FBI

COUNTERINTELLIGENCE STRATEGIC PARTNERSHIP INTELLIGENCE NOTE (SPIN)

MARCH 2018

(U) Huawei

(U) Chinese Government- Subsidized Telecommunication Company

(U) RISK OVERVIEW

(U) With the expanded use of Huawei Technologies Inc. equipment and services in US telecommunications service provider networks, the Chinese Government's potential access to US business communications is dramatically increasing. China's intelligence services and Chinese cyber actors could exploit Chinese Government-supported telecommunication equipment on US networks operating as an advanced persistent threat. China makes no secret that its cyber warfare strategy is predicated on controlling global communications network infrastructure.

(U) Since Huawei's inception in 1987, the company continues to receive open support from senior Chinese Communist Party officials and People's Liberation Army (PLA) Commanders. Bolstered by Chinese Government subsidization and direct financing, Huawei is able to offer unsuspecting US businesses low-cost offers in exchange for access to US networks.

(U) The purpose of this SPIN is to provide summaries of recent US investigative findings, private industry reporting, and news articles on Huawei Technology Inc.

(U) INVESTIGATIVE REPORT ON THE US NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANY HUAWEI

(U) Huawei and another China-based entity, ZTE, were both previously highlighted as concerns in a 2012 House Permanent Select Committee on Intelligence (HPSCI) report. The report noted, **"the protection of intellectual property and compliance with United States export control laws are a core concern for U.S. interests. The ability of a company to comply with these laws provide a useful test of that company's ability to follow international codes of business conduct and remain free of undue state influence."**

(U) UPDATES SINCE HPSCI

(U//FOUO) FBI Director Wray's Senate testimony at the Senate Intelligence Committee in February 2018 demonstrates that the US government remains concerned about the security risks posed by Chinese telecommunications companies.

(U) "We're deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks. That provides the capacity to exert pressure or control over our telecommunications infrastructure. It provides the capacity to maliciously modify or steal information. And it provides the capacity to conduct undetected espionage." –FBI Director Wray, 13 February 2018

(U) In January 2018, daft bill HR4747, also known as the "Defending US Government Communications Act," was introduced in the US House of Representatives. The bill cites reporting indicating that PRC companies Huawei and ZTE are "subject to state influence." It would prevent the use or procurement of any telecommunications equipment or services from Huawei or ZTE as a "substantial or essential component of any system, or as critical technology as part of any system" as related to USG contracts.

(U) The draft Senate version of the bill, S.2391, would prohibit USG agencies from purchasing and leasing hardware and services made by ZTE, Huawei and any affiliates and subsidiaries.

(U//FOUO) PRC LAWS APPLICABLE TO CHINESE COMPANIES IN THE US

- (U) **Cybersecurity Law of 2017** requires telecommunication network operators and ISPs to store data within China and allows Chinese authorities to conduct spot-checks on company network operations.
- (U) **PRC National Security Law of 2015** calls for citizens and organizations to provide information or other assistance for Chinese national security works.
- (U) **2015 Chinese Counterterrorism Law** requires that internet service providers (ISPs) provide technical means of support in terrorism and other national security cases.
- (U) **1996 Chinese Archive Law** requires all Chinese state organizations, armed forces, political parties, social organizations, state-owned enterprises, establishments, and citizens to regularly transfer information to the Chinese government in China for record keeping and archiving. Subsidiary companies of Chinese companies are included.

(U) "**Citizens** of the People's Republic of China, all state organs and armed forces, each political parties and mass organization, **enterprises**, public institutions and other social organizations, **all have the responsibility and obligation to preserve national security.**" **–PRC State Security Law**

(U) BACKDOORS AND UNDISCLOSED FEATURES

(U) Modern telecommunications are a complex ecosystem with multiple interoperable parts fulfilling different rules but all cooperating through shared standards. Any one of these parts could be a potential asset to a hostile foreign power. These inherent vulnerabilities are potentially in any equipment servicing and maintenance contracts. Additionally, manufactures regularly update most complex telecom products so even if there are no deliberate vulnerabilities now, some future update could install them. While some risks can be mitigated, it is highly unlikely that even careful inspections could identify all vulnerabilities.

