PRC Using Commercial Technology Industry to Support State Intelligence Initiatives

Part 1: PRC Global Hegemony as a Collective Effort

September 2021 • WP-2021-1
TLP: WHITE

Executive Summary

MS-ISAC Cyber Threat Intelligence (CTI) assesses that cybersecurity partnerships and commercial transactions with the People's Republic of China (PRC) companies, such as Alibaba and Huawei, indirectly support Chinese Communist Party (CCP) initiatives. The People's Liberation Army (PLA), the militarized wing of the CCP, owns or maintains ties with enterprises associated with transport, equipment repair, telecommunications infrastructure, and data processing.[1] The PRC seeks global hegemony through routine corporate espionage campaigns, economic and defense partnerships via the Belt and Road Initiative and replication of stolen or purchased proprietary technology for economic and military advantage.[2] The CCP acts on these initiatives through long-term cyber espionage and intellectual property (IP) collection campaigns targeted against Western assets by enlisting PLA-influenced enterprises for support.

Key Findings

Diplomatic information corridors established via the Belt and Road Initiative allow for commercial expansion into countries with ties to the U.S. Paired with the PRC's National Intelligence Law of 2017, this poses a significant threat to data traversing network infrastructure owned by Chinese private companies.

- Big-data analytics and telecommunication companies based in China are legally required to process or provide data to state intelligence agencies upon request.
- Since 2014, China banned foreign antivirus products and is actively replacing hardware and software used by government officials with domestic equipment.
- Leadership in Chinese-owned companies, such as Alibaba and Huawei, maintain strong connections with PRC leadership, the PLA, and/or the CCP, and receive special treatment when seeking loans from Chinese-owned banks or government approval when pursuing contracts with customers abroad.
- The Cyberspace Administration of China (CAC) published vulnerability disclosure regulations in July 2021, stating researchers must share vulnerability reports with state agencies within two days of a report. Researchers are also banned from sharing data with international organizations aside from product vendors and service providers. In effect, the requirement allows PRC actors to leverage vulnerabilities before vendors are able to address them and exert control over public disclosure timelines.

Background

A brief examination of Chinese military doctrine allows for a general understanding of how PRC commercial industry supports CCP initiatives. The PLA does not subscribe to Western models of conflict, which segregate peace and war into binary phases. Instead, PLA doctrine is built upon a range of Maoist-Marxist-Leninist influence with "struggle" as a scale and military competition marking one end of the spectrum.[3]

Information operations under the CCP are offensive in nature with an understanding that information dominance equates to victory. If PLA forces successfully disrupt an adversary's system of systems[1] while maintaining its own, then they gain a strategic advantage over their opponent. This is similar to U.S. network-centric strategies, which target systems coordinating activities across services; however, the PRC's model is implemented on a broader scale.[3] Many of the PLA's cyber intelligence operations seek to provide the CCP with this advantage, even if China is not in direct conflict with another nation-state.

The PLA's primary mission is to build a "qualitatively superior military" and to "build up China's national power and leadership" as part of their competition with the U.S.[4] This competition for global primacy extends into cyberspace via the Strategic Support Force. A part of the PLA, the Strategic Support Force (SSF) maintains responsibility for information operations. Their role is integral to China's "escalation dominance" strategy, which emphasizes gaining unseen information and intelligence advantages in peacetime. This behavior shapes adversarial responses in scenarios that are not yet considered full-scale conflict.[3] Global dominance in cyberspace does not always equate to overt, offensive operations, as legal procurement and partnerships via the Belt and Road Initiative offer new explicit yet deniable advantages to the CCP's overall objective of Chinese hegemony.

Leveraging Legal Procurement

The PRC solely obtaining sensitive information through data breaches and cyber espionage is a common misconception. China legally procures systems and software to deconstruct and recreate via their own means. In the early 1990s, China's official defense budget increased from 5 billion RMB (approximately 7 million USD) to 64.8 billion RMB (approximately 10 billion USD). [5] Thirty-four percent of the budget would be dedicated to equipment purchases over the next decade. Paired with access to foreign military equipment and technical assistance from other countries, such as Russia and Israel, the PRC is able to leverage its defense sector research and development firms to copy-produce and integrate advanced weapon systems into its arsenal.[5] The PLA successfully applies this methodology to its information operations, as well.

Recorded Future recently published an article detailing the SSF's purchase of foreign antivirus products, assessed for exploitation purposes.[5] The chart below lists U.S.-specific antivirus licenses purchased by the PLA.

