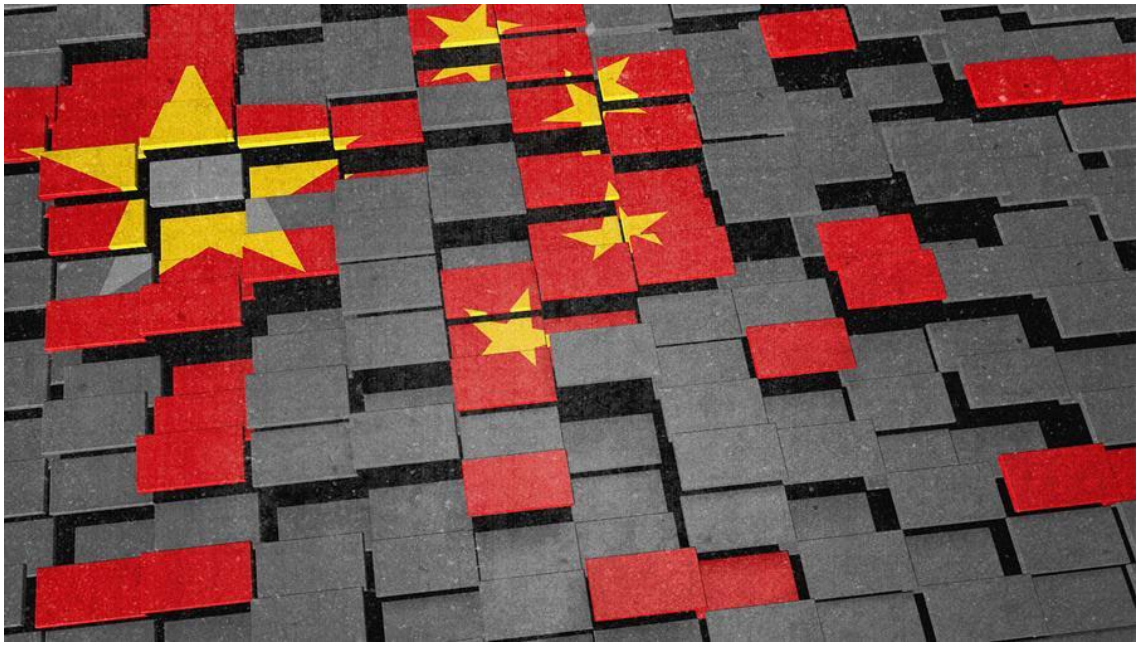
China's Cyber Power and Military-Civil Fusion



MARGIN RESEARCH

The research described in this report was sponsored by the Defense Advanced Research Projects Agency (DARPA) under Contract No. HR00112190088. The views expressed are those of the authors, and do not reflect any views or opinions of the United States Government.

www.margin.re

Contents

Foreword and Acknowledgements

At present China poses one of the most significant foreign cyber threats to the United States and its allies. To help meet this challenge Margin Research has engaged in an integrated program looking at both the development of potentially malicious software as well as the way China recruits skilled personnel, organizes their cyber operations, and integrates these activities in support of their military and intelligence services. The mechanism used by the PRC to accomplish this is their Military-Civil Fusion (MCF) program, which continues China's longstanding interest in information and its power and the usefulness of dominating it. Now the MCF program has greatly expanded China's its cyber capabilities in intelligence, espionage, deception, and cyber warfare.

This rapidly growing threat has received increasing notice and discussion in the open literature, although data supporting China's malicious cyber operations are limited. A prior report by Margin Research presents an analysis based on data generated by Chinese operations using code artifacts inserted into various software systems, resulting in an exploration of China's malicious cyber ecosystem.

The present report extends the analysis to the evolving MCF program that both enables and controls their cyber ecosystem. Based on a review of original materials and related analyses this report covers the current state of China's MCF activities. This is an area where the PRC invests heavily, supporting their cyber operations in a host of areas that are not yet widely appreciated.

This effort was made possible with support from the Defense Advanced Research Projects Agency (DARPA). The study team has benefited greatly from discussions with personnel from several U.S. Government agencies, as well as former officials and other experts. Supporting the work have been several research assistants, currently graduate and law students at Harvard University and New York University (NYU) School of Law. The views expressed do not reflect the views of any organization or the U.S. Government.

March 22, 2023

Executive Summary

National security threats from China have become an increasing concern to the United States and the Western allies. Among the most likely hostile actions the PRC might actually take are cyber operations, ranging from deniable espionage to full-scale cyberattacks on critical national sectors. Here China continues to invest heavily in developing these capabilities has been utilizing their Military-Civil (MCF) fusion program to accomplish these goals. For China this is a major initiative that is not well understood or appreciated at present.

In developing the MCF program China looked at examples in the U.S., such as DARPA, to see how the defense and private sector could be effectively integrated in the technology space to meet critical national requirements. China did not copy the U.S. examples but crafted their own unique structure that would enable the development of individual skills as well as organizational integration of universities, commercial firms, and their defense and intelligence agencies. Over the past several years China's implementation of the MCF strategy and program has significantly changed their ability to develop highly effective cyber tools and operations.

China's interest in cyber grew rapidly in response to what it observed in U.S. military operations starting with Operation Desert Storm in 1991. By 2013, China emphasized cyberspace as a crucially important area in the struggle with the United States and the West. China's cyber capabilities and operations have increased exponentially to the point where they pose a highly significant national security threat.

This paper draws on a range of materials and the previously published Margin Research study, *China's Cyber Operations: The Rising Threat to American Security*, to describe China's investment in Military-Civil fusion and offensive cyber capabilities. The analysis is informed by data collected on China's strategy, tactics, and actual operations in cyberspace.is of China's MCF) strategy.

China's starting point in the cyber arena, as in all other things, is control: ***controlling dissent and competition through controlling information*** while supporting its indigenous entrepreneurs and industries. Espionage and theft of intellectual property, personal data, and state secrets form a central part of China's approach to achieving information domination.

China's efforts in the cyber area, however, do not stop here. Over the past 20 years, China revised its cyber objectives to include major offensive capabilities including cyberwarfare, undertaking major reorganizations to support these objectives. These dramatic changes and details of the Chinese cyber threat are not well understood or appreciated – they need to become a central part of the U.S. national security discourse with respect to cybersecurity.

- From 2015 through 2016, the People's Liberation Army (PLA) reorganized, consolidating previously dispersed units under the Strategic Support Force (SFF).

- China issued new, extensive laws, policies, regulations, and standards to bolster a cyber governance regime designed to enhance both control of information and surveillance.
- China adopted a strategy of Military-Civil Fusion (MCF) managed by the Chinese Communist Party (CCP), chaired by President Xi, to enhance integration with a view to dominating the multi-billion-dollar cyber economy and cybersecurity.

China's methods embraced in MCF include promoting emerging technologies; coordinating with universities and commercial firms; and exploiting intellectual property and options financing. China prioritizes coordination of space, cyber, and electronic warfare as strategic weapons. MCF integrates private actors with the government and has replaced criminal hacking groups with domestic professionals. China also has coopted free-lancers—criminal elements and hackers—on whose patriotism China can rely, while increasingly looking to more conventional, university-developed talent.

Evolution of China's Cyber Strategy

For more than a century, Chinese leaders have seen the value of greater access to technology and information to support their national objectives and military capabilities. The CCP has always understood the importance of controlling information for domestic control, as well as in competition and conflict. Starting in the 1970s, China moved to acquire technologies in order to collect, store, process, and manage information. China still operates below the threshold of direct confrontation and at a level of visibility that reflects major advances made in this area, using the technology base as to radically shape the national cyber ecosystem and exploit it in new and innovative ways. This basis for control spans social media, the use of personal connected devices.

The PRC has already implemented applications that track individuals and their behavior, and is able to access Chinese sites, or versions of U.S. sites, as they monitor and control interactions with servers and sites outside China. The technology has also enabled Chinese espionage operations on a scale never before imagined Their operations include theft of intellectual property, extraction of personal data, and penetration of strategic systems—activities going far beyond the traditional intelligence mission of stealing secrets for national security purposes.

China's targets include vast amounts of data and access to protected networks, as well as commercial enterprises to make China more competitive in world markets. As part of their long-term competition with the United States, the CCP views collection and hoarding of information as an investment in the future. It is a strategic aim, not merely a near term tactic. In the area of cyberwarfare China sees cyberspace in the broader context of information space. The ultimate objective is not "control" of cyberspace but control of information, a vision that dominates China's cyber operations.

Organization of China's Cyber Operations

As part of its modernization effort the PLA consolidated previously decentralized cyber units into the SSF to improve the PLA's combat capabilities, transforming cyber operations from

loosely linked operators focused on access to trade secrets into a professional intelligence service to defend critical infrastructure, conduct espionage, and prepare for combat.

The Chinese strategy of "Military-Civil Fusion" (MCF, 军民融合) is designed to facilitate cooperation between China's civilian, commercial, and military and defense sectors and develop the PLA into a "'world class military' by 2049." Expansive in scope, the strategy includes everything from efforts in big data and infrastructure to logistics and national defense mobilization. Domains that have been prioritized for development are cyberspace, security and informatization, biotechnology, and artificial intelligence.

Cybersecurity and Informatization Bodies

- *Central Cyberspace Affairs Commission (CCAC,* 中共中央网络安全和信息化委员会*):* The CCAC integrates the structures and policy areas that previously composed China's approach to cyber.
- *Cyberspace Administration of China (CAC, 国家互联网信息办公室)*: As the office of the CCAC, the CAC is responsible for handling cyberspace and Internet content, enforcing the People's Republic of China (PRC)'s various data regulations, and managing information infrastructures, personal data protection, and data security.
- *Strategic Support Force (SSF, 战略支援部队)*: The SSF centralizes the PLA's strategic space, cyber, electronic, and psychological warfare missions.
- *Ministry of State Security (MSS, 国安部*): The MSS is China's main civilian intelligence authority responsible for domestic and foreign intelligence operations.
- *Ministry of Public Security (MPS, 公安部)*: The MPS oversees all police departments, with responsibility for supervising public information networks, public security work and policing.
- *Ministry of Industry and Information Technology (MIIT, 工业和信息化部)*: The MIIT is responsible for China's network infrastructure and issues of data security.

China's Offensive Cyber Security Landscape

As part of MCF China has eliminated barriers between its civilian-commercial industries and the state with technology firms, particularly domestic cybersecurity enterprises. Such firms constitute an important resource for China's government and military even while operating under increasing government restrictions. Cybersecurity experts have also moved from large firms and established their own companies, most of these firms are dedicated to vulnerability research, threat detection, and security intelligence, and a growing number of these firms also emphasize blockchain security. The PLA, China's security services, and policymakers increasingly use this ecosystem to support their cyber operations.

China's cybersecurity firms operate under rigid constraints. The government touts the strategic benefits of keeping knowledge of vulnerabilities close to home, noting that vulnerabilities are no longer of use once exposed publicly by Chinese hacking teams at competitions. China

therefore discourages its security researchers from participating in hacking competitions abroad, particularly those where zero-day vulnerabilities may be publicly disclosed.

Industry leaders in China see their cybersecurity universe as unique. Cybersecurity firms, particularly those dealing with personal data security, zero trust, cloud security, and privacy, are more likely to receive funding from the government, state-owned enterprises, and publicly listed companies than other candidates for Chinese government funding.

