Opening Statement for Chairman Rogers

Hearing on Threat Posed by Chinese Telecommunications Companies

September 13, 2012

As Prepared

- We invited these companies today as part of our ongoing investigation into the threat posed to the United States by telecommunications equipment manufactured by companies with believed ties to the Chinese government.

- Huawei and ZTE have become dominant global players in the telecommunications market leaving the world increasingly dependent on their telecommunications goods and services.

    - They do not yet dominate the U.S. market, but they seek to expand their footprint here.

    - They reap the benefit of billions of dollars in Chinese government financing, and nicely implement Beijing's explicit desire to be dominant in what China calls a "strategic sector."

    - We have heard reports about backdoors or unexplained beaconing from the equipment sold by both companies. And our sources overseas tell us that there is a reason to question whether the companies are tied to the Chinese government or whether their equipment is as it appears.

    - We have heard reports about their attempts to steal the tradesecrets of other companies, which gives them a competitive advantage and makes us question their ability to abide by any rules.

- At the same time, Chinese intelligence efforts against the United States are growing in scale, intensity, and sophistication.

    - Chinese actors are also the world's most active and persistent perpetrators of economic espionage.

- U.S. firms and cybersecurity specialists speak about an on-going onslaught of sophisticated computer network intrusions originating in China, that are almost certainly the work of, or done at the backing of, the Chinese government.

- Chinese intelligence services and private companies often use Chinese citizens with direct access to corporate networks to steal trade secrets and other sensitive proprietary data.

- Americans have become increasingly dependent on computer networks for every aspect of our lives. Our personal information, our banking information, our transportation infrastructure, medical records, education systems, and government all depend on computer networks.

- We must have trust and confidence in these networks. But those networks are already under attack. As General Alexander, head of U.S. Cyber Command, has recently explained, the U.S. has experienced a 17-fold increase in cyber attacks between 2009 and 2011.

    - Defending against the risk of cyber attacks becomes a bigger challenge when the system itself cannot be trusted. When the equipment and software is provided by companies we cannot trust, then we must constantly worry whether our systems our going to work against us.

    - A sophisticated nation-state actor like China has the motive to tamper with the global telecommunications supply chain, and the United States is a significant priority.

        - The ability to deny service or disrupt global systems allows a foreign regime the opportunity to exert pressure or control over critical infrastructure on which our country depends.

        - The ability to maliciously modify or steal information from government and corporate entities provides China access to expensive and time-consuming research and development that assists China's place in the world.

    - Huawei and ZTE provide a wealth of opportunities for Chinese intelligence agencies to insert malicious hardware or software implants into critical telecommunications components and systems. And under Chinese law, ZTE and

Huawei would likely be required to cooperate with any request by the Chinese government to use their systems or access for malicious purposes.

- When vulnerabilities in the equipment, such as backdoors and malicious code, can be exploited by another country, it becomes a priority national security concern.
    - Every piece of this equipment, every code of software, every update, provides that country a means to act against the United States.
    - We must trust our systems if we hope to fulfill the government's most-basic duty to maintain a defense against potential foreign aggression.

- We must get to the truth and see if these companies are tied to or influenced by the Chinese government; whether they provide a means for further economic and foreign espionage by a foreign nation-state known to be a major perpetrator of cyber espionage.

- In February 2011, Huawei issued an open letter to the U.S. government requesting a full investigation into its corporate operations to try to convince us that there is no threat.
    - We decided to give Huawei that investigation.

- In the course of the investigation, the Committee has been disappointed that the companies provided little actual evidence to ameliorate the Committee's concerns.
    - In particular, they did not provide documentation supporting or confirming their claims about their formal relationships or regulatory interaction with Chinese authorities, corporate structure, ownership, operations, or management.
    - We were willing to work with both companies, to find a reasonable way to answer our documents requests. But the companies refused, apparently because to turn over internal corporate documents would potentially violate China's state-secret laws. It is strange the internal corporate documents of purportedly private sector firms are considered classified secrets in China. This fact alone gives us a reason to question their independence.
    - We hope that this hearing finally gives us the opportunity to get fulsome answers and resolve these doubts about your companies.