Issue: 2012: Vol. 11, No. 2, Commentary

Commentary: The U.S. House Intelligence Committee Scapegoats Huawei

Article Author(s)

William Abbott Foster

William Foster, Ph.D. is a Senior Research Associate with the Center for International Strategy, Technology and Policy, Sam Nunn School of International Affairs, Georgia Institute of Technology, Atlanta, GA.

More Articles by the Author »

2012: VOL. 11, NO. 2, COMMENTARY

Editor's Note

Growth and Corruption in China

The 18th Party Congress: A Turning Point in Chinese Politics?

A Short History of the Party Congresses

An International Equity Exchange for China? Considering the Options

Commentary: Demonization of China Puts U.S. Interests in Jeopardy

>On October 8, 2012, the U.S. House Select Committee on Intelligence issued a report warning all American companies against using equipment from the Chinese telecom manufacturers Huawei and ZTE. The Committee report is available at: http://templatelab.com/huawei-zte-investigative-report/

The report argues that Huawei and ZTE's' ability to out-compete U.S. and European telecom providers was due to financial support from the Chinese government. The Committee said that this support gave the Chinese People's Liberation Army (PLA) and the Ministry of State Security the ability to force Huawei and ZTE to put "trap doors" in equipment that they sell to American companies and the U.S. government. Electronic trap doors would open a channel for transmission of information, presumably to the Chinese security apparatus. The report makes the claim that if American critical infrastructure is built with Chinese equipment, it cannot be considered secure.

The reality is that U.S. government agencies, hi-tech firms, and universities have already been penetrated by Chinese hackers working at cross-purposes with Huawei and LTE. It is important to point out that there is no evidence that Huawei has had anything to do with these breaches. Instead of dealing with the role of China's hackers and their Chinese People's Liberation Army sponsors, the U.S. House Intelligence Committee has made Huawei the scapegoat for the American government's inability to protect American companies from real threats.

The House Intelligence Committee report claims that Huawei and ZTE were not responsive to questions the Committee's researchers asked when visiting Shenzhen, China, and when called before the Committee during Congressional hearings. According to a source familiar with the visit to China, Huawei gave the researchers access to a wide assortment of decision-makers who did their best to explain a company and a culture which is very different from most in America. The report makes much of the fact that Huawei has a "Communist Party cell" on its premises. The report does not mention the fact that many multinationals in China have "Communist Party cells." It likewise does not cite academic research on the role of such cells.

The Committee also tried to show that Huawei's success was due to "special financing" from the Chinese Development Bank. What the Committee did not point out was how the Chinese Development Bank funding has gone not to Huawei but to many African countries that have begun to move from abject poverty to the possibility of prosperity. Loans from the Development Bank funded purchases of Huawei equipment to build cell phone telecommunications systems in these countries. It can be argued that Huawei's efforts in Africa have had a bigger impact on the continent than any U.S. aid effort.

Given the realities of current U.S. politics, the inability of the Congress to pass cyber-security legislation that could address the growing problem of Chinese cyber-espionage against U.S. hi-tech firms, and the pressure to protect domestic industries such as the U.S. communications giant Cisco, one must wonder whether the Committee went fishing for any sign that could be used as evidence that Huawei was controlled by the Chinese government and could not be trusted to supply infrastructure in the United States.

The Committee report digs up issues that have been brought up over and over, such as Huawei's work with an Iranian telecommunications company, an intellectual property lawsuit with Cisco and a suit regarding a couple of its associated employees working at Motorola. These are difficult accusations for Huawei to respond to under oath. My recommendation to Huawei is to admit that its governance structure has matured as it has become a global company. It has learned from mistakes and has resolved these issues in court. It has now created a company that adheres to all U.S. government rules and regulations and can be trusted by its competitors, suppliers and clients.

Though the Intelligence Committee report raises all sorts of questions about Huawei and ZTE's inability to explain their relationship with the Chinese government, after a year of investigation the Committee and the U.S. intelligence community have not been able to find one instance of Huawei or ZTE putting a back door in equipment they installed for a U.S. customer.

The report never touches on why Huawei has been so successful. It is a well-known fact that Huawei has a fanatical commitment to its customers. It has a well-earned reputation for integrating its customers' legacy systems into Huawei's existing systems, no matter how difficult and complex the integration effort. The basic

fact is that U.S. companies such as Motorola and Cisco just cannot compete with Huawei in terms of offering such custom solutions because of the high price of their programmers.

The case can be made that Huawei is so powerful in Chinese society that
the PLA simply does not have the clout to make Huawei do something that would run counter to the company's intense loyalty to its customers. Though much is made of Huawei President Ren Zhengfei's work as a PLA engineer and his immense "guanxi," or personal relations with power brokers in China, the U.S. Intelligence Committee report does not explore Huawei's claim that President Ren has deep Confucian morals and would not do anything, such as violating his relationships with his customers, that would be inconsistent with those values. Also Huawei's Chinese employees have most of their salaries tied to corporate profit-sharing, and most have hopes of becoming rich through stock ownership. They do not want to jeopardize their material dreams by doing anything that would lead to the discovery that Huawei had installed trapdoors for the People's Liberation Army into Western telecom equipment.

The House Intelligence Committee Report does not explore the intensely competitive environment of telecom in China in 1998, and how Huawei built its success by providing legacy solutions that incorporate emerging technologies that are perfect for the African, Asian and East European telecom markets. Huawei's "multi-mode" solution allows telecom companies to switch CDMA,WCDMA, GSM, WiMAX and LTE out of one box. Competitors such as Ericsson sell their customers separate boxes for each protocol. Huawei developed a business model based on being able to integrate any legacy system and provide a pathway to the latest technologies.

Sprint, for example, was desperate for Huawei's multi-mode solution, which even supported the Nextel-Integrated Enhanced Network (iDEN) protocol, a technology that Sprint needed to support because of a merger. Huawei bid $6 billion to upgrade the Sprint network while Ericsson bid $8 billion. The U.S. government opposed the Huawei-Sprint deal and then Secretary of Commerce Gary Locke intervened to make sure that Sprint went with Ericsson. The stock market did not react favorably to the forced Ericsson deal, and Sprint's stock value went down by 25% the quarter the deal happened.

Where does this leave Huawei? It was on track to becoming a $100 billion, highly profitable employee-owned company. These plans have been dashed as countries such as Australia have started to follow the U.S. in blacklisting Huawei as a national threat. Huawei has responded by focusing on making low-margin smart phones and tablets, and has become less profitable as a company.

It can be argued that a couple of years ago, Huawei had the opportunity to convince both the U.S. National Security Agency and the Chinese Communist Party that it was the ideal partner to provide secure technology for the global cloud.

The irony is that Huawei's technology could have been employed to protect the U.S. against real Chinese and other threats. Tony Rutkowski, one of the world's leading techno-diplomats, points out that the capability that the House Intelligence Committee attributes to Huawei is just what Huawei needs to address the new kinds of computer threats that we face. In Rutkowski's eyes, Huawei needs to be able to simultaneously update all firmware and software in its communication equipment worldwide in response to identified threats. This capability should be seen as an asset that makes Huawei a critical partner in the

implementation of the U.S. government's STIX automated threat-sharing system.

What few realize is how difficult it will now be to build a resilient global cloud, now that America has poisoned its relationship with the world's major telecom manufacturer.

Disclaimer:

William Foster reports that he has received no funding from Huawei, the U.S. government, or any private entity for his research on Huawei apart from a $5,000 grant from International Data Corporation (IDC) four years ago for a study of Huawei's development of a communications protocol called IMS (IP Multimedia Subsystem). The study was published by IDC.