May 2024

Commercial Enablers of China’s Cyber-Intelligence and Information Operations

Ethan Mansour  
*Virginia Tech*, ethanm03@vt.edu

Victor Mukora  
*Virginia Tech*, victor19@vt.edu

Follow this and additional works at: [https://digitalcommons.usf.edu/mca](https://digitalcommons.usf.edu/mca)

Part of the Computer and Systems Architecture Commons, Computer Law Commons, Digital Communications and Networking Commons, Intellectual Property Law Commons, International Relations Commons, Military, War, and Peace Commons, National Security Law Commons, and the Other Computer Engineering Commons

**Recommended Citation**

Mansour, Ethan and Mukora, Victor (2024) "Commercial Enablers of China's Cyber-Intelligence and Information Operations," *Military Cyber Affairs*: Vol. 7 : Iss. 1 , Article 1. Available at: [https://digitalcommons.usf.edu/mca/vol7/iss1/1](https://digitalcommons.usf.edu/mca/vol7/iss1/1)

This Article is brought to you for free and open access by the Open Access Journals at Digital Commons @ University of South Florida. It has been accepted for inclusion in Military Cyber Affairs by an authorized editor of Digital Commons @ University of South Florida. For more information, please contact digitalcommons@usf.edu.
Commercial Enablers of China's Cyber-Intelligence and Information Operations

Cover Page Footnote
This publication was supported by Award Number SA10012022020481 from the Griffis Institute for the VICEROY program. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the sponsor.

Erratum
Removed duplicate page numbers on web version.
Introduction

The Federal Bureau of Investigations (FBI) Director Christopher Wray stated, “The greatest long-term threat to our nation’s information and intellectual property, and our economic vitality, is the counterintelligence and economic espionage threat from China” [1]. Furthermore, former Commander of U.S. Cyber Command (USCYBERCOM), General Paul Nakasone, noted, “China is a challenge unlike any other we have faced. I have therefore created a China Outcomes Group under joint USCYBERCOM and National Security Agency (NSA) leadership to ensure proper focus, resourcing, planning, and operations to meet this challenge” [2].

The People’s Republic of China (PRC) Grand Strategy – a proposal that centers on China’s foreign policy objectives and the actions necessary to achieve them—emphasizes a whole-of-government approach [3]. United States citizens and government leaders rightly display skepticism of PRC-affiliated companies, as evidenced by the backlash of TikTok, the ban on Huawei infrastructure, and President Biden’s recent calls to shore up infrastructure vulnerabilities [4,5] materially. Most recently, Christopher Wray warned that the “PRC uses [Artificial Intelligence] AI—built in large part on stolen innovation and stolen data—to improve its hacking operations, including to steal yet more AI tech and data [6].” This emphasizes that PRC cyber operations continue to focus on exploiting foreign information and technology. Consequently, a cold war is waged through cyber and intelligence operations instead of the traditional battlefield. This shadowy campaign has entered a new phase, directed by institutional strategies that expand the use of commercial enablers to target domestic American populations especially [1]. These strategies have enabled various commercial enablers to hijack critical information and conduct cyber-intelligence operations that target sensitive U.S. persons, businesses, and information hubs.

Context: PRC Institutional Influence

The Chinese Communist Party’s (CCP) leadership has historically managed its strategic goals through top-down institutional campaigns. Initiatives such as Military-Civil Fusion (MCF) and the Thousand Talents Program (TTP), which expand commercial control and access, reflect this. Most evident, however, are the
mandates of Chinese national law, Article 6 of the National Intelligence Law, which ensure influence over organizations and individuals [7].

Military-Civil Fusion (MCF) targets third parties and government-adjacent organizations. Because the MCF integrates corporate projects with military research and development (R&D), they can develop dual-use technology and import intellectual property [8]. This is especially true with export-heavy telecommunications, multi-media, critical infrastructure, and electronics industries.

The Thousand Talents Program’s (TTP) [9] primary objective is to recruit those engaged in research within foreign countries (both public and private sectors). Naturally, this program enables the PRC to commit intellectual property theft on a large scale. A senate report recently identified that American taxpayer-funded research has helped China rapidly become a global power within the last twenty years [10]. The PRC’s access to leading world experts and institutions has aided their rise while encouraging more brazen abuse of foreign Research & Development (R&D) [10]. A prime example was the theft of the F-35 Joint Strike Fighter design, which a PRC-owned company, Shenyang Aircraft Corporation, used to develop the J-31, which is very similar to the F-35 [11].

Most notably, however, the PRC makes use of national and constitutional law to mandate and coerce any company or citizen of Chinese origin [12]. These laws mandate political appointments to executive staff and that all Chinese companies and persons share information with the CCP [13], [12]. This enables the Chinese government to not only take control of core businesses in China but also strictly enforce favorable viewpoints of the CCP [14].