Cyber Personnel Recruitment and Operations

Competition in cyberspace is, ultimately, a competition for talent, and China has recruited cyber personnel by appealing to hackers' patriotism and by co-opting existing criminal hacking collectives. China also recruits early generation hackers from universities into the PLA and other government institutions. More recently, China has emphasized professionalism in cybersecurity with education reforms to develop elite institutions, fostering extensive MCF and militia programs, as well as bolstering relationships with the private sector.

Chinese universities develop top talent, conduct sensitive research programs in tandem with or funded by the government, and act as recruitment pipelines for the PLA, MSS, and related contractors. These recruitment efforts in cyber are part of a larger effort to recruit expertise in a variety of national security areas and the "Thousand Talents" plan attempted to reverse the brain drain of Chinese scientists and academics who studied and remained overseas by incentivizing them to return to China.

In most offensive cyber campaigns, the PLA relies on contractors, and the PLA Strategic Support Force (SSF) began civilian recruitment in 2018 but has suffered from issues in hiring and retaining civilian talent as salary discrepancies and differences in culture between the SSF and the private sector likely make the SSF a less appealing place to work. China has tried to circumvent this problem by eliminating barriers between China's civilian research and commercial sectors, and its military and defense industrial sectors.

The PLA also recruits civilians with cyber expertise into a militia reserve force to supplement the regular military. This reserve force reportedly numbers over 10 million and is able to help the PLA exploit the civilian sector while retaining control over offensive cyber campaigns.

Defending Against Chinese Deception and Misinformation

Apart from defending against China's espionage and other data collection efforts, the United States must anticipate and deflect the strategic use of deception and misinformation, tactics that have been employed throughout China's political and military history. The failure to take these tactics seriously has inflated China's ability to succeed where they decide to compete.

China's use of deception and misinformation in the cyber area multiplies their political and economic advantages. Government's control over domestic cyber operations includes sophisticated deception operations with regard to the outer world, and the U.S. is unlikely to be able to determine how much China has shaped the content of data. A new approach is needed.

1. Overview of Cyber Power in China

China's interest in cyber grew rapidly in response to what it observed in U.S. military operations starting with Operation Desert Storm in 1991. By 2013, China emphasized cyberspace as a crucially important area in the struggle with principal competitors and adversaries such as the United States and the West. At present, China's cyber capabilities and operations have increased exponentially to the point where they pose a highly significant national security threat to the U.S. and all China's perceived adversaries. China continues to invest huge sums in this effort.

This paper draws on open-source materials and the previously published Margin Research study, *China's Cyber Operations: The Rising Threat to American Security*, to describe China's large-scale investment in military-civil fusion and offensive cyber capabilities. The findings are informed by a large body of data collected by the research team to examine China's strategy, tactics, and operations in cyberspace as well as Internet communications in Chinese software development and cyber operations.

As with the prior work, this effort was sponsored by the Defense Advanced Research Projects Agency (DARPA) under its SocialCyber program, to use artificial intelligence (AI) to investigate and mitigate security risks to open-source software (OSS). It also supplements the previous work with an initial discussion of China's military-civil fusion (MCF) strategy—though there is still much more research to be done.

China's starting point with respect to international competition in the cyber arena, as in all other things, is control: ***controlling dissent and competition through controlling information*** while supporting its indigenous entrepreneurs and industries. Espionage and theft of intellectual property, personal data, and state secrets form a central part of China's approach to achieving information domination.

China's efforts in the cyber area, however, do not stop here. In the past 20 years, China revised its cyber objectives to include major offensive capabilities including cyberwarfare and adapted its structures in line with them, undertaking major reorganizations to support these evolving objectives. These dramatic changes and details of the Chinese cyber threat are not well understood or appreciated; they need to become a central part of the U.S. national security discourse with respect to cybersecurity.

- From 2015 through 2016, the People's Liberation Army (PLA) modernized through reorganization, consolidating previously dispersed units under the Strategic Support Force (SFF).
- China issued new, extensive laws, policies, regulations, and standards to bolster a cyber governance regime designed to enhance control of information.
- China adapted a strategy of Military-Civil Fusion (MCF) managed by the Chinese Communist Party (CCP) Central Commission for Military-Civil Fusion Development,

chaired by President Xi, to enhance cross-sector integration with a view to dominating the multi-billion-dollar cyber economy, including with respect to cybersecurity.

China's methods include promoting emerging technologies, coordinating with institutes of higher education, and exploiting intellectual property and options financing. China prioritizes coordination of space, cyber, and electronic warfare as strategic weapons. It integrates private actors with government and, since 2015, has increasingly replaced criminal hacking groups with domestic professionals. China also has coopted free-lancers—criminal elements and hackers—on whose patriotism China can rely, while increasingly looking to more conventional, university-developed talent.

The Chinese government entered the global competition for talent and has used a number of incentives, including money and positions, to achieve success. China also developed world class cybersecurity schools that emphasize AI, among other emerging technologies. Seven universities in particular, known as the Seven Sons of National Defense, feed PLA capabilities.

Evolution of China's Cyber Strategy

For more than a century, Chinese leaders have seen the value of greater access to technology and information to support their national objectives and military capabilities. The CCP has always understood the importance of controlling information for domestic control and in competition and conflict. Starting in the 1970s, China moved to acquire technologies in order to collect, store, process, and manage information, with the result most visible in areas such as AI and 5G communications.

China has been operating below the threshold of direct confrontation and at a level of visibility that reflects major advances made in this area. China has used the technology base as an opportunity to radically shape the national ecosystem and exploit it in new and innovative ways. This basis for innovation and control spans social media, the use of personal connected devices including mobile phones, laptops, and others.

The Chinese government has implemented a number of applications that track individuals and their behavior. Users are able to access Chinese sites, or versions of U.S. sites, but the government monitors and controls interactions with servers and sites outside China.

The technology has also enabled espionage operations on a scale never before imagined. Operations include the theft of intellectual property, extraction of personal data, and penetration of strategic systems—activities going well beyond the traditional intelligence mission of stealing secrets for national security purposes. China's targets include vast amounts of data and access to protected networks, as well as commercial enterprises to make China more competitive in world markets. As part of their long-term competition with the United States, the Chinese government and CCP view collection and hoarding of information as an investment in the future. It is a strategic aim, not merely a near term tactic.

In the area of cyberwarfare, the western governments see cyberspace as a "fifth domain" of warfare. The Chinese government and its affiliates, however, look at cyberspace in the broader context of information space. The ultimate objective is not "control" of cyberspace but control of information, a vision that dominates China's cyber operations.

Organization of China's Cyber Operations

China's cyber operations have undergone extensive reorganization. As part of its modernization effort, beginning in December 2015 and throughout 2016, the PLA consolidated previously decentralized cyber units into the SSF to improve the PLA's combat capabilities. This effort transformed China's cyber operations from loosely linked operators focused on access to trade secrets into a professional intelligence service engaged in cyber operations to defend critical infrastructure, conduct espionage, and prepare for combat. In addition to the SSF, two civilian ministries, the Ministry of State Security (MSS) and the Ministry of Public Security (MPS) – the PRC's intelligence services – make up the main Chinese state entities engaged in cyber operations.

China also developed an extensive cyber governance regime to maintain control over the domestic flow of information and influence over cyberspace internationally. This regime is comprised of laws, policies, regulations, and standards overseen by several departments under the guidance of the Central Cyberspace Affairs Commission.

The Chinese strategy of "Military-Civil Fusion" (MCF, 军民融合) is designed to facilitate cooperation between China's civilian, commercial, and military and defense sectors and develop the PLA into a "'world class military' by 2049." Expansive in scope, the strategy includes everything from efforts in big data and infrastructure to logistics and national defense mobilization. Domains that have been prioritized for development are cyberspace, security and informatization, biotechnology, and artificial intelligence.

Cybersecurity and Informatization Bodies

- *Central Cyberspace Affairs Commission (CCAC,* 中共中央网络安全和信息化委员会*):* The CCAC was formed in 2014 to integrate the "fragmented bureaucratic structures and policy areas" that had previously composed China's approach to cyber.
- *Cyberspace Administration of China (CAC, 国家互联网信息办公室)*: As the office of the CCAC, the CAC is responsible for handling cyberspace and Internet content, enforcing the People's Republic of China (PRC)'s various data regulations, and managing information infrastructures, personal data protection, and data security.
- *Strategic Support Force (SSF, 战略支援部队)*: The SSF is a theatre command-level organization that centralizes the military's strategic space, cyber, electronic, and psychological warfare missions.
- *Ministry of State Security (MSS, 国安部*): The MSS is China's main civilian intelligence and anti-espionage authority responsible for domestic and foreign intelligence operations, including human intelligence and cyber operations. It can compel Chinese citizens and organizations to engage in and support intelligence activities.
- *Ministry of Public Security (MPS, 公安部)*: The MPS oversees all provincial and local police departments, with responsibility for supervising public information networks,

public security work and policing. It shares the counterintelligence mission with, and is directed by, the MSS.

- *Ministry of Industry and Information Technology (MIIT, 工业和信息化部)*: The MIIT is responsible for China's network infrastructure and assigned to tackle issues of data security.

Chinese Cybersecurity Laws

- *Cybersecurity Law (CL)*: The CL was the first of several regulations governing data protection in China and establishes requirements for data storage, as well as guidelines for maintaining network security, and also authorizes government authorities to conduct security checks of networks.
- *Data Security Law (DSL)*: The DSL governs data collected and stored in China and determines the requirements for its storage and transfer depending on its potential impact on national security. It also prohibits Chinese organizations and individuals from transferring data stored in China to the justice or law enforcement institutions of foreign countries without approval.
- *Personal Information Protection Law (PIPL)*: The PIPL is a legal framework designed to regulate how companies collect, process, and transfer personal data and applies to entities that collect, store, use, transmit, provide, or otherwise handle personal information of persons within the PRC, even if that entity is located or conducts business entirely outside of China. It also requires entities that handle critical infrastructure information, and which process a "large amount of personal information" to store personal information within China.

China's Offensive Cyber Security Landscape

As China's quest to become a superpower evolves, Beijing has moved to eliminate barriers between its civilian-commercial industries and the state. Technology firms, particularly domestic cybersecurity enterprises, increasingly stand at the forefront of their fields, offering insight and services that constitute an important intellectual, personnel, and hardware resource for China's government and military even while operating under increasing government restrictions.

Cybersecurity experts have also moved from large firms and established their own companies. A survey of selected Chinese cybersecurity firms indicates specific areas of focus, backgrounds of their founders, and, in some cases, their partners and investors. Most of these firms are dedicated to vulnerability research, threat detection, and security intelligence. Their services offer clients protection from offensive cyber activities.

A growing number of these firms also emphasize blockchain security. While their investors are predominantly Chinese venture capital firms, these companies service clients and maintain partnerships around the world. The PLA, China's security services, and policymakers increasingly use this ecosystem to support their cyber operations.

The trajectory of China's cyber industry is closely related to the proliferation of firms engaged in cybersecurity research. As part of its MCF approach, China's leadership has emphasized the need to foster innovation in domestic technologies and has called on private enterprises to contribute to the security of the state and its citizens. People embedded in China's cybersecurity industry stress that start-ups and smaller firms are an important source of this innovation and will continue to play a formative role in China's national cyber strategy.

China's cybersecurity firms operate under rigid constraints. The government touts the strategic benefits of keeping knowledge of vulnerabilities close to home, noting that vulnerabilities are no longer of use once exposed publicly by Chinese hacking teams at competitions. China therefore discourages its security researchers from participating in hacking competitions abroad, particularly those where zero-day vulnerabilities may be publicly disclosed.

