamental interests of the majority of the people of China (not limited to proletariats).

16 人民日报 [*People's Daily*], October 19, 2000.

17 周武胜 [Zhou Wusheng], "军民结合、平战结合、寓军於民一军民融合是中国特色国防科技工业发展的必由之路 [Civil-Military Integration, Peace-War Integration, Locating Military Potential in Civilian Capabilities: Military-Civil Fusion is the Road for the Development of National Defense Technology and Industry with Chinese Characteristics]," 中国军转民 [*China Spin-On*], No. 7 (2016), p. 11.

18 孙艳红 [Sun Yanhong], "习近平军民融合重大战略思想的科学内涵 [The Scientific Connotation of Xi Jinping's Strategic Thinking on Military-Civil Fusion]," 国防 [*National Defense*], No. 7 (2016), p. 32.

19 人民日报 [*People's Daily*], March 12, 2013; 人民日报 [*People's Daily*], March 13, 2015.

20 Brian Lafferty, "Civil-Military Integration and PLA Reforms," in *Chairman Xi Remakes the PLA* (Washington D.C.: National Defense University Press, 2019), p. 631.

21 中国军民融合发展报告2016 [*Report on China's Military-Civil Fusion Development 2016*] (Beijing: 国防大学出版社 [NDU Press], 2016), pp. 59-61.

22 人民日报 [*People's Daily*], May 31, 2015.

23 解放军报 [*PLA Daily*], February 3, 2017.

24 Jiang et al., *On the Military-Civil Fusion Development Strategy*, p. 17.

25 人民网 [*People's Daily Online*], October 29, 2018.

26 中华人民共和国中央人民政府 [Central People's Government of the People's Republic of China], last modified March 17, 2016, http://www.gov.cn/xinwen/2016-03/17/content_5054992.htm.

27 中华人民共和国中央人民政府 [Central People's Government of the People's Republic of China], last modified December 4, 2017, http://www.gov.cn/zhengce/content/2017-12/04/content_5244373.htm.

28 U.S.-China Economic and Security Review Commission, "2017 Report to Congress of the U.S.-China Economic and Security Review Commission," November 2017, pp. 531-532.

29 Marukawa Tomoo, "Chugoku no Haiteku Hatten wo Yugameru 'Chugoku Seizo 2025' ['Made in China 2025' Distorts China's High-Tech Development]," *Gaiko* [*Diplomacy*], No. 54 (March/April 2019), p. 28.

30 Elsa B. Kania, "China's Threat to American Government and Private Sector Research and Innovation Leadership," Testimony before the House Permanent Select Committee on Intelligence, July 19, 2018, p. 4.

31 人民日报 [*People's Daily*], January 8, 2009.

32 Marcel Angliviel de la Beaumelle et al., *Open Arms: Evaluating Global Exposure to China's Defense-Industrial Base* (Washington D.C.: C4ADS, 2019), p. 15.

33 Sahashi Ryo, "Beikoku no Taichu Seisaku [The U.S. Policy on China]," *Gijutsu Haken: Beichu Gekitotsu no Shinso* [*Technological Hegemony: Deepening of U.S.-China Confrontations*] (Tokyo: Nikkei Business Publications, 2020), p. 58.

34 Kazama Takehiko, "Chugoku no Gijutsu Kakutoku Senryaku―Gunmin Yugo no Katsuyo to Kanren Seisaku (2) [China's Technology Acquisition Strategy: Use of Military-Civil Fusion and Related Policies (2)]," *CISTEC Journal*, No. 181 (May 2019), p. 311.

35 中华人民共和国中央人民政府 [Central People's Government of the People's Republic of China], last modified September 9, 2015, http://www.gov.cn/xinwen/2015-09/09/content_2927580.htm; 孝感市人民政府 [People's Government of Xiaogan City], last modified November 17, 2017, http://gkml.xiaogan.gov.cn/gzdtjxw/50283.jhtml.

36 Kazama, "Chugoku no Gijutsu Kakutoku Senryaku," pp. 310-311.

37 环球网 [*Huanqiu Online*], September 12, 2015; 新华网 [*Xinhuanet*], February 24, 2017.

38 解放军报 [*PLA Daily*], March 15, 2016.

39 中华人民共和国中央人民政府 [Central People's Government of the People's Republic of China], last modified March 2, 2018, http://www.gov.cn/guowuyuan/2018-03/02/content_5270143.htm; 解放军报 [*PLA Daily*], July 7, 2018.

40 中华人民共和国中央人民政府 [Central People's Government of the People's Republic of China], last modified December 4, 2017, http://www.gov.cn/zhengce/content/2017-12/04/content_5244373.htm.

41 中华人民共和国中央人民政府 [Central People's Government of the People's Republic of China], last modified January 22, 2017, http://www.gov.cn/xinwen/2017-01/22/content_5162263.htm.