"The task of finding and eliminating every significant vulnerability from a complex product is monumental. If we also consider flaws intentionally inserted by a determined and clever insider, the task becomes virtually impossible" -- 2012 HPSCI report

(U) DISRUPTION AND DATA EXFILTRATION

(U//FOUO) Huawei and ZTE provide finished equipment, components, and services to network routers. Routers are used to connect users between networks, and network customers typically subscribe to an Internet service provider (ISP) to transport data between networks. If the routers were disabled, it could severely disrupt the internet, as traffic would no longer be routed between networks, except where carriers had their own private peering arrangements. Additionally, routers are comprised of integrated circuits and may include backdoors or other vulnerabilities that would allow for remote, unauthorized, and undetected

access by the manufacturer or a malicious actor. These vulnerabilities could potentially allow for exfiltration of data to Chinese-based servers.

(U) 5G TECHNOLOGIES

(U//FOUO) Huawei could insert backdoors into current, 4G LTE, critical telecommunications infrastructure equipment it provides such as routers, switches, and phones. This could give Beijing potential access to national communications. If Huawei partners with telecommunications carriers to develop the next generation wireless network, 5G, then the backdoors could end up on far more telecommunications equipment to include cell phone towers.

(U) HUAWEI THEFT OF US PROPRIETARY INFORMATION

(U) T-Mobile created a phone-testing robot called Tappy that in a matter of days could test daily phone use and everyday functionality, compared to the weeks this testing used to take. As a handset supplier to T-Mobile in 2012, Huawei was granted access to the testing lab and the Tappy Robot after signing a clean room letter and non-disclosure agreements that prohibited photography, copying of source code, or any other theft of the technology.

(U) Despite T-Mobile taking significant steps to protect its robot intellectual property, in May 2013 Huawei employees took photographs and stole T-Mobiles trade secrets including the robot finger. In 2017, T-Mobile won its civil lawsuit against Huawei, who was found to have misappropriated trade secrets belonging to T-Mobile, who was awarded $4.8 million by a jury. This shows the lengths that Huawei went to steal T-Mobile's proprietary information and how it treats its business partners, despite having signed legal agreements.

(U) OUTLOOK AND IMPLICATIONS:

(U) US assets are largely in the hands of the private sector, not the government. If your company or agency has information or assets that could help our adversaries advance their interests, then your company or agency is almost certainly being targeted. You must identify and protect your priority information and assets, and you should engage with your local FBI office to exchange intelligence and report suspicious activity. Prevention of harm is essential. Once a foreign country has acquired U.S. information or assets, the damage cannot be undone by punishing those who were responsible.

***See Appendix 2 for key industries for potential PRC targeting**

(U) SOURCES

1. (U) House Permanent Select Committee on Intelligence; 8 OCT 2012; (U) Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE.
2. (U) Senate Select Committee on Intelligence; 13 February 2018; (U) Open Hearing: Worldwide Threats Hearing.
3. (U) Defending U.S. Government Communications Act, H.R.4747 (2017-2018).
4. (U) Defending U.S. Government Communications Act, S.2391 (2017-2018).
5. (U) Foreign Government Document; PRC National Security Law 2015; 02 JUL 2015; 30 June 2015; Xinhua Domestic Service; (U) 15th Session of the Standing Committee of the 12th National People's Congress; Unclassified.