Industry leaders in China see their cybersecurity universe as unique. They expect domestic companies' growth to continue to outpace that of overseas counterparts. Cybersecurity firms, particularly those dealing with personal data security, zero trust, cloud security, and privacy, are more likely to receive funding from the government, state-owned enterprises, and publicly listed companies than other candidates for Chinese government funding.

Cyber Personnel Recruitment and Operations

Competition in cyberspace is, ultimately, a competition for talent. Historically, China has recruited talented cyber personnel by appealing to hackers' patriotism and by co-opting existing criminal hacking collectives. China also recruited early generation hackers from universities into the PLA and other government institutions. More recently, China has emphasized professionalism in cybersecurity with education reforms to develop elite institutions, fostering extensive military-civil fusion and militia programs, as well as bolstering relationships with the private sector.

University Recruitment and Involvement in Cyber Operations

Like Western institutions that have trouble fitting gifted, self-educated cyber experts into conventional institutions and institutional categories, China's behavior suggests that Beijing also prefers personnel with a traditional profile. Since 2015, China has sought to replace its criminal hacking groups with domestic professionals. The CCP recognizes that talent is essential to the country's cyber efforts and improving education is central to cultivating this talent, in addition to attracting overseas Chinese talent. Chinese universities develop top talent, conduct sensitive research programs in tandem with or funded by the government, and act as recruitment pipelines for the PLA, MSS, and related contractors.

China's recruitment efforts in cyber are part of a larger effort to recruit expertise in a variety of national security areas. The "Thousand Talents" Plan, for example, attempted to reverse the brain drain of Chinese scientists and academics who studied and remained overseas by incentivizing them to return to China. The Ministry of Education and Central Cyberspace Administration also launched an initiative to develop World Class Cybersecurity Schools (一流网络安全学院) to cultivate domestic cybersecurity programs that would allow the country to grow its pool of cyber talent.

China's universities intentionally produce graduates capable of attacking and defending networks, regardless of how they are ranked. Two of the 11 World Class Cybersecurity Schools, Wuhan University and Huazhong University, jointly created the National Cybersecurity School at the National Cybersecurity Talent and Innovation Base (国家网络安全人才与创新基地, the National Cybersecurity Center), which also contains two government-focused laboratories.

Academic links to China's military and defense industry run deep. The government has established 29 national defense science and technology laboratories (国防科技重点实验室) in civilian universities, supervised by the PLA. In addition, 36 national defense labs (国防重点学科实验室) and 53 Ministry of Education defense labs (教育部国防重点实验室) operate out of nonmilitary universities. These schools graduate thousands of students who join organizations engaged in defense research every year.

In addition to training next-generation offensive cyber talent and conducting cutting-edge research on behalf of government ministries, Chinese universities have engaged in cyberattacks and conduct espionage. The APT1 hackers attributed to PLA Unit 61398 had connections to the PLA Information Engineering University (PLAIEU). Members of Unit 61398 were linked to Shanghai Jiao Tong University and likely recruited graduate students for the Unit from Zhejiang University's College of Computer Science and Technology.

The MSS operates the University of International Relations in Beijing and Jiangnan Social University. The MSS uses designated faculty elsewhere for intelligence purposes. The MSS works closely with other universities for training, conducting research, and cyber activities. Faculty at Hunan University and Tianjin University have been designated as MSS experts and awarded prizes by the ministry.

Military Recruitment and Military-Civil Fusion

In most offensive cyber campaigns, the PLA relies on contractors; in its earlier efforts in offensive cyber, the PLA recruited hackers. With the reorganization of the military in 2015 and 2016, many of China's cyber operations were transferred from the PLA to the MSS.

The PLA Strategic Support Force (SSF) began civilian recruitment in 2018 but has suffered from issues in hiring and retaining civilian talent. Salary discrepancies and differences in culture between the SSF and the private sector likely make the SSF a less appealing place to work for domestic information security professionals. China has tried to circumvent this problem by eliminating barriers between China's civilian research and commercial sectors, and its military and defense industrial sectors.

The PLA recruits civilians with cyber expertise into a militia reserve force to supplement the regular military. While these reserves would likely be limited to logistics espionage, rather than offensive operations, this force reportedly numbers over 10 million. Military-civil fusion and the militia reserve force help the PLA exploit the civilian sector while retaining control over targeted offensive cyber campaigns.

The Role of Chinese AI in Open Source Code

Open source software development solicits input from its community of users through technical standards meetings, code submissions, and online discussions, typically small communities that are targets for adversarial influence campaigns and software supply chain attacks. China exploits this regime and especially the Linux operating system to leapfrog development and to penetrate and manipulate the open code. There is no established trust metric to vet accounts or individuals that submit code. An attacker may contribute to the code libraries and submit deliberately vulnerable code or functional backdoors that will be exploited after the code is adopted.

China has developed a robust open source community that chips away at the security of U.S. software. Much of the world's software relies on open source code that is freely available online and that may be redistributed and modified. Multiple open source libraries have been deliberately or accidentally corrupted by maintainers and developers, in China and elsewhere. China has open source code in its sights for malicious operations or operations designed to give advantages to China in its struggle with the United States and others.

By 2020, some 87% of Chinese companies were using open source software. GitHub, a primary platform for open source worldwide, features a large number of Chinese repositories with most major open source projects supported by Chinese companies. Alibaba, PingCAP, Baidu, Tencent, JD, and Huawei are the top six Chinese accounts on GitHub. Worldwide, China is second only to the U.S. in the number of GitHub users and contributors.

The volume of Chinese contributions to Western open source software has skyrocketed. In 2021, Huawei beat out Intel as the top contributor to the Linux Kernel. This software is the baseline of Western technologies like Google's Android, NASA's satellite software, and the Army's Common Operating Environment. Huawei has also contributed code to over 40 mainstream Western technical communities, including Kubernetes, OpenStack, Hadoop, TensorFlow, httpd, and MySQL.

Chinese military leaders want to use AI for offensive cyber operations. An analysis of 343 AI-related contracts executed by the PLA in 2020 shows a focus on procuring AI for intelligence, information warfare, and navigation and target recognition in autonomous vehicles. Military academics in China also look to use AI for stealth, scale, and adaptability in information operations, as well as for hyper-targeted phishing attacks.

President Xi Jinping's stated goal in AI—to pursue both world leadership and self-reliance in AI technology—is in line with China's use of open source technologies. Open source is also featured in China's AI innovation plans. The MIIT New Generation AI Innovation Key Task List contained a task on "open source, open platforms," to use open source and expand the number of data sets, models, and users for machine learning technologies.

China circumvents an overreliance on proprietary Western software by utilizing open source alternatives. After the United States sanctioned Huawei in 2019, the firm was barred from importing most U.S.-made chips and was no longer able to use the Android operating system in

their phones. Subsequently, the United States has sought to prevent investment in Huawei and other Chinese companies with connections to the defense sector.

Preempting Chinese Cyber Operations

The present effort to discover suspicious cyber activity uses new AI techniques to create an analysis pipeline that surfaces highly significant insights about Chinese contributions to the Linux kernel, including the HULK robot. The analysis pipeline consists of a technology stack that ingests the Linux Kernel Mailing List (LKML) and the Linux Git repository, annotates the data, and then creates graphs of the annotated data searchable by analysts. Thus far, it has been possible to analyze the 36,000 contributors to the Linux kernel, highlighting 30 individuals exhibiting suspicious behavior, of which several are known to have submitted "hypocrite commits" that introduced exploitable vulnerabilities to the kernel. The individuals highlighted by the algorithm exhibit the same type of behavior, allowing analysts to explore this behavior in far greater detail than previously possible.

The HULK Robot is not the only automated bug-finding tool belonging to Chinese institutions. The Chinese government funds university labs conducting automated bug hunting in the Linux Kernel, which likely has a defensive purpose, but can easily be transferred to, or shared with, the larger Chinese national security community conducting research on offensive cyber activities.

Defending Against Chinese Deception and Misinformation

Apart from defending against China's espionage and other data collection efforts, the United States and its allies must anticipate and deflect the strategic use of deception and misinformation. Such tactics have often been employed throughout China's political and military history. The historical failure to take these tactics seriously has inflated China's ability to succeed where they decide to compete. This activity goes back years, and it is not well-known or understood in the West. Indeed, it is one of the main reasons Beijing has been so successful.

China's use of deception and misinformation in the cyber area multiplies the country's political and economic advantages. The Chinese government's control over domestic cyber operations includes sophisticated deception operations with regard to the outer world. The United States is not likely to be able to determine how much China has shaped the content of data. Knowing that China has "official" uses of cyber technologies does not itself enable the United States to drill into China's cyber landscape and understand it fully. A new approach is needed.

Hacker conferences, where "hacker" is not synonymous with "criminal," constitute an important source of knowledge about vulnerabilities and threats as well as innovations. Such conferences, especially those focused on security, offer ideal venues for recruiting and a space for government organizations, private companies, established hacking groups, and up-and-coming individuals to network. Sponsored by both the government and large tech companies such as Baidu, Alibaba, and Venustech, conferences like XPwn2017 and Tianfu Cup are often used by the PLA and MSS to recruit university students and other individual hackers.

Cutting off the exchange of knowledge between U.S. and Chinese cyber industries would undermine the ability of service providers to protect their products and network infrastructures and

would also undercut visibility into changing developments in potential offensive cyber activities. But domestic cyber enterprises, as in most countries, also play a vital role in providing infrastructure, talent, and resources to state operations, sometimes by choice, sometimes under legal and political pressure.

2. What is Military-Civil Fusion?

China has adopted an assertive stance against what it sees as the efforts of the United States to stifle and contain its growth."[1] As part of its efforts to bolster competitiveness, the CCP has adopted a national strategy of "Military-Civil Fusion" (MCF, *junmin ronghe*, 军民融合). MCF seeks to facilitate cooperation between China's civilian, commercial, and military-defense sectors to streamline technological innovation[2] and develop the PLA into a "'world class military' by 2049."[3] The strategy aims to unify the military, academic institutions, commercial enterprises, and government and defense agencies to allow the state to pursue a variety of strategic priorities.[4]

Recognizing that economic and strategic interests are often intertwined, MCF seeks to modernize China's approach to national security and domestic development by eliminating barriers between commercial and defense activities.[5] MCF primarily aspires to bolster the independence of the domestic defense industry by exploiting indigenous innovation in the civilian market, particularly in the areas of advanced sciences and technology.[6]

MCF encourages the development of linkages between commercial, academic, and defense enterprises to create a tightly woven military-industrial system. Beijing intends for this system to allow for the mutual exploitation of civilian and military resources, infrastructure, and innovation, such that military enterprises will be able to draw from civilian research and development to improve defense technology, and commercial firms will likewise profit from military invention. This strategy is part of a larger national undertaking to build a stronger country, create a "world-class" military, and enhance international competitiveness.[7]

---

[1] Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China, Annual Report to Congress* (2021).

[2] 习近平谈军民融合：是国家战略 关乎国家安全和发展全局 [Xi Jinping Discusses Military-Civil Fusion: A National Strategy Concerning National Security and Overall Development], 中国共产党新闻 (January 23, 2017), cited in Zi Yang, *Opening Up While Closing Up: Balancing China's State Secrecy Needs and Military-Civil Fusion*, Asia Policy (January 2021).

