FBI

COUNTERINTELLIGENCE STRATEGIC PARTNERSHIP INTELLIGENCE NOTE (SPIN)

SPIN: 15-002 **FEBRUARY 2015**

(U) Huawei

(U) A Chinese Government-Subsidized Telecommunication Company

(U) RISK OVEVIEW

(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. Chinese Government-supported telecommunication equipment on US networks may be exploited through Chinese cyber activity, with China's intelligence services operating as an advanced persistent threat to US networks. Huawei has been identified publicly for selling or attempting to sell US intellectual property to export restricted countries (Iran/Cuba), making it a clear threat through its targeting of US economic and proprietary information. China makes no secret that its cyber warfare strategy is predicated on controlling global communications network infrastructure.

HUAWEI

(U//FOUO) Huawei is a threat to intellectual property and business communications due to its opaque relationship with the Chinese Government. Huawei has legal obligations to work on behalf of the Chinese state, probably through the Chinese Communist Party (CCP) committee residing within Huawei. This relationship likely influences the company's decision-making through threats of corruption investigations.

(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. With over $100 billion in Chinese Government subsidization and direct financing, Huawei is able to offer unsuspecting US businesses low-cost offers difficult to refuse in exchange for access to US networks.

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

(U) Ministry of State Security

(U) People's Liberation Army

(U) HUAWEI'S EXECUTIVE TIES TO CHINESE MILITARY AND INTELLIGENCE SERVICES

(U) Sun Yafang reportedly worked for the Ministry of State Security (MSS) for an unspecified period of time before joining Huawei in 1989. She quickly rose through the company's ranks to serve as the company's Chairwoman of the Board from 1998-2011.

(U) Ren Zhengfei, a retired PLA officer and director of the PLA's General Staff Department Information Engineering Academy, founded Huawei in 1987. In 1988, he became the president of Huawei and has held the position ever since, according to Open Source reporting.

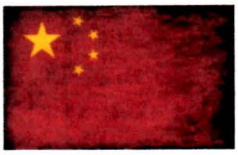
(U) HUAWEI IN OTHER COUNTRIES

(U) The US is not the only highly capitalized country targeted by Huawei. The United Kingdom (UK) engaged with Huawei, only to regret its decision. The UK's national security policy makers were highly concerned with how Huawei discreetly accessed its critical telecommunication infrastructure. The government had difficulties trusting a cyber-security evaluation process to help secure Huawei's integration, according to a report by the Parliamentary Intelligence and Security Committee. Australia, on the other hand, proactively decided twice to keep Huawei out of its national broadband infrastructure.

(U) Secret Intelligence Service (MI6)

(U) House of Commons

(U) NATIONAL SECURITY IMPLICATIONS OF INVESTMENTS AND PRODUCTS FROM THE PEOPLE'S REPUBLIC OF CHINA IN THE TELECOMMUNICATIONS SECTOR



(U) The Chinese Government views the telecommunications sector as a "strategic" industry and has expended significant effort and resources to promote and enable new business opportunities in the telecommunications field. These efforts are supported by national-level policies, as the country's senior leadership perceives investment in high-technology sectors to be instrumental in closing the technological gap between China and western nations.

(U) The large and growing state-controlled telecommunications sector is also a major source of government revenue. National security concerns have accompanied the dramatic growth of China's telecom sector. Signals intelligence is a significant source of Chinese intelligence collection, and there is growing public concern over the impacts of cyber espionage incidents that appear to originate in China. Additionally, large Chinese companies are subject to direction by the CCP, to include support for Chinese state policies and goals. From this point of view, the clear economic benefits of foreign investment in the United States must be weighed against *potential* security concerns related to infrastructure.

(U) Internet exchange points (IXP) use a host of networking equipment, including sophisticated routers and switches, which enables traffic to be properly routed. This equipment is comprised of integrated circuits that can be severely impacted, thereby modifying functionality, including backdoors and/or kill switches. Although hostile actors manufacturing such products could conceivably target all integrated circuits to be used in routers, they might instead target integrated circuits used in the most sophisticated equipment. The Internet in the United States could theoretically be brought down or severely disrupted because the routers and switches serving the IXPs were disabled. Traffic would no longer be routed between networks, except where carriers had their own private peering arrangements.