Date of Procurement Order	Product Name	Subscription Length	Number of Users	Country of Supplier
April-May 2019	McAfee Total Protection	2 years	30 user terminals	US
April-May 2019	Norton Security Premium	2 years	10 user terminals	US
April-May 2019	Symantec Endpoint Protection Subscription	2 years	10 user terminals	US
November 2019	Trend Micro Worry-Free Services Advanced	2 years	10 user terminals	US-Japan

U.S. Antivirus Purchases by SSF. *Recorded Future. May 5, 2021.*

Of note, the licenses obtained by the SSF were English-language versions. Recorded Future assesses that Mandarin-language versions of these software products would indicate the purchase was intended for legitimate

[1] According to MITRE, a system of systems is a collection of independent systems which interoperate together to achieve additional capabilities.

use. Notably, the Chinese government has not used foreign antivirus software for legitimate purposes since it was banned in 2014.[8] Two likely scenarios stem from these acquisitions. The first is the PLA using the software in testing environments for newly-developed malware. By testing malware against foreign antivirus products, the PLA can determine its ability to evade detection. The second scenario is the PLA reverse engineering the antivirus software. Reverse engineering teaches the PLA how these antivirus tools are detecting current threats as well as allows the PLA to find new vulnerabilities for exploitation in future operations.[6]

The PRC's intent with legal procurement can lead to offensive operations. For example, Chinese cyber actors have "demonstrated a pattern of software supply chain exploitation in multiple cyber intrusion campaigns, including against some of the foreign antivirus software purchased in 2019." [6] From 2017-2021, Chinese state-sponsored threat actors:

- successfully breached Avast twice;
- exploited two zero-day[2] vulnerabilities in Trend Micro security products;
- targeted the Biden's campaign email system in 2020 via McAfee Total Protection, antivirus software which was purchased by the same PLA unit in 2019; and
- exploited four zero-days gaining access to Microsoft Exchange servers.[6]

The CAC's new regulation on vulnerability disclosure places the CCP at a strategic advantage in that vulnerabilities must be disclosed to the Ministry of Industry and Information Technology (MIIT) within two days of discovery.[7] This means Western-based bug bounty platforms must comply with this requirement in order to legally receive vulnerability reports from PRC researchers. It is likely that PRC researchers must also hand over vulnerability data to the MIIT within two days of receipt from international partners. This allows PRC actors to leverage vulnerabilities before vendors are able to address them, effectively creating a pipeline for zero-day exploits. Additionally, the CCP may gain an advantage to pressure companies to keep certain vulnerabilities in place or restrict public disclosure of discovered vulnerabilities. The regulations enter into effect starting September 1, 2021.

Digital Silk Road and the Pursuit of Economic Hegemony

The PRC's Digital Silk Road (DSR) represents a segment of the Belt and Road Initiative (BRI), which is Beijing's overall strategy to provide aid, political support, and assistance to recipient nations. A focus on infrastructure and critical technologies through the BRI "creates leverage, improves China's collection capabilities, and increases dependence on China while reducing reliance on Western-based networks and technology."[10]

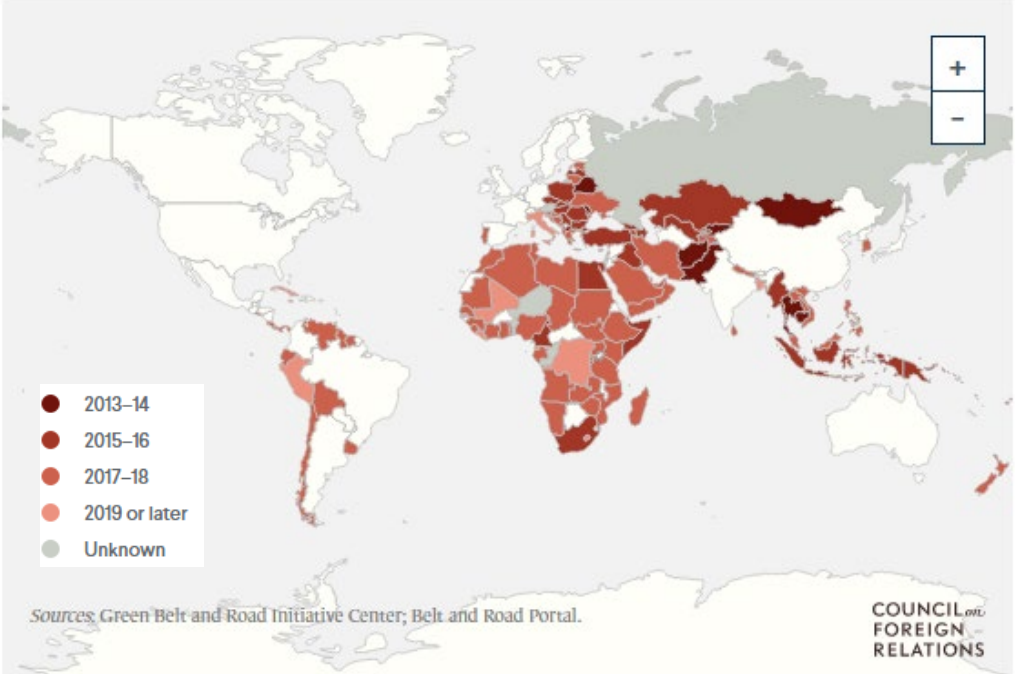
The DSR also provides support to Chinese telecommunication companies, such as Huawei and ZTE. Chinese firms led by Huawei are global leaders in supplying artificial intelligence surveillance technology used for public security.[11] Under DSR initiatives, the Ministry of Industry and Information Technology encourages companies such as Huawei, ZTE, Alibaba, and Baidu, as well as others, to develop digital infrastructure in BRI countries. This is particularly concerning as many countries with BRI partnerships also host U.S. military installations. A few of these countries include Iraq, Kuwait, Djibouti, Saudi Arabia, and Italy, among others.