[3] Department of State, *Military-Civil Fusion and the People's Republic of China* (January 5, 2022).

[4] Emily S. Weinstein, *Testimony before the U.S.-China Economic and Security Review Commission on "U.S. Investment in China's Capital Markets and Military- Industrial Complex,"* (CSET, March 19, 2021).

[5] 国防大学军民融合发展研究中心, 新时代军民融合发展的科学指南 [A Scientific Guide to the Development of Military-Civil Fusion in the New Era], 中国共产党新闻 (December 13, 2017).

[6] 习近平：扎扎实实推进军民融合深度发展 为实现中国梦强军梦提供强大动力和战略支撑 [Xi Jinping: Solidly Promote the In-Depth Development of Military-Civil Fusion to Provide Strong Motivation and Strategic-Support for the Realization of the Chinese Dream], 中国共产党新闻 (March 18, 2018).

[7] *A Scientific Guide to the Development of Military-Civil Fusion in the New Era*.

MCF is an "essential ingredient in Beijing's long-term effort to make China a technological superpower."[8] It is an effort to establish sufficient regulatory and institutional mechanisms to facilitate defense procurement through civilian technological innovation. However, it is also a "philosophy for organizing the national economy," insofar that it reflects an attempt on the part of Beijing to organize the exchange of resources in a way that maximizes economic development, encourages self-sufficiency, and promotes indigenous technological innovation.[9]

As the People's Liberation Army (PLA) shifts from information warfare – the exploitation of information systems to gain or improve advantages over military opponents – to intelligentized warfare – the use of artificial intelligence and related technologies for "military applications" – civilian innovation in critical sectors is an integral element of Chinese military modernization.[10] Given that the private sector remains the predominant locale for innovation in these technologies, MCF has played and will continue to play a critical role in China's military development.

Notably, however, the development and execution of MCF as a national strategy reflect a continuous source of tension for the Chinese Communist Party. One of China's strengths has been the apparent willingness and flexibility of the Party and government to draw from the history, experience, and practices of other states to adapt its own policies.[11] Much of China's drive towards civil-military integration throughout its history was inspired by its study of the U.S. defense industry's close ties with the private sector.[12] Several defense experts in China view the United States as a model for the successful implementation of military-civil fusion.[13]

This willingness to study foreign counterparts and apply lessons learned to the Chinese context underscored much of China's rapid economic development. Under MCF, this acquisition of knowledge from overseas has persisted, often in quite literal ways. Yoram Evron, for example, suggests that one of the greatest achievements of MCF has been the transfer of "advanced military-related expertise from foreign sources to China's military establishment."[14]

---

[8] Richard A. Bitzinger, "China's Shift from Civil-Military Integration to Military-Civil Fusion," 16 *Asia Policy* 5, 8 (January 2021).

[9] *Interview with Greg Levesque, Commercialized Militarization: China's Military-Civil Fusion Strategy*, NBR (June 30, 2021).

[10] Bitzinger, *China's Shift from Civil-Military Integration to Military-Civil Fusion* at 8.

[11] See, for example, the discussion of "powerful countries in history" and their use of military-civil integration to transform national power and strengthen their armies in *A Scientific Guide to the Development of Military-Civil Fusion in the New Era*.

[12] 姬文波, 从"军民结合"到"军民融合"——改革开放以来中国国防科技工业领导管理体制的调整与完善 [From Civil-Military Integration to Military-Civil Fusion: The Adjustment and Improvement of the Leadership and Management System of China's Defense Technology Industry Since Reform and Opening Up], 党史博览 (2018); Elsa B. Kania, *In Military-Civil Fusion, China is Learning Lessons from the United States and Starting to Innovate*, The Strategy Bridge (August 27, 2019).

[13] Elsa B. Kania and Lorand Laskai, *Myths and Realities of China's Military-Civil Fusion Strategy*, CNAS (January 2021).

[14] Yoram Evron, "China's Military-Civil Fusion and Military Procurement," 16 *Asia Policy* 25 (January 2021).

Despite these successes, institutional rigidity and the need for the Party to exert top-level dominance over industries that it views as potentially threatening to stability or state power have often constrained the execution of MCF initiatives. Moreover, even in areas where MCF has been implemented, the manner in which MCF has been executed may in fact stifle innovation.

Nevertheless, the explosive growth of China's defense industry can likely be attributed both to the country's overall strong economic success and the PLA's modernization efforts, including MCF.[15] On a list of global defense companies measured by revenue, 7 Chinese defense enterprises were ranked among the top 20.[16] These companies are responsible for providing technologies and equipment to China's military in several key areas, including aviation, advanced weaponry, defense electronics, aerospace, and shipbuilding.[17]

As state-owned enterprises, these seven companies are eager participants in military-civil fusion, contributing vast sums of money to MCF funds,[18] producing equipment for the PLA,[19] and sharing talent, facilities, and expertise with the military. Yet, they represent a small share of the players in China's industrial defense ecosystem. To understand the complex interplay between actors that now participate in the defense industry in China, we must look at how military-civil fusion has developed over time, and what the doctrine looks like now under the rule of Xi Jinping.

[15] Fenella McGerty and Meia Nouwens, *A Strong 2021 for China's Defence Companies*, IISS (August 17, 2022).
[16] *Defense News Top 100*, Defense News (2022), https://people.defensenews.com/top-100/.
[17] McGerty and Nouwens, *A Strong 2021 for China's Defence Companies*.
[18] Scott Kennedy, *China's Military-Civil Fusion Funds: Big but Not Necessarily Effective*, CSIS (October 4, 2019).
[19] McGerty and Nouwens, *A Strong 2021 for China's Defence Companies*.

3. From Civil-Military Integration to Military-Civil Fusion

Military-civil fusion is the culmination of decades of long-term policy making by the Chinese Communist Party. China has a long history of integration between civilian sectors and the military. In the early days of the post-1949 PRC, elite cadres from the PLA eagerly participated in the development of the country's political and economic policies, "giving elite-level political calculus a militarized slant."[20] Operating under the assumption that there was an insurmountable connection between technological development and national power, these elites encouraged a system of innovation that promoted interaction between the military and organizations engaged in the exploration and production of science and technology.[21]

In the early 1960s, fearful of the potential exposure of defense-related industrial infrastructure to attack, the CCP relocated defense-adjacent industries to the interior regions in the Northwest and Southwest, away from more easily targeted geographic locations.[22] Known as the Third Front Movement (*sanxian jianshe*, 三线建设), the policy marked the "first large-scale state-led initiative to fuse defense industry development with national economic growth."[23]

As China entered into its reform and opening-up period, the impetus for pursuing civil military integration shifted from national defense to China's economy. Concerned with the promoting development, Deng Xiaoping proposed a policy of civil-military integration (*junmin jiehe*, 军民结合), primarily with the intent to apply military resources for economic purposes .[24] Defense technologies, manufacturing centers, and other military infrastructure were converted to civilian use in order to rectify "acute economic, structural, and organizational problems."[25]

During this time, defense production lines were co-opted to produce civilian goods, and several military assets, such as airports, ports, railway lines, communication lines, storage facilities, and land, were conveyed to "civilian partners."[26] Hundreds of civilian economic projects were permitted to use military technology, and "some 10,000 patents were transferred to the civilian sector."[27] Critically, vast numbers of defense personnel were either sent to civilian

[20] Toby Warden, *A Revolutionary Evolution: Civil-Military Integration in China*, Australian Institute of International Affairs (October 1, 2019).
[21] *Id.*
[22] Yang, *Opening Up While Closing Up: Balancing China's State Secrecy Needs and Military-Civil Fusion*.
[23] *Id.*
[24] 姬文, *From Civil-Military Integration to Military-Civil Fusion.*
[25] Bitzinger, *China's Shift from Civil-Military Integration to Military-Civil Fusion* at 13.
[26] Zi Yang, *Opening Up While Closing Up* at 49.
[27] *Id*.

positions or provided technical support for commercial operations.[28] Moreover, many enterprises in the defense industry, such as aviation companies, began to enter into joint ventures with Western counterparts.[29]

While the defense industry likely benefited from general economic growth, most gains in this time period were realized in the commercial sector. Bitzinger estimates that "80%–90% of the value of China's defense industry output was nonmilitary" by the late 1990s.[30] It was not until the mid-1990s that leadership began to entertain notions of military modernization more seriously.[31]From this point, China began to move towards the promotion of dual-use industrial systems that would provide both military and commercial benefits.[32]

Government documents from the early 2000s reveal a strong belief that indigenous technological innovation was an essential element of China's economic and national security.[33] Not only could military technologies and infrastructure be "spun-off" for commercial use, but advanced technologies and processes from the private sector could be spun-on "to benefit defense R&D and production."[34] The ability to bypass arduous R&D processes by drawing from civilian invention provided a more direct and rapid path for defense reform and progress.

Beijing began to prioritize development in key sectors, such as "microelectronics, space systems, new materials (such as composites and alloys), propulsion, missiles, computer-aided manufacturing, and IT." Moreover, in addition to promoting "linkages and collaboration" between the defense industry and civilian tech enterprises, the Chinese government encouraged universities and other institutes to invest in research on dual-use technologies and build connections with foreign technology enterprises.

Meanwhile, foreign firms looking to invest in China were urged to develop "joint R&D centers and transfer their technology."[35] It was also around this time that the CCP helped found the China Electronics Technology Group Corporation (CETC), a state-owned company that operates in communications, IT, software, and electronics.[36] CETC is now the country's third-largest information technology company.[37]

The term "military-civil fusion" was first used by Hu Jintao at the 17th Party Congress in 2007, where he advocated for the pursuit of "a path of military-civil fusion with Chinese characteristics."[38] This marked a break from earlier articulations of the relationship between the

[28] *Id*.
[29] Bitzinger, *China's Shift from Civil-Military Integration to Military-Civil Fusion* at 13.
[30] *Id.* at 14.
[31] Kania, *In Military-Civil Fusion, China is Learning Lessons from the United States and Starting to Innovate.*
[32] Bitzinger, *China's Shift from Civil-Military Integration to Military-Civil Fusion* at 15.
[33] Warden, *A Revolutionary Evolution: Civil-Military Integration in China*.
[34] *Id.* at 15.
[35] Bitzinger, *China's Shift from Civil-Military Integration to Military-Civil Fusion* at 17.
[36] Bitzinger, *China's Shift from Civil-Military Integration to Military-Civil Fusion* at 16.
[37] Shunsuke Tabeta, "China to Create 'IT Aircraft Carrier' Through Tech Megamerger," *Nikkei Asia* (February 26, 2021).
[38] *Selected Words from Hu's Report*, China Daily (last accessed March 18, 2023).

defense industry and the private sector. Whereas earlier initiatives of civil-military integration promoted a more superficial type of collaboration, Hu Jintao's expression of military-civil fusion promised to take a more active approach to deepening the entanglement of the military and civilian ecosystems.[39] Military-civil fusion moved beyond simply combining the two sectors in favor of more comprehensive integration.[40] In particular, it sought to intensify cooperation between the military and private sector in order to allow for the mutual exploitation of resources.