(U) FOREIGN INVOLVEMENT IN BRITISH CRITICAL NATIONAL INFRASTRUCTURE: IMPLICATIONS FOR NATIONAL SECURITY

(U) **British Parliamentary Report:** Huawei was allowed to gain a large foothold in the UK's Critical National Infrastructure (CNI); the question now is whether or not that foothold has implications for the UK's national security. When British Parliament Ministers were finally informed about Huawei's involvement in 2006, it was because approval was sought to carry out checks on Huawei's equipment.

(U) **Outlined Threat:** The British Security Service told the British Parliament in early 2008 the Chinese State may be able to exploit any vulnerabilities in Huawei's equipment in order to gain access to the British Telecom network. The Joint Intelligence Committee (JIC) had previously warned if a hostile actor were to exploit such an opportunity, an attack "would be very difficult to detect or prevent and could enable the Chinese to intercept covertly or disrupt traffic passing through Huawei supplied networks."

(U) The assessments underlined what could be at stake through Huawei's involvement in the UK's CNI. The British Parliament questioned how the government would react in the event of an attack, if it was detected. The Cabinet Office explained they would "have the option of putting pressure on the

Communications Service Providers (CSPs) to terminate any contract with Huawei. But the British Government would have to have firm evidence of Chinese attribution." The Committee is concerned at the apparent absence of any strategy to monitor or react to potential breaches. Any vulnerability would call into question whether a product is sufficiently well engineered. An insecure product would risk a third party exploiting its weaknesses to access UK networks for hostile purposes. While we [Intelligence and Security Committee] are reassured by GCHQ's confidence in BT, we also note they acknowledge the risk of unauthorized access cannot be entirely eliminated.

(U) **Conclusion:** The British Parliament remains concerned there is no guarantee any weaknesses or vulnerability in equipment deployed on UK networks, through no fault of the operator, could have serious security implications.

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

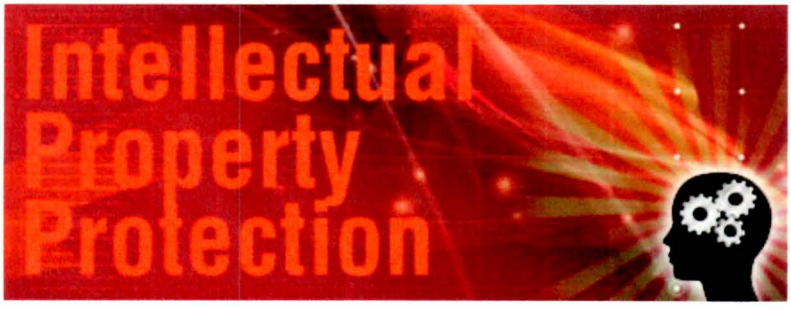
(U) ***The United States should view with suspicion the continued penetration of the US telecommunications market by Chinese telecommunications companies*** –United States House Permanent Select Committee on Intelligence (HPSCI), Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Huawei and ZTE, October 8, 2012

(U) **HPSCI Recommendation:** Private-sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with Huawei for equipment or services. US network providers and systems developers are also strongly encouraged to seek other vendors for their projects. Based on available information, Huawei cannot be trusted to be free of foreign state influence and thus poses a security threat to the United States and to our systems.

(U) **Overview:** The threat posed to US national-security interests by vulnerabilities in the telecommunications supply chain is an increasing priority given the country's reliance on interdependent critical infrastructure systems, the range of threats these systems face, the rise in cyber espionage, and the growing dependence all consumers have on a small group of equipment providers. China has the means, opportunity, and motive to use telecommunications companies for malicious purposes. Suggested "mitigation measures" cannot fully address the threat posed by Chinese telecommunications companies providing equipment and services to US critical infrastructure.

(U) **Findings:** The Committee finds Huawei **did not**:

- **Fully cooperate with the investigation** and was unwilling to explain its relationship with the Chinese Government or CCP, while credible evidence exists Huawei fails to comply with US laws.
- **Explain its relationships with the Chinese Government**, and its assertions denying support by the Chinese Government are not credible.
- **Explain what the Party Committee does** on behalf of the Party or which individuals compose the Committee.
- **Provide information** about the Chinese Government's 1999 investigation of the company for tax fraud, which exemplifies a company that refuses to be transparent.
- **Revile sufficient details or supporting documentation** on its operations, financing, and management in the United States, undermining its claims of being a completely independent subsidiary of Huawei's parent company in Shenzhen, China.
- **Provide details of its operations** in Iran, though it denied doing business with the Government of Iran, and did not provide evidence to support its claims that it complies with all international sanctions or US export laws.
- **Provide details on its Research and Development (R&D) programs**, and other documents, undermining its claim that Huawei provides no R&D for the Chinese military or intelligence services.