Types of PRC Commercial Enablers

The PRC uses a spectrum of commercial enablers to position and launch information and cyber-intelligence operations to hold US persons, technology, and information capabilities at risk. However, distinct cyberspace, intelligence, and information operations should be related as cooperative capability areas [15]. While cyberspace operations focus on activities within the computer systems and networks, the purpose (and increasingly, the effect) of these operations is often to impact information resources and decision-making. Furthermore, activities in this space rely upon critical intelligence, often cyber-related, throughout the operational life cycle. This reality has become more evident as 21st-century information technologies advance toward accessibility and increased human-system of systems connectivity. Companies, not bureaucratic and monolithic governments, lead this evolution in technology and present a decisive front for the conduct of these operations.

The PRC’s network of commercial enablers can be separated into three broad categories: Direct, Subsidiary, and At-Risk. The first category comprises companies that national leadership directs, often gathering intelligence from and releasing targeted information against specific domestic, foreign, and American
populations. These groups are frequently linked to PRC intelligence agencies or have CCP members within their top leadership and organizational structure. Some examples we identified include corporations like ByteDance, Huawei, I-Soon, and Dahua. These groups are headquartered in China, which means they must abide by the established National Security Law [12], including handing over all data and technology in possession. This means that various data—code, meta, and personal—can be collected on applications and users abroad for analysis and eventual use by PRC agencies. These companies are also becoming critical cyber terrain for the macro-ingestion of global data. Recent leaks of I-Soon's intelligence operations corroborate this. [16]

The second group, “Subsidiary enablers,” are companies—often foreign in origin—that are significant, majority, or wholly owned by Chinese parent companies. Prime examples include Motorola, which Lenovo, a Chinese-based company, owns; TikTok, which ByteDance owns; and Temu, which PDD Holdings owns. The headquarters of these subsidiary companies reside outside China. However, since the parent company or companies are direct commercial enablers, they often funnel their subsidiary’s data to the government. Furthermore, business and user data can be stored on their parent companies' servers, giving PRC cyber-intelligence entities direct access.

These companies are convenient as they exploit free-market laws and often provide in-demand products to large customer bases, thus making them financially and popularly entrenched. In 2020, former President Trump tried to urge Congress to ban TikTok, which has since exploded in popularity. Despite federal bans on the
“presence or use” of social media apps as connected to government devices, young Americans (including service members) remain heavy recreational users [17]. There have already been indications that the PRC is targeting intelligence and information operations, particularly anti-American and abusive, at America’s unwitting youth [18]. For example, TikTok audited U.S. citizens who did not work for the company to gain access to location data on users’ devices [19]. Since Bytedance, a Chinese company, owns TikTok, the CCP can coerce them to surrender all their data on U.S. citizens. Furthermore, all other Chinese-based companies can be forced to give up data stored on cameras or risk exploiting their systems to gather intelligence [12].

Finally, the last category identifies “At-Risk” organizations with weak—often complacent or compromised—security. As the model indicates, these companies are indirectly vulnerable to various information and cyber-intelligence methods. Perhaps the most obvious is using PRC or affiliated hacker groups to hack or establish exploits in vulnerable networks, often to steal information from companies' servers. This is particularly effective against organizations that cannot afford comprehensive security or have grown complacent through poor training and human error. For example, Exceedium, a network company with a contract with the Office of Personnel Management (OPM), was hacked by PRC-linked groups in 2014 [20]. This compromised the personnel records, including personally identifiable information and social security numbers, of approximately 4 million federal employees. This information could be used to personally target the organizational leadership and current and former federal employees.

At-risk enablers may also be heavily dependent on cheaper PRC-manufactured information technologies. Often, this problem originates from a tainted supply chain whereby software or hardware from a subsidiary or direct enabler is marketed and utilized downstream. Once connected, applications and connections can covertly gather information about the users on the portal or enable backdoor access. A 2018 report reported on Chinese-linked hardware on microchips that enabled backdoor access into any connected system [21]. This report indicated that companies like Amazon and Apple had been compromised by small chips placed on Supermicro motherboards produced in China. Although Amazon and Apple are widely acknowledged for their robust security measures, a lack of due diligence in supply chain security exposed them to potential risks, particularly their less capable commercial customers.

According to the U.S. intelligence community [22], the PRC can exploit the BIOS, or the Basic Input/Output System, on various computers. This is problematic as BIOS, executed first when a computer is powered on, cannot be detected or erased as it is not part of the underlying operating system. The Defense Intelligence Agency (DIA) even stated that China could place BIOS implants on air-gapped computers to gather sensitive information on their subjects [21]. As a result, the DIA speculates that AMI and Phoenix Technologies have had their respective BIOS
software compromised. Both examples show the sophistication of cyber-intelligence operations in using exported hardware and software.

Key Terrain in the Information Domain

The DoD identifies operations, activities, and investments (OAI) as a three-pronged strategy for countering Chinese state-owned enterprises [23]. Irrespective of whether clandestine PRC operations are focused internationally or internally, there is compelling evidence that many corporations based out of China operate as hubs for cyber-intelligence operations and information operations intended to influence international populations and leaders.