In 2010, the State Council and Central Military Commission produced a guiding document that identified six problems hindering civil military integration in science and technology: poor coordination mechanisms between government, commercial, and research institutions; barriers to civilian participation in the defense market; "insufficient resource sharing between civilian and military sectors"; the need for reform in institutional mechanisms; "underdeveloped" related industries; and "poorly designed or incomplete policies and guidelines."[41]

To address these concerns, the government began encouraging civilian firms to enter the defense market by certifying them to produce new military or dual-use technologies.[42] Defense enterprises began to develop strategies to attract civilian investment. It was also during this time period that the government began developing coalitions between university researchers and commercial producers and experimenting with the establishment of industrial bases to serve as centers for talent recruitment and innovation.[43]

Despite these efforts, China's attempt to combine its commercial and defense industries had limited effect.[44] In the aviation sector, for example, commercial and military aircraft manufacturing remained largely compartmentalized from each other, with little overlap between the technologies in civil and military aviation.[45] China was also plagued with low levels of indigenous design and manufacturing in high technologies and was reliant on foreign enterprises for more advanced technologies. Institutional barriers – such as weak guidelines, protectionist tendencies among firms, and underdeveloped local industries – inhibited collaboration between civilian enterprises with the military.[46]

Military-Civil Fusion under Xi Jinping

After his ascension to the head of the Party, Xi Jinping seems to have first raised the idea of MCF as a national strategy at the 12th National People's Congress in March 2014. Speaking to the PLA delegation, Xi emphasized the need for a state-led drive to coordinate economic growth with the development of the defense industry. Balancing the role of the state with that of market forces in civilian industries, Xi suggested, would promote innovation in both civilian and defense

[39] Brian Lafferty, Aaron Shraberg, and Morgan Clemens, *China's Civil-Military Integrati*on, SITC Research Briefs (2013).
[40] Audrey Fritz, *China's Evolving Conception of Civil-Military Collaboration*, CSIS (August 2, 2019).
[41] Lafferty, Shraberg, & Clemens, *China's Civil-Military Integration*.
[42] *Id*. at 4.
[43] *Id.* at 5.
[44] Bitzinger, *China's Shift from Civil-Military Integration to Military-Civil Fusion* at 18.
[45] *Id.*
[46] *Id.* at 19.

sectors and improve the efficiency of policies targeting the development of military technology.[47] Most importantly, Xi sought to "rejuvenate the nation" and improve the competitiveness of China with other states.[48] Beijing was also eager for tactics to avoid the fate of the Soviet Union, and strategists had pointed to the Soviet's failure to adequately integrate its military with broader industry as contributing to the collapse of its economy.[49]

In 2015, Xi Jinping officially codified MCF as a national military strategy. As a national strategy, military-civil fusion calls to "fully integrate the civilian industrial base into the PLA's supply chain."[50] While Xi's version of MCF seeks to tightly interweave all elements of the economy into one ecosystem, much of the strategy focuses on military exploitation of civilian research and development in high-technology areas. In reality, China's desire to be a technological superpower capable of competing with the United States also required the exploitation of foreign technologies to supplement knowledge gaps in domestic industries.

Under the leadership of Xi Jinping, the project of MCF has been interwoven with the promotion of Xi Jinping Thought (XJT). XJT, which was incorporated into the Party's Constitution in 2017,[51] is best understood as a political ideology that serves as "a blueprint for consolidating and strengthening power at three levels: the nation, the party and Mr. Xi himself."[52] The ideology heavily stresses the consolidation of nearly all political, social, and economic processes under the absolute leadership of the CCP, with Xi at the helm. Beijing has aggressively pushed for the widespread adoption of XJT across political, military, and civilian institutions. Several universities have established departments or institutes devoted to its study,[53] and the doctrine was made part of the national curriculum for schoolchildren by the education ministry in 2021.[54]

Military-civil fusion is no exception to this trend. The Deputy Director of the Military-Civil Fusion Office of the Heilongjiang Provincial Party Committee wrote that deep study of Xi Jinping Thought was a prerequisite to adequately implementing MCF.[55] In fact, in a status report

[47] *Xi Jinping Discusses Military-Civil Fusion: A National Strategy Concerning National Security and Overall Development*.

[48] Alex Stone and Peter Wood, *China's Military-Civil Fusion Strategy* (Aerospace Studies Institute, 2020).

[49] 习近平任主任！中央军民融合发展委员会准备做什? [Xi Jinping as Director! What is the Central Commission for Integrated Military and Civilian Development Going to Do?], 凤凰军事 (January 23, 2017).

[50] Bitzinger, *China's Shift from Civil-Military Integration to Military-Civil Fusion* at 21.

[51] John Garrick and Yan Chang Bennett, "Xi Jinping Thought": Realisation of the Chinese Dream of National Rejuvenation?, *China Perspectives* (2018).

[52] Chris Buckley, "Xi Jinping Thought Explained: A New Ideology for a New Era," *New York Times* (February 26, 2018).

[53] Tom Phillips, "Xi Jinping Thought to be Taught in China's Universities," *Guardian* (October 27, 2017); and Zhu Lvhe, *Tsinghua Establishes Institute for Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era*, Tsinghua University (2018).

[54] "China to Add 'Xi Jinping Thought' to National Curriculum," *Reuters* (August 24, 2021).

[55] 李豪岩, 以思想大解放开创军民融合发展新局面 [Create a New Phase in Military-Civil Fusion Through the Liberation of Thought], 黑龙江新闻 (2019).

on the state of military-civil fusion presented to the Central Commission, one problem the investigatory team pointed to was that the Party's "innovative theory" was not sufficiently in place.[56] The leader of the team thus suggested that learning to understand and implement Xi Jinping Thought was an important step in resolving the existing problems in the execution of MCF.

Reviewing the trajectory of military-civil fusion from a historical perspective reinforces the importance of recognizing the relatively persistent belief throughout the CCP's history that indigenous technological innovation is an essential component of national power. Erroneously assuming that military-civil integration is a novel pursuit, rather than a consistent strategic effort throughout China's political history, may lead U.S. officials to underestimate the Party's structural commitment to MCF.[57]

[56] 姜雨薇，中央第三巡视组向中央军民融合发展委员会办公室反馈巡视情况 [Report of the Third Inspection Team of the Central Committee to the Office of the Central Commission for Military-Civil Fusion Development], 中央纪委国家监委网站 (July 23, 2022).

[57] Warden, *A Revolutionary Evolution: Civil-Military Integration in China*.

4. MCF Implementation and Organization

Xi Jinping's approach to military-civil fusion introduced two key institutional innovations: (1) it provided "an ideational foundation" where actors could orient themselves toward a common goal of civilian-military integration even as they pursued their own preferences and interests when constructing policies, and (2) it improved the ability of the Party to coordinate MCF initiatives through changes to the organizational structure for implementing policy.[58] MCF under Xi Jinping also provided the much-needed "top-level design" that was lacking in earlier attempts to coordinate the defense and civilian sectors.[59]

When MCF was elevated to the level of national strategy, the Party outlined several strategic tasks: constructing infrastructure and exchanging resources; developing the domestic defense science, technology, and weapons industry; promoting innovation in science and technology through military-civil collaboration; cultivating joint training and the exchange of talent between the military and domestic enterprises; coordinating the development of social services with military logistics; and modernizing national defense mobilization while deepening integration between the military and civilians in emerging fields.[60] Xi pointed to several changes that would be necessary to complete these tasks, such as promoting the rule of law, removing barriers to civilian participation in military projects, and reforming military procurement, taxation, and pricing procedures.[61]

In 2017, the CCP established the Central Commission for Military-Civil Fusion Development,[62] which serves as the predominant decision-making body for implementing military-civil fusion.[63] The Commission is directly responsible to the Politburo and is chaired by Xi himself. It also includes several members of the Politburo and Central Military Commission, in addition to ministry-level leaders.[64]

This decision diverged greatly from the approach under Hu Jintao by moving the "coordinating authority" for MCF away from the Ministry of Industry and Information Technology and placing it under the direct supervision of the Party.[65] Among various oversight responsibilities, the Central Commission sets long and short-term objectives for pursuing integration, issues policy

[58] Aaron L. Freidberg, "Competing with China," *Survival* (2018).
[59] *Id.*
[60] 朱英, 习近平：开创新时代军民融合深度发展新局面 [Xi Jinping: Initiating a New Era of In-Depth Development of Military-Civil Fusion], 新华社 (March 2, 2018).
[61] *Id.*
[62] Bitzinger, *China's Shift from Civil-Military Integration to Military-Civil Fusion*.
[63] *Xi Jinping as Director! What is the Central Commission for Integrated Military and Civilian Development Going to Do?*
[64] *Interview with Greg Levesque.*
[65] Freidberg, *Competing with China*.

directives, and clarifies "roles and responsibilities across the government and military."[66] Several provincial and municipal governments have followed suit, establishing MCF development committees and issuing localized development plans.[67]

Military-civil fusion proposes a multi-domain approach for prioritizing development. This includes major security domains including maritime, space, and cyber, nascent technological areas such as biotechnology, new energy, artificial intelligence, and traditional domains including manufacturing, science and technology, education, social services, and emergency and public safety.[68]

Related to the traditional domains is what have been called Systems of Systems (SoS), akin to "dynamic ecosystems that operate across domains to achieve operational effects."[69] Each system is organized and implemented by a network of State Council organizations, military organs, academic and research institutions, private companies, state and military-linked enterprises, and provincial governments, among other organizations.[70]

The **Advanced Defense Science, Technology, and Industrial SoS** concentrates on promoting integration between the defense industrial base and civilian industrial manufacturing base "to transfer mature technologies" between the two sectors.[71] Key technologies under this system include aerospace, communications and transportation, and equipment and materials.

The **Military-Civil Science and Technology Coordinated Innovation SoS** prioritizes research and development in science and technology, particularly in "advanced dual-use technology."[72] Major tasks under this system include strengthening domestic innovation and research capabilities, implementing S&T "megaprojects" and programs, improving the quality of the workforce, encouraging the exchange of scientific resources, and promoting entrepreneurship.[73]

The **Fundamental Domain Resource Sharing SoS** focuses on incorporating military needs into the construction of civilian infrastructure and exploiting "China's civilian construction and logistics capacities and capabilities for military purposes."[74] Priority areas in this domain include transportation, space, information, topography, weather, and standardization infrastructures.[75]

---

[66] *Interview with Greg Levesque.*
[67] *Interview with Greg Levesque*; *Xianning City Action Plan for In-Depth Development of Military-Civil Fusion (2021-2025) (Revised Draft),* CSET (January. 11, 2022) (translated by Etcetera Language Group, Inc.); *Tianjin Municipal Action Plan for Military-Civil Fusion Special Projects in Intelligent Technology*, CSET (October 14, 2019) (translated by Ben Murphy and Lorand Laskai).
[68] Stone and Wood, *China's Military-Civil Fusion Strategy* at 30.
[69] *Id.* at 31.
[70] Maj. Gen. P K Mallick, *Military Civil Fusion in China*, Vivekananda International Foundation (August 1, 2022).
[71] *Id.*
[72] *Id.*
[73] Stone and Wood, *China's Military-Civil Fusion Strategy* at 79-81.
[74] Mallick, *Military Civil Fusion in China*.
[75] Stone and Wood, *China's Military-Civil Fusion Strategy* at 55.