These same companies maintain ties with the PLA and receive preferential treatment through government policy support[11] while also obtaining major lines of credit through state-owned commercial banks.[14, 16] This allows them to sell products 30 to 40 percent cheaper than non-Chinese competitors. Huawei's ability to enter new markets at

[2] Zero-day vulnerabilities are software security flaws with no existing patch due to the lack of knowledge of the flaw at the time they are exploited.

a cost less than competitors opens doors for additional Chinese companies to follow while also allowing them to obtain a better foothold in adjacent markets.[11] An article published on the People's Daily Online, China's largest newspaper group, detailed public concerns regarding Internet companies such as Baidu and Tencent forming strong CCP connections.[12] Such penetration of BRI countries is concerning given all Chinese technology companies are legally bound to enable intelligence work on behalf of the CCP under the PRC's 2017 National Intelligence Law if requested.[13]

Expansion provided by the DSR strengthens China's global collection capability through bundled technology product sales, such as smart cities, smart ports, and 5G-based artificial intelligence (AI) data analytics. Through bundling technological sales in BRI contracts, the PRC controls greater access to data transiting through its products. Canadian universities' use of the Alibaba Global Accelerator to avoid network congestion and reduce delays for videoconferencing gave the Canadian Security Intelligence Service cause for concern because of the access to proprietary data.[15] Targeting specific technologies, such as 5G and AI, confers specific benefits to the PRC for data collection at scale and optimizing the processing and exploitation of large data sets.[10] Data aggregation via DSR presents a challenge to state intelligence agencies desiring to leverage its contents for ongoing or future operations. If a certain agency is unable to conduct big-data analytics internally, they can leverage private sector entities to assist according to the 2017 National Intelligence Law.[12]



Official BRI Participants by Year of Joining. *Council on Foreign Relations.*

The Commercial Wing of the CCP

China's weaponization of personal data is perpetuated by its coercion of big-data analytics companies. In 2017, China passed a revised version of its National Intelligence Law.[19] This legislation obligates organizations to cooperate with state intelligence requests and initiatives according to Article 7, which states:

> Any organization or citizen shall support, assist, and cooperate with the state intelligence work in accordance with the law, and keep the secrets of the national intelligence work known to the public. The State protects individuals and organizations that support, assist, and cooperate with national intelligence work.[12]

Companies such as Huawei or Alibaba would be required to comply with state requests for information if prompted, according to this law.

The foundation of the DSR's success is laid by private industry organizations like Huawei and ZTE. In an article published by Foreign Policy, current and former U.S. officials found evidence of these companies working with Chinese intelligence services on a daily basis.[20] The PRC's ability to collect data, through DSR contracts or otherwise,[21] and process that data in a meaningful way allows for an advantage over foreign competitors and adversaries. According to William Evanina, former director of the U.S. National Counterintelligence and Security Center, "Chinese technology companies play a key role in processing this bulk data and making it useful for China's intelligence services."[20] Companies with big-data analytics capabilities, such as Alibaba and Baidu, can be tasked by Chinese intelligence agencies to process information of intelligence value stolen from data breaches. An example of such data is the 21.5 million background investigation records stolen following the successful compromise of the U.S. Office of Personnel Management (OPM) by PRC actors in 2015.