6. (U) Website; www.npc.gov.cn; "(U) Cybersecurity law of the People's Republic of China, Standing Committee of National People's Congress"; http://www.npc.gov.cn/nc/xinwen/lfgz/flca/2015-07/06/content1940614.htm; accessed on 04 October 2017; Website is official Chinese Government posting on law.
7. (U) Foreign Government Document; (U) Counterterrorism Law of the People's Republic of China; 27 December 2015; Standing Committee of the National People's Congress; http://news.xinhuanet.com/politics/2015-12/27/c_128571798.htm. Unclassified.
8. (U) Foreign Government Document; (U) Law on Archives of the People's Republic of China' 05 July 1996; Unclassified. (U) USCC; JAN 2011;
9. (U) The National Security Implications of Investments and Products from the People's Republic of China in the Telecommunications Sector.
10. (U) Industry Report; Northrop Grumman Corporation; 07 MAR 2012 (U) Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage; Report prepared for the US-China Economic and Security Review Commission.
11. (U) Nathaniel Ahrens, "China's Competitiveness: Myth, Reality, and Lessons for the United States and Japan," Center for Strategic and International Studies; http://csis.org/files/publication/130215_competitiveness_Huawei_ casestudy_Web.pdf.
12. (U) Sheridan Prasso, "What Makes China telecom Huawei so Scary," CNN Money; 28 JUL 2011; http://tech.fortune.cnn.com/2011/07/28/what-makes-china-telecom-huawei-so-scary/
13. (U) Reuters, http://www.reuters.com/article/2013/01/31/us-huawei-skycom-idUSBRE90U0CC20130131
14. (U) The Washington Free Beacon; http://freebeacon.com/national-security/chinese-military-linked-telecom-firm-shippedu-s-equipment-to-cuba/
15. (U) ABC News; 29 OCT 2013; Government maintains NBN ban on Chinese telco Huawei after security briefings; http:// www.abc.net.au/news/
16. (U) MANDIANT; APT1-Exposing One of China's Cyber Espionage Units.
17. (U) Online news article; Forbes; "Chinese Government Helps Huawei with 5G;" 8 May 2018.
18. (U) Online news article; Dave Waterson on Security; "Security Implications of 5G;" 9 March 2015.
19. (U) Online news article; Reuters; "China's Huawei Set to Lead Global Change to 5G Networks;" 23 February 2018.
20. (U) Online news article; Trade Secret; "Chinese Company Steals T-Mobile's 'Tappy' Robot Tech, Complaint Alleges;" 19 September 2014.
21. (U) T-Mobile United States Inc. V. Huawei Device United States Inc., United States District Court W.D. Washington, at Seattle.
22. (U) Online news article; The Seattle Times; "Jury Awards T-Mbole $4.8M in Trade Secrets Case Against Huawei;" 18 Mary 2017.
23. (U) Online news article; techcrunch.com; "Huawei Puts $1M into a new AI research partnership with UC Berkeley"; 11 October 2016; https://techcrunch.com/2016/10/11/huawei-puts-1m-into-a-new-ai-partnership-with-uc-berkeley/; accessed on 26 September 2017; website provides technology news.
24. (U) Online news article; venturebeat.com; "Amazon, Google, Huawei, and Microsoft sponsor UC Berkeley RISELab, AMPLab's successor; 23 January 2017; https://venturebeat.com/2017/01/23/amazon-google-huawei-and-microsoft-sponsor-uc-berkeley-riselab-amplabs-successor/; accessed on 26 September 2017; website provides technology news.
25. (U) Web site; Stanford Pervasive Parallelism Laboratory; "PPL Member Companies"; 01 January 2016; https://ppl.stanford.edu/membership; accessed on 26 September 2017; Website for Stanford University Engineer Pervasive Parallelism Laboratory.

APPENDIX 1

(U) BUSINESS CONSIDERATIONS

(U//FOUO) **Mergers/Acquisitions**: Has your company been approached for a merger or acquisition opportunity by a foreign competitor?

(U//FOUO) **Joint Projects/Collaborations**: Which specific programs/offices within your company have liaison relationships/joint efforts with domestic and foreign entities? Who initiated the partnership effort? What processes do you use with regard to your due diligence when vetting potential foreign partners?

(U//FOUO) **Foreign Government Activities**: What is the nature of foreign government involvement in your industry overseas?

(U//FOUO) **Major Foreign Competitors**: Who are your major foreign competitors, particularly those with whom you share some cooperative endeavors? Are you aware of any of your main US/domestic competitors working or negotiating with foreign competitors?

(U//FOUO) **Circumventing/Manipulating US Laws and Regulations**: When you deny access to your facility or classified, trade secret, and proprietary information, have you experienced attempts to circumvent? Have foreign businesses or groups attempted to circumvent US law, regulation, or company security systems?

(U//FOUO) **Visitors or Others Collecting Information**: What are other ways you receive unsolicited requests for information? Are there certain members of visiting delegations who tend to ask most of the questions when you are hosting groups to your facility? Are questions submitted in advance or asked randomly?

(U//FOUO) **Targeted Technology/Proprietary Information**: What technologies do you want to protect from your competitors? Do you believe you are adequately protecting them? What information or technology (including expertise in manufacturing, production, or operations) are foreign competitors lacking that keeps them from being competitive?