The **Military Personnel (Talent) Cultivation SoS** concentrates efforts on developing military and civilian expertise in key technologies and industries. It also covers personnel and knowledge exchange between the private sector and military-defense industries.[76]

The **Socialized Support and Sustainment SoS** conceives of "two lines of effort."[77] The first looks to harness civilian resources to support military logistics functions relating to quality of life – primarily essential services like healthcare, utilities, food, and housing.[78] The second consists of constructing "a modern logistics support system capable of supporting and sustaining integrated joint operations and overseas non-war and wartime missions."[79]

Finally, the **National Defense Mobilization SoS** is concerned with building mechanisms and processes that will enable the CCP and military to mobilize all aspects of the civilian economy for national development and security.[80]

Policy Initiatives Under MCF

One relatively fruitful policy under military-civilian fusion has been government investment in key industries. The MCF Industrial Development Fund has committed billions of RMB to fund research and manufacturing initiatives across the country. Provincial and some municipal MCF offices also often have their own coffers for funding projects.[81]

For their part, Chinese enterprises have quietly invested tremendous sums of money in U.S. firms, many of which develop national security-adjacent technologies.[82] Following the financial crisis in 2008, several Chinese corporations saw an opportunity to gain access to U.S. technology by acquiring "foreign companies at a low cost."[83]

Some U.S. companies have even turned to Chinese funding in the absence of U.S. alternatives. For example, Neurala, an artificial intelligence company that provided assistance in robotics to the U.S. Air Force, received funding from "an investment firm backed by a state-run Chinese company" when the U.S. military failed to provide needed funding.[84] Other Chinese firms with connections to the government or state-owned companies have invested in U.S. start-ups working on rocket engines, sensors for navy ships, and flexible screens for fighter planes.[85]

---

[76] Mallick, *Military Civil Fusion in China*.
[77] Stone and Wood, *China's Military-Civil Fusion Strategy* at 87.
[78] Mallick, *Military Civil Fusion in China*.
[79] Stone and Wood, *China's Military-Civil Fusion Strategy* at 87.
[80] *Id.*
[81] 中共北京市委军民融合发展委员会办公室 2022 年财政预算信息 [2022 Budget Information of the Office of the Military-Civil Fusion Development Committee of the Beijing Municipal Committee of the Communist Party of China] (2022).
[82] Nathan Picarsic and Emily de La Bruyere, "Vultures at the Gate: The National Security Risk of Silicon Valley Bank's Failure," *The Hill* (March 17, 2023).
[83] Emily de La Bruyere and Nathan Picarsic, *When the Iron is Hot: The Chinese Communist Party's Subversion of US Recovery Investment*, Horizon Advisory (2020).
[84] Paul Mozur and Jane Perlez, "China Bets on Sensitive U.S. Start-Ups, Worrying the Pentagon," *New York Times* (March 22, 2017).
[85] *Id.*

(Funding has also flowed from American companies to China – Chinese subsidiaries of American venture capital firms, for example, have invested heavily in Chinese space startups.[86])

Provincial governments play an important role in implementing MCF on the ground, developing specific strategies for their own regions. This will often take the form of government funding for industry projects or facilitating the construction of industrial MCF bases. Sichuan Province, which had been appointed a pilot area for testing innovation and reform in 2015, signed an agreement with a number of military enterprises in 2017 to establish an MCF "industrial cluster," with the aim of creating an environment more conducive to designing and executing MCF projects.[87] In 2018, the province raised nearly 12 billion yuan to fund MCF initiatives and engaged 29 companies in MCF programs.[88] In the same year, Shandong built an MCF investment fund of 10 billion yuan.[89]

Another feature of MCF in China has been the establishment of alliances, organizations, and institutions that provide a venue for government, military, industry, university, and other research personnel to meet and engage in joint collaboration. The China Military-Civil Fusion Innovation Alliance established in Beijing was an early iteration of this type of forum, bringing government and military leaders together with several state-owned enterprises.[90]

Construction of MCF industrial innovation centers, bases, or zones has also been a preferred strategy of the Chinese government. These areas generally serve specific industries and act as central locales for the cross-exchange of resources, talent, training, and expertise between private firms, military organs, and state-owned enterprises.[91] Typically, the zones are "anchor[ed]" around a state-owned defense enterprise and then an "ecosystem" is formed around it.[92]

There is no statute or law in China that mandates companies to participate in military-civil fusion.[93] While some laws, such as the National Intelligence and Counter-espionage Laws, do obligate Chinese citizens and organizations to cooperate with the government and Party to support national security and national interests,[94] there is little evidence that China has used these laws to obligate civilian participation in MCF.[95] The CCP is likely reluctant to use coercive methods to

[86] Aria Alamalhodaei, "As Tensions Build, Silicon Valley's Chinese Affiliates Invest in Sensitive Space Tech," *TechCrunch* (March 2, 2023).

[87] 陆茜, 四川将建军民融合产业集群 [Sichuan Will Build a Military-Civil Fusion Industrial Cluster], 新华社 (March 10, 2017).

[88] *Id.*

[89] 雷丽娜, 山东设立军民融合产业基金 总规模 100 亿元 [Shandong Sets Up a 10 Billion Yuan Military-Civil Fusion Industry Fund], 新华社 (March 28, 2023).

[90] 千帆, 中国军民融合协同创新联盟在北京成立 [The China Military-Civil Fusion Innovation Alliance is Established in Beijing], 中国新闻网 (March 21, 2017).

[91] *Interview with Greg Levesque*.

[92] *Id.*

[93] Kania and Laskai, *Myths and Realities of China's Military-Civil Fusion Strategy*.

[94] *China's Cyber Laws and Regulations*, Margin Research (January 30, 2023).

[95] Kania and Laskai, *Myths and Realities of China's Military-Civil Fusion Strategy*.

entice participation by private enterprises, as disgruntled firms could easily sabotage military projects with poor performance or leak confidential information.

The Role of Universities

Universities sit at the heart of China's military-civil fusion strategy.[96] Like those in the U.S., academic institutions play a foundational role in research and development of dual-use and emerging technologies and cultivate talent that can be recruited to participate in military-related enterprises. As a result, the Chinese government has invested heavily in improving the quality of China's university system, and schools are expected to be at the "forefront" of MCF.[97]

Academic links to China's military and defense industry run deep. Several universities "have launched their own platforms for MCF" or established joint programs for defense-related research.[98] As of 2009, the PLA and the State Administration for Science, Technology and Industry for National Defense (SASTIND) supervised around 74 national defense science and technology key laboratories, 39 of which were located in civilian universities.[99] In addition, 36 national defense key discipline labs and 53 Ministry of Education defense labs operate out of nonmilitary universities.[100]

Some academic institutes have taken a more direct role in supporting military initiatives. Several offensive cyber-attacks attributed to Chinese actors have been traced back to professors or students at universities.[101] Colleges in China have also facilitated the creation of several MCF innovation centers and zones. The Academy of Military Science, for example, helped establish the Tianjin Artificial Intelligence Military-Civil Fusion Innovation Center.[102] Wuhan University and Huazhong University jointly built the National Cybersecurity School at the National Cybersecurity Talent and Innovation Base.[103]

Notably, overseas universities have, perhaps unwittingly, played a role in the PLA's modernization effort. ASPI estimates that between 2007 and 2017, the PLA sent over 2,500 military scientists – some undercover – to foreign universities to gain skills and knowledge through training or work.[104]

---

[96] Manoj Joshi, *China's Military-Civil Fusion Strategy, the US Response, and Implications for India*, Observer Research Foundation (2022).

[97] 赵长禄, 大学应站在军民融合的前线 [Universities Should Be at the Forefront of Military-Civil Fusion], 人民日报 (March 14, 2017).

[98] Kania and Laskai, *Myths and Realities of China's Military-Civil Fusion Strategy*.

[99] Alex Joske, *The China Defence Universities Tracker* (Barton: Australian Strategic Policy Institute, November 25, 2019).

[100] *Id.*

[101] Dave Aitel et. al, *China's Cyber Operations: The Rising Threat to American Security*, (New York: Margin Research, August 2022).

[102] Kania, *In Military-Civil Fusion, China is Learning Lessons from the United States and Starting to Innovate*.

[103] Dakota Cary, *China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain*, CSET (July 2021).

[104] Alex Joske, *The China Defence Universities Tracker*, ASPI (November 25, 2019).

Challenges for Implementation

Party leadership has stressed the desire to "strengthen unified leadership, top-level design, reform, and innovation" as part of MCF.[105] But implementing this kind of coordinated effort has been "messier" in reality – policies can be applied inconsistently despite attempts to impose standardization across the board, and the administrative architecture necessary to enforce consistency has not yet been sufficiently realized.[106] Entrenched and sluggish institutional mechanisms also inhibit the realization of a more unified top-down approach. Military-civil fusion suffers from many of the same problems as other top-down tactics attempted by the CCP: corruption, insufficient regulatory mechanisms, poor coordination in leadership, etc.[107]

China's authoritarian system may afford advantages that benefit its approach to MCF.[108] The Chinese government is likely able to funnel investment funds into MCF projects more easily than the United States, which must first pass through several bureaucratic hoops.[109] Some have argued that Beijing's ability to leverage a "whole of society" approach with greater directness than the United States has also benefited the PRC, insofar that China be empowered to take a more deliberate approach to developing its military-civilian industrial complex.[110]

It is essential, however, not to overestimate the Party's ability to unilaterally impose its will on cadres and local governments across the country. China's political system has been aptly described as "fragmented authoritarianism," insofar that while the CCP may dictate the boundaries of its national directives, it is local governments that develop policy on the ground.[111] This style of governance, in which "policy processes in China are more of a negotiation than coercion, and more incremental than sweeping" has been enormously successful for China's economic development by allowing actors to adapt centrally imposed policies to local conditions.[112]

It remains to be seen whether military-civil fusion will play out in the same way. At the moment, although involvement with MCF by private enterprises has been rising, the proportion of participating firms in comparison to the total number of enterprises in China's technology sector appears low.[113] References to MCF in official government documents also appear to be declining.[114] The initiative does seem to have been more successful in the academic sector, with "several hundred Chinese universities" accepting funding, educating military students, conducting

[105] 习近平在中国共产党第十九次全国代表大会上的报告 [Xi Jinping's report at the Chinese Communist Party 19th National Congress], China.com.cn (October 27, 2017), cited in Kania and Laskai, *Myths and Realities of China's Military-Civil Fusion Strategy*.
[106] Kania and Laskai, *Myths and Realities of China's Military-Civil Fusion Strategy*.
[107] *IntelBrief: China's Military-Civil Fusion Strategy*, The Soufan Center (August 13, 2020).
[108] Kania and Laskai, *Myths and Realities of China's Military-Civil Fusion Strategy*.
[109] *Id.*
[110] Freidberg, *Competing with China*.
[111] Yuen Yuen Ang*, How China Escaped the Poverty Trap*, (Ithaca: Cornell University Press, 2016), pp. 73-102, *cited in* Freidberg, *Competing with China*.
[112] Freidberg, *Competing with China* at 7.
[113] Kania and Laskai, *Myths and Realities of China's Military-Civil Fusion Strategy*.
[114] *How Should the U.S. Respond to China's Military-Civil Fusion Strategy?*, ChinaFile (May 22, 2021).

military-adjacent research, and establishing a variety of joint ventures with private defense companies, other research institutions, or military organs.[115]

[115] Kania and Laskai, *Myths and Realities of China's Military-Civil Fusion Strategy*.