After sorting through exfiltrated data, the Ministry of State Security (MSS) and other PRC agencies can deconflict with intelligence gathered by other sources to target and disrupt U.S. intelligence operations. This is precisely what the PRC did with undercover Central Intelligence Agency (CIA) operatives in Africa and Europe following analysis of the data exfiltrated during the OPM breach.[21, 23] Russia also benefited from China's bulk collection, as the Kremlin successfully identified new CIA officers in the U.S. Embassy in Moscow shortly after the OPM breach occurred.[20, 23, 24] Even companies and individuals that may not agree with the National Intelligence Law must comply with intelligence operations when requested by the state or face consequences.[25]

Conclusion

Examining the PRC's approach to governance and military strategy provides a level of awareness regarding the frequency of corporate espionage campaigns and information operations tactics leveraged by Chinese actors. The CCP views global competition and adversaries as those who deepen their perceived struggle as a nation.

In pursuit of global hegemony, the CCP expects cooperation from the general population and private companies as part of a collective effort to fully pursue state initiatives. Commercial transactions and data exchanges with Chinese-based companies can be leveraged by PRC state intelligence agencies for operations and should be given higher levels of scrutiny or reconsidered entirely based on the aggregated assessments above.

Analytic Confidence

Analytic confidence in this assessment is high. Source reliability is moderate with minimal conflict. The analyst used the circleboard structured analytic method in this analysis.

Content and assessments herein are the first installment of two CCP State Initiative focused White Papers. The second publication will detail the PRC's Thousand Talents Plan and debt trap techniques used to reduce Western influence across BRI countries.

For questions or comments, please contact the MS-ISAC Cyber Threat Intelligence (CTI) team at intel@cisecurity.org.

References

1. https://online.ucpress.edu/as/article-abstract/34/5/460/23156/The-Chinese-Military-and-Its-Business-Operations?redirectedFrom=fulltext
2. https://foreignpolicy.com/2019/04/25/chinas-debt-diplomacy/
3. https://inss.ndu.edu/Media/News/Article/1651882/chinas-strategic-support-force-a-force-for-a-new-era/
4. https://www.rand.org/t/RRA447-1
5. https://www.rand.org/content/dam/rand/pubs/monographs/2005/RAND_MG334.pdf
6. https://www.recordedfuture.com/china-pla-unit-purchasing-antivirus-exploitation/
7. https://therecord.media/chinese-government-lays-out-new-vulnerability-disclosure-rules/
8. https://www.reuters.com/article/us-china-software-ban/beijing-to-bar-symantec-kaspersky-anti-virus-in-procurement-report-idUSKBN0G30QH20140803
9. https://asiasociety.org/sites/default/files/2020-09/Weaponizing%20the%20Belt%20and%20Road%20Initiative_0.pdf
10. https://www.cfr.org/report/chinas-belt-and-road-implications-for-the-united-states/introduction
11. https://www.aspi.org.au/report/mapping-chinas-tech-giants
12. dangjian.people.com.cn/n1/2018/0326/c117092-29889441.html
13. https://ijoc.org/index.php/ijoc/article/view/8405
14. https://www.cnbc.com/2014/09/15/alibabas-link-to-elite-military-family-is-etched-in-stone.html
15. https://www.theglobeandmail.com/politics/article-csis-warns-canadian-universities-about-alibabas-online-platform/
16. https://www.wsj.com/articles/americans-wont-be-banned-from-investing-in-alibaba-tencent-and-baidu-11610563890
17. https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf
18. https://nationalinterest.org/feature/exploring-china%E2%80%99s-orwellian-digital-silk-road-111731
19. https://www.reuters.com/article/us-china-security-lawmaking/china-passes-tough-new-intelligence-law-idUSKBN19I1FW
20. https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies
21. https://www.brusselstimes.com/news/belgium-all-news/168376/are-chinese-agents-operating-at-liege-airport-vincent-van-quickenborne-alibaba-commercial-intelligence-security/
22. https://www.afr.com/technology/tech-giants-are-giving-china-a-vital-edge-in-espionage-20210107-p56sbr
23. https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/
24. https://news.yahoo.com/shattered-inside-the-secret-battle-to-save-americas-undercover-spies-in-the-digital-age-100029026.html
25. https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/2017_surveillance_law.pdf

MS-ISAC®

EI-ISAC®

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

31 Tech Valley Drive

East Greenbush, NY 12061

SOC@cisecurity.org - 1-866-787-4722

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

https://www.us-cert.gov/tlp/