(U) HPCSI Conclusion: Huawei exhibits a pattern of disregard for the intellectual property rights of other entities and companies in the United States. Huawei employees provided evidence of ostensibly illicit behavior by Huawei

(U//FOUO) T his product was prepared by the FBI Strategic Partnership Unit (CD-4F). Please provide any questions or comments to your local Strategic Partnership Coordinator (SPC) or CD-4F at Strategic_Partnerships@ic.fbi.gov.

(U) Key Intelligence Questions

(U) If you have any information that would help answer the following Key Intelligence Questions or would like additional information, please contact your local FBI Strategic Partnership Coordinator or FBI field office.

(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? Which specific titles/positions within your company work with individuals from foreign companies? How is this access being exploited by your partners? What processes do you use with regard to your due diligence when vetting potential foreign partners?

(U//FOUO) **Foreign Government Activities:** Describe the nature of foreign government involvement in your industry overseas. Please be as broad as government-funded R&D programs or as specific as exact offices/positions within a foreign company that liaise with their government representatives.

(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 entry to your facility or access to your classified, trade secret, and proprietary information by a group or individual, have you experienced any attempts by these individuals to circumvent your actions (e.g., gain access to your facility, information, or personnel by other means?). If so, please explain. Have foreign businesses or groups/employees suggested or attempted to circumvent US law, regulation, company security systems. or policies, and if so, how?

(U//FOUO) **Visitors or Others Collecting Information:** What are the positions or titles of foreign representatives who contact your company? Why are you typically contacted? Are there certain members of visiting delegations who tend to ask most of the questions when you are hosting groups to your facility? If so, please identify these individuals. Are questions submitted in advance or asked randomly? What are other ways you receive unsolicited requests for information? How are requests for visas and visits handled and documented?

(U//FOUO) **Targeted Technology:** What technologies do you want to protect from your competitors (e.g., R&D, supply chain, pricing and customer service information, contracts, production and maintenance records, etc.)? Do you believe you are adequately protecting them? Can you rank these items by level of importance? What information or technology (including expertise in manufacturing, production, or operations) are foreign competitors lacking that keeps them from being competitive? Identify the various applications (both military and commercial) of your product or service.

(U//FOUO) **Criminal and Suspicious Activities:** Describe 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) **Visitors:** What are the most common type of questions you receive when you are hosting foreign and domestic visitors and groups to your facility? I s there a distinct difference between these two groups in the type of questions they ask? What questions stand out as suspicious?

(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 (if applicable)?

(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.

(U//FOUO) **Mergers/Acquisitions:** Has your company been approached for a merger or acquisition opportunity by a foreign competitor? If so, please explain the circumstances.

(U) Sources

1. (U) HPSCI; 08 OCT 2012; (U) Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE.

2. (U) Intelligence and Security Committee Presented to Parliament by the Prime Minister on behalf of Her Majesty; JUN 2013; (U) Foreign involvement in the Critical National Infrastructure: The implications for national security.

3. (U) USCC; JAN 2011; (U) The National Security Implications of Investments and Products from the People's Republic of China in the Telecommunications Sector.

4. (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.

5. (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.

6. (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/

7. (U) Counter-espionage Law of the People's Republic of China; 01 NOV 2014; Standing Committee of the National People's Congress; http://news.xinhuanet.com/politics/2014-11/01/c_1113074346.htm

8. (U) Reuters, http://www.reuters.com/article/2013/01/31/us-huawei-skycom-idUSBRE90U0CC20130131

9. (U) The Washington Free Beacon; http://freebeacon.com/national-security/chinese-military-linked-telecom-firm-shipped-u-s-equipment-to-cuba/

10. (U) ABC News; 29 OCT 2013; Government maintains NBN ban on Chinese telco Huawei after security briefings; http://www.abc.net.au/news/

11. (U) MANDIANT; APT1-Exposing One of China's Cyber Espionage Units.