5. Key Domains and Industries

While China's leadership aspires for MCF to be implemented throughout the entire Chinese economy, MCF's development strategy emphasizes three major security domains: maritime, space, and cyberspace.[116] Emerging technologies in energy, artificial intelligence, quantum computing, and biotechnology are also critical industrial focuses.[117] Importantly, investment in industries and technologies where China lags behind other countries, such as semiconductors, can help maintain the infrastructure and institutions necessary to give domestic enterprises time to catch up to their foreign counterparts.[118]

Cyber and Information Technologies

The Central Cyberspace Affairs Commission once published an article by the Deputy Director of the War and Crisis Response Training Center at the National Defense University, in which he referred to network information technology as the "frontier" of military-civil fusion in China.[119] Pointing to the improving offensive cyber capabilities in countries like Russia and China, the increase in espionage activities conducted through cyberspace, and the danger of internal leaks to the military's information network, he posited that military-civil fusion was an essential requirement for the security of China's cyberspace.[120]

China has been keenly aware that developments in cyber and information technologies have not only become a driving force in economic development but have also fueled military competition across the globe. The integration of these technologies into nearly every aspect of life has made cyberspace security critical not only for the military, but for ordinary civilians as well. Deploying MCF to exploit infrastructure, talent, and resources in both defense and civilian sectors is therefore an obvious step in meeting the security needs of both the people and the military: "joint defense, joint insurance, joint management, and joint control."[121]

Moreover, most innovation and expertise in cyber has been concentrated in the private sector, but the knowledge and technologies generated by commercial enterprises have strong potential for application in the military context. Areas of interest for cyber under MCF include communications infrastructure, electromagnetic management technology, cybersecurity,

[116] Mallick, *Military Civil Fusion in China*.
[117] *Id.*; Elsa Kania and Wilson VornDick, *China's Military Biotech Frontier: CRISPR, Military-Civil Fusion, and the New Revolution in Military Affairs*, China Brief (2019).
[118] Bradford Waldie, *How Military-Civil Fusion Steps Up China's Semiconductor Industry*, DigiChina (April 1, 2022).
[119] 李明海,网络信息体系军民融合战略的思考 [Thoughts on the Military-Civil Fusion Strategy for Network Information Systems], 网络传播杂志 (November 12, 2018).
[120] *Id.*
[121] *Id.*

electronic intelligence, and integrating space-terrestrial information networks.[122] For the military, the private cyber industry is also an important source of talent for recruitment.

Several industry partners have entered into joint ventures to advance research and development in information technologies. CETC and Baidu established a joint laboratory for intelligent command and control technology, with the goal of advancing new applications in computing, data, and other information technologies.[123] Qihoo 360, one of China's largest private cybersecurity companies, entered into a cooperative agreement with the SASTIND to promote MCF and the development of network security for the national defense technology industry.[124] Qihoo 360's CEO referred to cyberspace as a "strategic highland" for MCF, and he promised to transfer "the most advanced" technical capabilities to the national defense industry for network security, all while serving as a model for MCF in cyberspace.[125]

Chinese tech companies have increasingly taken steps to demonstrate closer ties to the CCP, but this may be an attempt to appease the Party's wariness towards tech firms, which have come under fire for a variety of reasons in the last few years, e.g., for failing to protect data privacy, promoting vulgar content, and labor violations.[126] Didi, which operates China's predominant ride-hailing app, committed to hiring a thousand people belonging to the CCP after facing harsh scrutiny when a female rider was murdered by one of its drivers.[127] Similarly, ByteDance and Tencent promised to hire thousands of content reviewers after being reprimanded for promoting "vulgar content" on their platforms.[128]

Maritime

China's military shipbuilding sector benefited greatly from China's push toward civil-military integration in the period between 1997 and 2017.[129] Not only has China improved ship design and streamlined construction processes, but they have also modernized operations, constructed several dry docks, and increased shipbuilding capacity.[130] China now controls "the world's second-largest shipping fleet" and dominates the maritime supply chain.[131]

---

[122] *NIDS China Security Report 2021: China's Military Strategy in the New Era* at 68.

[123] 栾永胜, 中国电科 28 所与百度公司成立"智能指挥控制技术联合实验室" 推动军民融合向新技术领域纵深迈进 [CETC's 28th Institute and Baidu Established the Joint Laboratory for Intelligent Command and Control Technology to Promote Military-Civil Fusion In New Technology Fields], Sohu (January 1, 2023).

[124] 国防科工局信息中心与 360 企业安全签署战略合作协议 [The State Administration for Science, Technology and Industry for National Defense and Qihoo 360 Signed A Strategic Cooperation Agreement], 环球网 (Apr. 19, 2022).

[125] *Id.*

[126] Pham, *Why China's Tech Giants are Cozying Up to the Communist Party*.

[127] *Id.*

[128] *Id.*

[129] Bitzinger, *China's Shift from Civil-Military Integration to Military-Civil Fusion* at 17.

[130] *Id.*

[131] Jude Blanchette, Jonathan E. Hillman, Maesea McCalpin, and Mingda Qiu, *Hidden Harbors: China's State-backed Shipping Industry*, (Washington: CSIS, July 2020).

China views modernizing its navy as an essential element of becoming a global power. Investing in intelligent shipbuilding projects was one of the first priorities of MCF, and government officials saw "smart ocean engineering" as an illustration of a "model" military-civil fusion project.[132] Shipping "is a core pillar of China's approach to power projection," and, consequently, the military maintains close ties with shipping enterprises.[133] For example, the state-owned company, COSCO Shipping, which owns one of the world's largest shipping fleets, has founded a research center in the Qingdao Military-Civil Fusion Innovation Demonstration Zone.[134]

Since merging its military and commercial shipyards together, China has become "the world-leader in shipbuilding"[135] and is responsible for approximately 41% of global production.[136] China State Shipbuilding Corporation (CSSC) alone has a 21.5% share of the global shipbuilding market.[137] Some 32% of trade traveling through global ports passes through China, and state-owned enterprises control "18 percent of the world's container line capacity, around 13 percent of the world's LNG shipping capacity, and 12 percent of the world's crude oil carrier capacity."[138] Several state-owned enterprises have also invested in ports around the globe, with ownership in at least 60 countries, including Germany, Israel, Angola, Mauritania, and Greece.[139]

China, however, remains dissatisfied with domestic innovation in the sector[140] and looks to enterprises like the CSSC to act as "a linchpin" in fusing together China's commercial maritime activities with the PLA's naval modernization project.[141] CSSC shipyards, for example, may one day host a container ship from France[142] and the next day launch a PLA amphibious assault ship.[143] (In 2021, the PLA commissioned "eight guided-missile destroyers, two amphibious assault ships and one nuclear-powered ballistic missile submarine" from CSSC.)[144] Perhaps alarming, foreign

[132] 姜晨, 工信部：把智慧海洋工程做成典型的军民融合工程 [Ministry of Industry and Information Technology: Make Smart Ocean Engineering a Model Military-Civil Fusion Project], 工业和信息化部网站 (April 13, 2018).
[133] Nathan Picarsic and Emily de La Bruyere, "Insuring Against Military-Civil Fusion Risks," *RealClear Defense* (February 10, 2022).
[134] *Id.*
[135] *Foreign Orders Boost China Shipbuilding Firm Linked to Military*, Al Jazeera (May 17, 2022).
[136] Jonathan Holslag, *Every Ship a Warship: The Security Role of China's Maritime Sector and its Consequences for Europe* (2022).
[137] Matthew P. Funaiole, Brian Hart and Joseph S. Bermudez Jr., *In the Shadow of Warships: How Foreign Companies Help Modernize China's Navy*, (Washington: CSIS, 2022).
[138] Holslag, *Every Ship a Warship* at 2-3.
[139] Elisabeth Braw, *Countries Wary of China Need Patriotic Investment Plans*, Foreign Policy (November 1, 2022); John Xie, *China's Global Network of Shipping Ports Reveal Beijing's Strategy*, VOA (September 13, 2021).
[140] *Id.*
[141] Funaiole, Hart and Bermudez, *In the Shadow of Warships*.
[142] *Id.*
[143] Jr Ng, "China's CSSC Launches Third Type 075 Amphibious Assault Ship," *Asian Military Review* (February 3, 2021).
[144] McGerty and Nouwens, *A Strong 2021 for China's Defence Companies*.

companies have been eager to purchase ships, exchange technology, and enter into joint ventures with CSSC.[145]

Other maritime interests under MCF include constructing deep-sea testing facilities, improving underwater measuring and data-transmission technologies, building deep-sea stations and nuclear power offshore platforms, manufacturing deep-sea monitoring equipment, and developing resources and equipment for use in polar regions. [146]

Aerospace and Aviation

Space technologies and the use of space are key areas of focus for MCF.[147] The industry is dominated by state-owned enterprises: China Aerospace Science and Technology Corporation (CASC), the Aviation Industry Corporation of China (AVIC), and the China Aerospace Science and Industry Corporation (CASIC) are among the "top 10 military-industrial complex conglomerates" in China. [148] AVIC, CASIC, and CASC also topped the list of global defense companies when ranked by revenue, sitting respectfully in 6th, 11th, and 18th place.[149]

While access to the space industry in China was previously limited to state-owned enterprises, Beijing began allowing private investment in the sector in 2014.[150] Accompanying this change, the General Armament Department of the PLA introduced a number of policies to encourage private companies to participate in defense procurement, including "simplifying licensing procedures, improving pricing mechanisms, and reforming procurement systems and tax policies for military equipment."[151] Both the central and provincial governments have developed specific MCF funds that target investment in aviation and aerospace.

These policies appear to be having an effect. As of 2018, there were 141 aerospace enterprises registered in China: "36 satellite manufacturing enterprises; 22 launch vehicle manufacturing enterprises; 39 satellite operation enterprises; and 44 satellite applications enterprises."[152]

Under the banner of MCF, both the Chinese military and government have provided critical support to aerospace firms by sharing expertise, talent, and funding.[153] Enterprises participating in established MCF Zones that focus on aviation and aerospace, such as the Shanghai Minhang

[145] Funaiole, Hart and Bermudez, *In the Shadow of Warships*.
[146] *NIDS China Security Report 2021: China's Military Strategy in the New Era*, NDS (2021), http://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2021_A01.pdf.
[147] *NIDS China Security Report 2021: China's Military Strategy in the New Era.*
[148] Cheng Li, *China's Military-Civil Fusion: Objectives and Operations, China-US Focus* (August 30, 2022).
[149] *Defense News Top 100*.
[150] *NIDS China Security Report 2021: China's Military Strategy in the New Era.*
[151] Andrew W. Hull, David R. Markov and Eric Griffin, *"Private" Chinese Aerospace Defense Companies*, (China Aerospace Studies Institute (2021).
[152] *NIDS China Security Report 2021: China's Military Strategy in the New Era.*
[153] *NIDS China Security Report 2021: China's Military Strategy in the New Era* at 55.

National MCF Zone, receive several benefits, such as certification as a defense contractor, and may sometimes receive some form of subsidies.[154]

State-owned enterprises, Party organs, and government ministries have generally transferred technologies to commercial aerospace firms "to promote innovation in dual-use technology."[155] While many of these private companies are in the early stages of development, there has been comparatively little technological transfer back to the military at this point in time.