42 Lafferty, "Civil-Military Integration and PLA Reforms," pp. 643-645.

43 Ibid., p. 646.

44 姬文波 [Ji Wenbo], "党的十八大以来军民融合发展战略的深化与拓展 [The Deepening and Expansion of the Military-Civil Fusion Development Strategy since the 18th National Congress of the Chinese Communist Party]," 国防 [*National Defense*], No. 8 (2017), p. 26; 河北政协新闻网 [Hebei Political Consultative News Network], last modified May 27, 2019, http://www.hbzxxw.com/news/zxxw_7/2019/201905275969.html.

45 Kazama, "Chugoku no Gijutsu Kakutoku Senryaku," pp. 313-314; *South China Morning Post*, July 29, 2017; 澎湃新闻 [*The Paper*], July 24, 2017.

46 Susan M. Puska et al., "Commissars of Weapons Production: The Chinese Military Representative System," in *Forging China's Military Might* (Baltimore: Johns Hopkins University Press, 2014), pp. 89-91; 军事大辞海（上）

[*Military Dictionary (Vol. I)*] (Beijing: 长城出版社 [Chang Cheng Publication], 2000), p. 1239.

47 Sun and Wang, *Study of the Military-Civil Fusion Development Strategy in the New Era*, p. 40.

48 人民网 [*People's Daily Online*], February 26, 2020.

49 *Report on China's Military-Civil Fusion Development 2016*, pp. 31-32.

50 全军武器装备采购信息网 [All-Army Weapons and Equipment Procurement Information Network], accessed July 22, 2020, http://www.weain.mil.cn/.

51 北京市经济和信息化局 [Beijing Municipal Bureau of Economy and Information Technology], last modified December 6, 2016, http://jxj.beijing.gov.cn/jxdt/tzgg/201911/t20191113_505612.html.

52 国家国防科技工业局 [State Administration for Science, Technology and Industry for National Defense], last modified May 15, 2018, http://www.sastind.gov.cn/n157/c6801436/content.html.

53 国防部 [Ministry of National Defense of the People's Republic of China], last modified October 19, 2016, http://www.mod.gov.cn/leaders/2016-10/19/content_4750526.htm.

54 新民晚报 [*Xinmin Evening News*], August 21, 2017.

55 新华网 [*Xinhuanet*], last modified October 23, 2015, http://www.xinhuanet.com//mil/2015-10/23/c_128348509.htm.

56 *Report on China's Military-Civil Fusion Development 2016*, pp. 16-21.

57 国防部 [Ministry of National Defense of the People's Republic of China], last modified March 15, 2018, http://www.81.cn/2018zt/2018-03/15/content_7973046_2.htm.

58 河北政协新闻网 [Hebei Political Consultative News Network], last modified May 27, 2019, http://www.hbzxxw.com/news/zxxw_7/2019/201905275969.html.

59 解放军报 [*PLA Daily*], February 3, 2017.

60 韩秋露 [Han Qiulu] et al., "军民融合背景下的国防動员建设分析 [Analysis of National Defense Mobilization and Buildup against the Background of Military-Civil Fusion]," 中国经贸导刊 [*China Economic and Trade Herald Journal*], No. 5 (2019), pp. 34-36.

61 Jiang et al., *On the Military-Civil Fusion Development Strategy*, pp. 160-161.

62 法制网 [*Legal Daily*], last modified February 27, 2019, http://www.legaldaily.com.cn/army/content/2019-02/27/content_7782179.htm.

63 解放军报 [*PLA Daily*], October 13, 2018; 解放军报 [*PLA Daily*], October 16, 2018.

64 Miyao Emi, "Chugoku Kokubodoinho no Seitei [Establishment of National Defense Mobilization Law of China]," *Gaikoku no Rippo* [*Foreign Legislation*], No. 246 (December 2010), p. 102.

65 Kazama, "Chugoku no Gijutsu Kakutoku Senryaku," p. 303.

66 de la Beaumelle et al., *Open Arms*, pp. 47-50.

67 Alex Joske, "Picking Flowers, Making Honey: The Chinese Military's Collaboration with Foreign Universities," Australian Strategic Policy Institute, October 2018.

68 *Yomiuri Shimbun*, January 29, 2020.

69 中国人大网 [*National People's Congress Online*], February 26, 2010.

70 U.S. Department of State, "Why China Technology-Transfer Threats Matter," October 24, 2018.

71 See Center for Information on Security Trade Control (CISTEC), last modified March 19, 2019, https://www.cistec.or.jp/service/uschina/5-ndaa2019_gaiyou.pdf.

72 See CISTEC, last modified March 12, 2020, https://www.cistec.or.jp/service/uschina/16-20200302_doko.pdf.

73 European Commission, "EU-China: A Strategic Outlook," March 12, 2019, pp. 5-6. In January 2020, the Union of Industrial and Employers' Confederations of Europe also released a report encouraging reexamination of economic relations with China. BusinessEurope, "The EU and China: Addressing the Systemic Challenge," January 2020.