(U//FOUO) **Criminal and Suspicious Activities**: What are the various ways you may have experienced loss, theft, or targeting of your trade secrets, proprietary, and critical or emerging technologies, and by whom?

(U//FOUO) **Targeting Trends**: Has your company observed any trends in the way a domestic or foreign competitor is targeting your proprietary or trade secret information?

(U//FOUO) **Research and Development Losses**: Which countries are your most valuable customers? How do they support your research and development efforts? What is the estimated value of losses of your trade secret or proprietary information?

(U//FOUO) **Collaboration Among Foreign Partners**: How is your company connected to international partners (e.g., through supply chains, joint R&D, acquisition processes, distribution, etc.)? How do you determine your supply chain is sound and you are getting the quality products you purchased/requested? Have international partners sought any quality assurance testing on your products, either before or after a sale?

(U//FOUO) **Financial Matters**: Identify any suspicious financial activities of your business partners, distributors, suppliers, and employees that may aid business competitors or foreign organizations.

APPENDIX 2

(U//FOUO) KEY TECHNOLOGIES IDENTIFIED IN "MADE IN CHINA 2025" ROADMAP IN CHINA'S 13TH FIVE YEAR PLAN

1. New Generation Information Technology
2. High-Grade Computer Numerical Control Machine (CNC) Tools and Robotics
3. Aerospace Equipment

4. Marine Engineering Equipment and High Technology Ships
5. Advanced Rail Transportation Equipment
6. Energy Efficient and New-Energy Automobiles
7. Electric Power Equipment
8. Agricultural Equipment
9. New Materials
10. Biomedicine and High-Performance Medical Instruments

(U//FOUO) Chinese Government Encourages Targeting, Acquisition, and Exploitation of Dual-Use US Information and Technology

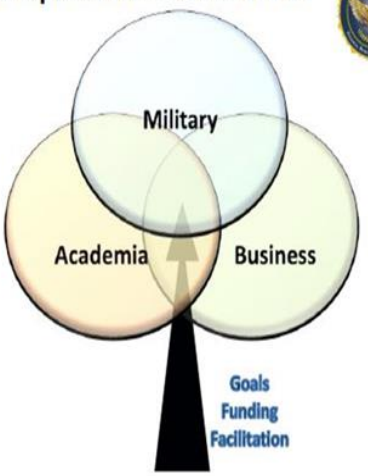
(U//FOUO) The Chinese Government encourages Chinese non-traditional collectors (NTCs) to target, acquire, and exploit dual-use US information and technology to close critical military and commercial technology gaps with the United States. Two key ways the Chinese Government accomplishes this is through significant focus on science and technology (S&T) priorities that overlap multiple sectors and the promotion and implementation of civil-military integration.

(U) Intersecting S&T Priorities

(U//FOUO) The Chinese Government's national development plans for S&T largely focus on S&T priorities that reside across its military, business (commercial), and academic sectors (see Venn diagram). These overlapping S&T priorities are supported by similarly overlapping financial resources, which incentivize NTCs across the various sectors to target dual-use information and technology that can fill multiple gaps. In addition, the overlapping S&T priorities allow maximum information sharing across government operated enterprises that support both military and commercial technology development, and make it easier to exploit the US S&T infrastructure which also promotes cross-sector collaboration between military, business, and academic sectors.

(U) Civil-Military Integration

(U//FOUO) China's ability to effectively exploit acquired dual-use US information and technology stems from its dedication to civil-military integration (CMI). For China, CMI is a strategy aimed at leveraging its significant civilian industry resources and S&T community to further modernize China's military. Through CMI, China's military-related sectors are able to gain access to technologies acquired by civilian entities or through civilian projects of state-owned enterprises. China has exhibited its commitment to CMI by recently launching the National Defense Industry Enterprise Military and Civil Integration Alliance and a Central Commission for Integrated Military and Civilian Development, whose Chairman is Chinese President Xi Jinping. The spirit of CMI is represented in Former Chinese leader Deng Xiaoping's 16-Character Policy (see graphic).



The PRC's 16-Character Policy

軍民結合
平戰結合
軍品優先
以民養軍

"Jun-min jiehe" (Combine the military and civil)

"Ping-zhan jiehe" (Combine peace and war)

"Jun-pin youxian" (Give priority to military products)

"Yi min yan jun" (Let the civil support the military)