Likewise, a report from the Shanghai government in 2021 stated that "China's commercial aviation industry is lagging behind international competitors," alleging that MCF was in fact "stifling innovation" in aviation.[156] The report pointed to persistent barriers inhibiting civilian participation in military initiatives and suggested that the "state dominance of the industry and institutions" has held back "collaborative research and development."[157]

Despite these tensions, the commitment to pursuing growth in aerospace and aviation is clear. [158] In particular, China's competitive ambitions in space are quite apparent. It was recently revealed, for example, that PLA scientists are heading a project that will deploy thousands of satellites built by China Satellite Network Group – another state-owned enterprise[159] – in a bid to "suppress" SpaceX's Starlink network.[160] The State Council has also expressed interest in projects involving "large carrier rockets, nuclear power facilities, deep-space exploration, in-orbit servicing, and maintenance systems."[161]

Artificial Intelligence

Given China's belief that the military's future lies in intelligentized warfare, artificial intelligence and quantum technology have been another domain of interest for military-civil fusion. Both technologies were emphasized as priorities in the 2017 Science and Technology Military-Civil Fusion Special Projects Plan.[162] Similarly, the AI Development Plan issued in the same year called for the "two-way transfer of military and civilian scientific and technology achievements," with an emphasis on applying AI technology for defense purposes.[163] It also encouraged civilian scientists to participate in defense-related research.

From this perspective, the primary focus for MCF appears to be operationalizing artificial intelligence for military applications and integrating it into other technologies, systems, and

[154] *Interview with Greg Levesque*
[155] *Id.* at 56.
[156] Amanda Lee, *China's aviation capabilities stuck at 'low-end' as military-civil fusion weighs on innovation: official report*, SCMP (April 16, 2021).
[157] *Id.*
[158] *Id.*
[159] Tracy Qu, *China's New Bid to Take on Elon Musk's Starlink: A State-Owned Satellite Enterprise*, SCMP (May 9, 2021).
[160] Stephen Chen, *China Aims to Launch Nearly 13,000 Satellites to 'Suppress' Elon Musk's Starlink, Researchers Say*, SCMP (February 24, 2023).
[161] *NIDS China Security Report 2021: China's Military Strategy in the New Era* at 68.
[162] Kania, *In Military-Civil Fusion, China is Learning Lessons from the United States and Starting to Innovat*e.
[163] Mallick, *Military Civil Fusion in China*.

processes.[164] Beijing also sees investment in artificial intelligence as an opportunity to "leapfrog" the U.S. military.[165] Notably, China has signaled a willingness to take the lead in establishing international norms governing artificial intelligence. In 2021, its ambassador submitted the country's first proposal to the UN to regulate the military applications of AI.[166]

Since 2017, China has launched a number of open innovation platforms "to advance AI development." [167] Led by industry leaders, such as Baidu, Alibaba, Tencent, iFlytek, and SenseTime, these platforms have provided collaborative spaces for enterprises to experiment with applying artificial intelligence to a variety of uses, including "driving, smart cities, medicine, smart voice, and intelligence perception."[168]

While the U.S. has generally maintained an edge over China in AI technologies, the gap between U.S. and Chinese capabilities may be narrowing. Some have argued that China is likely to edge ahead of the United States within the next year in applying AI to products and services.[169] In one potent example, in the U.S. Department of Commerce's National Institute of Standard and Technology's ranking of companies by the accuracy of their facial recognition technology, the top five companies are all Chinese.[170] If, however, Baidu's response to ChatGPT is representative of the rest of the domestic AI industry, U.S. counterparts appear to remain ahead for now.[171]

Semiconductors

Although China's domestic semiconductor production still lags behind other countries, efforts under MCF to support private enterprises help provide an environment in which domestic semiconductor manufacturing can advance military needs and industry growth.[172] In particular, Waldie notes that despite the fact that there remains little indigenous innovation in China's semiconductor industry, MCF has helped "prop-up" globally uncompetitive companies that are critical to the PLA.[173]

This lifeline gives companies enough time to acquire the necessary expertise and capacity to survive global competition. Sustaining domestic semiconductor production reduces China's reliance on foreign chips, increasing the country's resilience to fluctuations in foreign supply. This also allows Beijing to reserve some autonomy in response to foreign sanctions or overseas attempts to limit Chinese access to key technologies.

---

[164] Elsa B. Kania, *Chinese Military Innovation in Artificial Intelligence*, (Washington: CNAS, June 7, 2019).
[165] Waldie, *How Military-Civil Fusion Steps Up China's Semiconductor Industry*.
[166] *China Submits Position Paper on Regulating Military Applications of AI*, Xinhua (December 14, 2021).
[167] Kania, *Chinese Military Innovation in Artificial Intelligence*.
[168] *Id.*
[169] Craig S. Smith, *China's AI Implementation Is Edging Ahead Of The US*, Forbes (January 14, 2023).
[170] *FRVT 1:1 Verification*, NIST (2022), https://pages.nist.gov/frvt/html/frvt11.html.
[171] Rita Liao, *China's ChatGPT Rival Baidu Ernie is off to a rough start*, TechCrunch (March 16, 2023).
[172] Waldie, *How Military-Civil Fusion Steps Up China's Semiconductor Industry.*
[173] *Id.*

6. Expert Opinions

Experts familiar with China's strategy of military-civil fusion disagree on the nature and extent of a "proper response" from the United States and its allies. Elsa Kania and Lorand Laskai argue that MCF is still in its nascent stage and that the success of the strategy remains "difficult to evaluate."[174] The PLA has historically been "cordoned off from… the dynamic high-tech commercial economy," and confidentiality and licensing requirements remain "significant hurdles" to enterprises hoping to coordinate with the military.[175]

Attempts at reform have run afoul of entrenched practices, and structural features of the military-industrial complex – such as the monopolization of industries by state-owned enterprises – have impeded efforts to encourage collaboration. Importantly, Xi Jinping's desire to develop the rule of law and public accountability mechanisms to undergird MCF is constrained by China's typical difficulty in the area – namely, the tension between the Party's desire to exert central control and the need to establish an independent regulatory system to implement the rule of law. As such, MCF's goals of civilian-military integration will likely take substantial effort and time to achieve progress, despite some initial achievements.

Given this, Kania and Laskai caution against turning MCF into a bogeyman and suggest that the U.S. should develop a "highly targeted" response, which "accounts for the complexities of international cooperation and competition in science, technology, and innovation."[176] Exactly what such a response might entail remains to be seen.

In contrast, Christian Brose, former staff director of the Senate Armed Services Committee, emphasizes that there has been significant evidence that the progression of China's warfighting capabilities has outpaced predictions over the last two decades.[177] Emily Weinstein, a research analyst at the Center for Security and Emerging Technology, argues that even if MCF has fallen short of Beijing's lofty aspirations, it is important to evaluate the strategy within the broader context of China's actions. According to Weinstein, the U.S. has already taken a "targeted, nuanced, and evidence-based" approach, but MCF is a "moving target" that requires constant attention to "changing dynamics and evolution."[178]

As of 2021, Tai Ming Cheung, the director of the University of California Institute on Global Conflict and Cooperation, thinks that the U.S. still needs to get "the Western analytical house in order" before committing to any response to MCF.[179] According to Cheung, MCF is still

[174] Kania and Laskai, *Myths and Realities of China's Military-Civil Fusion Strategy*.
[175] *Id.*
[176] *Id.*
[177] Emily Weinstein, *Don't Underestimate China's Military-Civil Fusion Efforts*, Foreign Policy (February 5, 2021).
[178] *Id.*
[179] *How Should the U.S. Respond to China's Military-Civil Fusion Strategy?*, ChinaFile (May 22, 2021).

in its early stages, and current research has failed to illuminate a sufficiently comprehensive understanding of what the strategy is, how it works, and how it compares to other countries. He also notes that use of the term MCF has somewhat fallen out of favor by Chinese authorities in recent years.[180]

Leo Carter, Director at Rice, Hadley, Gates & Manuel, and Anja Manuel, Co-Founder, argue that the U.S. should focus on its own innovation policies, rather than fixating on China's agenda.[181] Overreacting to MCF in the wrong ways will be counter-productive to U.S. goals. Peter Wood, program manager at BluePath Labs, agrees that the U.S. should focus on investing more heavily in its own competitiveness.[182]

[180] *Id.*
[181] *Id.*
[182] *Id.*

References

Bateman, Jon, *Maintaining a Military Edge Over China - U.S.-China Technological "Decoupling": A Strategy and Policy Framework.* (Carnegie Endowment for International Peace, April 25, 2022)

Bitzinger, Richard A., "China's Shift from Civil-Military Integration to Military-Civil Fusion," *Asia Policy* (2021)

Bitzinger, Richard, *Civil-Military Integration and Chinese Military Modernization*, (Asia-Pacific Center for Security Studies, December 2004)

Bruyère, Emily de La and Nathan Picarsic, *Defusing Military-Civil Fusion* (Foundation of Defense of Democracies, May 27, 2021).

Cheung, Tai Ming and Eric Anderson, *Chinese Defense Industry Reforms and Their Implications for US-China Military Technological Competition,* (SITC Research Briefs, 2017)

Cheung, Tai Ming, *Innovate to Dominate: The Rise of the Chinese Techno-Security State* (Ithaca: Cornell University Press, 2022)

Department of State, *Military-Civil Fusion and the Peoples Republic of China* (May 2020)

Evron, Yoram, "China's Military-Civil Fusion and Military Procurement," *Asia Policy* (January 2021)

Fritz, Audrey "At the Nexus of Military-Civil Fusion and Technological Innovation in China". *The Diplomat*. (July 14, 2021)

Fritz, Audrey. *China's Evolving Conception of Civil-Military Collaboration,* (Washington: Center for Strategic and International Studies. August 2, 2019)

Fritz, Audrey, "The foundation of innovation under military-civil fusion: The role of universities" *Synopsis* (October 8, 2021)

Grevatt, Jon, "China launches 'deregulation trial' for private sector defence contractors". *Janes* (June 23, 2021)

"How Should the U.S. Respond to China's Military-Civil Fusion Strategy?" *China File* (May 22, 2021)

Interview with Greg Levesque, Commercialized Militarization: China's Military-Civil Fusion Strategy, NBR (June 30, 2021)

Kania, Elsa B., "*In Military-Civil Fusion, China is Learning Lessons from the United States and Starting to Innovate*," *The Strategy Bridge* (August 27, 2019)

Kania, Elsa B., *Military-Civil Fusion, China is Learning Lessons from the United States and Starting to Innovate,* (Washington: Center for a New American Security, August 27, 2019)

Kania, Elsa and Lorand Laskai, *Myths and Realities of China's Military-Civil Fusion Strategy* (Washington: Center for a New American Security, January 28, 2021)

Laskai, Lorand, *Civil-Military Fusion: The Missing Link Between China's Technological and Military Rise* (New York: Council on Foreign Relations, January 29, 2018)

Levesque, Greg, "Military-Civil Fusion: Beijing's "Guns and Butter" Strategy to Become a Technological Superpower". *China Brief* (October 8, 2019)

Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China, Annual Report to Congress* (2021)

Stone, Alex and Peter W. Singer, "China's Military-Civil Fusion Strategy: What to Expect in the Next Five Years". *Defense One* (February 18, 2021)

Weinstein, Emily, "Don't Underestimate China's Military-Civil Fusion Efforts," *Foreign Policy* (February 5, 2021)

Weinstein, Emily, S., *Testimony before the U.S.-China Economic and Security Review Commission on "U.S. Investment in China's Capital Markets and Military- Industrial Complex,"* (CSET, March 19, 2021)

Yang, Zi *China's Military-Civil Fusion Strategy: Development, Procurement, and Secrecy* (National Bureau of Asian Research, January 28, 2021)

Yang, Zi, "Opening Up While Closing Up: Balancing China's State Secrecy Needs and Military-Civil Fusion," *Asia Policy* (January 2021)

Yujia, He, *How China is preparing for an AI-powered Future,* (Washington: The Wilson Center, 2017)