For these operations to be effective, comprehensive behavioral data must be gathered either forcibly through cyber-intelligence operations or surreptitiously through applications and interactions (both virtual and physical). As mentioned previously, the PRC influence of multi-media companies such as TikTok allows them access to potential U.S. target audiences, which they can manipulate to (1) discourage anti-Chinese messaging, (2) encourage anti-American narratives, and (3) engage in destructive behavior. TikTok spread disinformation on its platform about the initial cause of COVID-19 and how the PRC handled the pandemic and explicitly programmed the algorithm to deny and suppress anti-PRC statements [24]. Furthermore, they ensured that any information on the app primarily pertained to the U.S.’ poor handling of the pandemic [25], thus spreading distrust and uncertainty across American audiences. Combining this tactic with censorship is an effective and low-cost propaganda tool. Other examples include censorship of creators and influencers who spoke out on the abuse of the Uyghurs (a predominantly Muslim ethnic group in China) or PRC aggression in the South China Sea [26].

The complex and expanding network of human-machine systems is as geographic as it is virtual now. Commercial enablers with access to strategic physical terrain and populations constitute the key terrain the U.S. seeks to protect through OAI.

Huawei and Telecommunications Conduits

Perhaps the most formidable PRC commercial threat to the U.S. and its allies is Huawei and other telecommunications giants. This is because of Huawei’s significant market share in the 5G and Wi-Fi industry, including widespread submarine cables.

An NSA briefing states that Huawei had helped the Chinese government access TAT 14 related to defense industry communications [27]. This occurred through Mitsubishi subcontracting Huawei to help repair their submarine cables and upgrade the system with a PRC-owned high-end router [27]. This could suggest
that Huawei utilizes its telecommunications and existing infrastructure to gather intelligence from its routers and hubs. Given how extensive and wide-reaching Huawei’s submarine cables are (as seen in Figure 1 [28]), Huawei poses an unprecedented national and global security threat.

Figure 1. Depiction of Huawei’s extensive submarine cable.

Figure 2. Display of PRC’s primary tech giants.

Figure 2, retrieved from the project Mapping China’s Tech Giants [28], displays other PRC-owned technology giants on the Internet, surveillance, technology, and communications sectors and their presence overseas. These tech giants help provide technologies like Wi-Fi, 3G, or 5G networks globally. The PRC
uses its telecommunications hubs as cyber-intelligence conduits worldwide—threatening communications above and below [27].

Countering the Threat

Commercial enablers of PRC intelligence and cyber operations fit under the large umbrella of the PRC’s Grand Strategy. As noted, this is managed through PRC directives and campaigns like TTP and MCF. To effectively mitigate these threats, the relationships between the three distinct categories of commercial enablers must be addressed but engaged individually. Because the PRC uses commercial enablers as their new front for conducting key information and cyber-intelligence operations, holistic, whole-of-government OAs must be targeted to protect, reassure, and deter. The influence of the PRC on commercial enablers (mainly the direct and wholly owned subsidiaries) can be effectively diminished by reducing dependence, citizen access, and U.S. involvement with them. President Joe Biden approving a ban on TikTok for government devices is a step in this direction [29]. Subsidiary services or products the National Counterintelligence and Security Center identified as critical to U.S. infrastructure must be 100% non-PRC linked and replaced [30]. Assisting “at-risk” companies with robust, comprehensive security programs tailored towards mitigating insider, supply chain, and cyber-related attacks will prove indispensable for minimizing any indirect interference from the PRC. This includes educating critical personnel about the PRC’s threat [30].

Finally, the CCP manages an intricate cyber intelligence strategy that utilizes its commercial enablers to degrade critical infrastructure and influence target populations. Their aggressive strategic information campaigns, export of potential surveillance technology, and expansion of state-owned enterprises serve to project the PRC’s global economic, military, and social interests. As a result, domestic agencies focused on intelligence and commerce must work closely with companies across all levels to curb U.S. dependence on PRC commercial enablers most controlled by Beijing. This may mean divesting from “At-risk” companies, forcing subsidiaries, antitrust action, and federal mandates on precise and current mitigations. Further, PRC companies that conduct cyber-intelligence and information operations in the U.S. should not be afforded the same status or protections as domestic enterprises.

About the Authors

Victor Mukora

Victor Mukora is a recent May 2023 graduate of Virginia Tech who majored in Computational Modeling and Data Analytics with minors in Data and Decisions, Statistics, and Mathematics. He now does full-time work at Deloitte as an analyst in the government and public services sector.
Ethan Mansour
Ethan Mansour is an Army Reserve Officer Training Corps (ROTC) cadet and a Virginia Tech junior. He is majoring in political science with a focus on national security. Outside of academic work, he has been an undergraduate researcher with the Viceroy program for the last two years, contributing to the research and reports for two projects.

Acknowledgement
This publication was supported by Award Number SA10012022020481 from the Griffiss Institute for the VICEROY program. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the sponsor.

References


Implementation Guidance. Director of the OMB, 2023, M-23-13 (whitehouse.gov).


