The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 3761 | OCTOBER 23, 2012

China Cyber Threat: Huawei and American Policy Toward Chinese Companies

Derek Scissors and Steven Bucci

On October 8, the House Permanent Select Committee on Intelligence released a report, *U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*. The report concluded that using telecommunications hardware and infrastructure from these two firms entails a risk to American economic and national security.[1]

While Congress and the Administration should favorably consider important aspects of the report, they must not use it as an excuse for protectionism. Telecom is one of the few industries where national security concerns are sharp. Most Chinese firms do not pose a threat to American security and in fact offer investment and trade benefits to the U.S.

China Cyber Threat. It is not surprising that Chinese intelligence and military services are trying to steal American military blueprints and data. The report cites several studies that point to the People's Republic of China (PRC) as the greatest source of cyber attacks and intrusions. These incidents are often widespread and coordinated, suggesting state involvement or even leadership.

Examples include the first known large-scale act of cyber espionage, Titan Rain, in which China-based hackers broke into the networks of the Departments of State, Defense, Energy, and Homeland Security, as well as the networks of defense contractors, stealing an estimated 10–20 terabytes of data.[2] Additional espionage campaigns are thought to have infiltrated thousands of computers across dozens of countries and international organizations to steal information for the PRC.[3]

Chinese hackers also steal private-sector technology and intellectual property. Computer security company McAfee very roughly estimates the cost of global cyber crime to be as high as $1 trillion annually. McAfee competitor Symantec adds that U.S. companies lose $250 billion in intellectual property a year, which may be a low estimate.[4]

Chinese commercial espionage is more than a decade old and has no easy solution. It is perhaps best illustrated by the sustained infiltration of Canadian telecom company Nortel, which was then followed by a jump in the technological level and competitiveness of Chinese telecom companies such as Huawei and ZTE.[5]

Huawei and ZTE. While Huawei and ZTE seem to have benefited, that does not mean they engaged in the Nortel hack or other cyber intrusion. A key challenge for U.S. policymakers is deciding how the poor Chinese national record should bear on individual Chinese firms. Here, the nature of the telecom sector matters a great deal.

Huawei and ZTE deal in the hardware, infrastructure, and integrated software that undergird the cyber realm. Unlike normal cyber threats, when networks are compromised through social engineering attacks or by software holes, Huawei and ZTE could in theory purposefully include and conceal holes in the underpinnings of computer systems. Software programs are relatively easy to update or replace; the threat of embedded and exploitable gaps would be more difficult to mitigate, and the affected organizations might never realize that infiltrations are occurring.

American critical infrastructure relies on telecommunication.

This paper, in its entirety, can be found at **http://report.heritage.org/ib3761**

Produced by the Asian Studies Center

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

A Disturbing Trend

2001: Two people funded by state-owned Datang Telecom indicted for stealing secrets from Lucent.

2002: Two people funded by Hangzhou city government indicted for stealing secrets from four firms.

2003: PetroChina employee arrested for attempting to steal seismic imaging software from Silicon Valley firm (later pled guilty).

2004: Canada's Nortel discovers that China-based hackers have compromised its entire network.

2005: Chinese national working at U.S. unit of Dutch firm AkzoNobel begins stealing material needed to replicate advanced industrial coating.

2006: Two people indicted for stealing proprietary information from auto parts maker Metaldyne and seeking to pass it to Chinese firms.

2007: Chinese national employed by Dow begins transferring trade secrets to Chinese government-controlled institutes.

2008: Former DuPont employee picked by state-owned Pangang to make titanium dioxide, supposedly using DuPont production method (later pled guilty to espionage).

2009: Ford Motor employee arrested for stealing trade secrets—later found guilty—supposedly on behalf of Beijing Auto.

2010: Dozens of multinationals disclosed as targeted in China-based hacking of Google.

2011: American Superconductor sues top Chinese turbine maker Sinovel for stealing software used to drive wind turbines.

2012: NSA director acknowledges that China-based hackers compromised a company that provides computer security services to defense firms such as Lockheed Martin.

Chinese hackers could use a deliberately placed subroutine or hardware modification to alter the flow of financial information, disrupt the electric grid, or take other actions to damage the U.S.

In addition, money could be siphoned or technology stolen from American companies and individuals. There is a track record for this: Huawei has been accused of stealing intellectual property from Cisco, while ZTE has been accused of stealing intellectual property by Huawei.[6]

Many countries consider telecom to be sensitive. China is one of them, having declared telecom to be an area for absolute state control. Beijing thus deems Huawei and ZTE (and all other entities in the sector) entirely under state direction. Huawei claims to be independent—ZTE does not—but the PRC government disagrees.

Moreover, were Huawei to resist government orders to try to undermine American economic and national security, it would have no legal recourse: Chinese courts are completely controlled by the Communist Party. If Huawei actually tried to act independently, it would be crushed very quickly.

1. *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, House Permanent Select Committee on Intelligence, 112th Congress, 2nd Sess., October 8, 2012, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf (accessed October 22, 2012).
2. Nathan Thornburgh, "The Invasion of the Chinese Cyberspies," *Time*, August 29, 2005, http://www.time.com/time/printout/0,8816,1098961,00.html (accessed October 16, 2012).
3. "Major cyber spy network uncovered," BBC News, March 29, 2009, http://news.bbc.co.uk/2/hi/americas/7970471.stm (accessed October 16, 2012), and Dmitri Alperovitch, "Revealed: Operation Shady RAT," McAfee, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf (accessed October 16, 2012).
4. Rich Dandliker, "Putting a Face on Intellectual Property Theft," Symantec, July 11, 2012, http://www.symantec.com/connect/blogs/putting-face-intellectual-property-theft (accessed October 16, 2012), and "America's Top Cyberwarrior Says Cyberattacks Cost $250 Billion a Year," *International Business Times*, June 13, 2012, http://www.ibtimes.com/americas-top-cyberwarrior-says-cyberattacks-cost-250-billion-year-722559 (accessed October 16, 2012).
5. Derek Scissors, "Chinese Commercial Espionage: U.S. Policy Recommendations," Heritage Foundation *Issue Brief* No. 3564, April 9, 2012, http://www.heritage.org/research/reports/2012/04/chinese-commercial-espionage-us-policy-recommendations, and Siobhan Gorman, "Chinese Hackers Suspected in Long-Term Nortel Breach," *The Wall Street Journal*, February 14, 2012, http://online.wsj.com/article/SB10001424052970203363504577187502201577054.html (accessed October 16, 2012).
6. Michael Lee, "Cisco issues legal challenge to Huawei, tiptoes US-China dispute," *ZDNet*, October 12, 2012, http://www.zdnet.com/cisco-issues-legal-challenge-to-huawei-tiptoes-us-china-dispute-7000005657/ (accessed October 16, 2012), and Wang Jiapeng, "Huawei Sues ZTE on IPR Infringement," *Caixin Online*, April 29, 2011, http://english.caixin.com/2011-04-29/100254224.html (accessed October 16, 2012).

Fixing the Problem. The Intelligence Committee's main finding is correct: Huawei and ZTE should not be considered reliable partners for work involving sensitive systems. It is equally true that the particular nature of telecommunications means that the Committee's finding should not be extended to other industries where there is no equivalent to cyber attack. There was a rush of Chinese investment into the U.S. in the first half of 2012, benefiting America considerably and bringing no security threat.[7]

Other public- and private-sector decisions are considerably more difficult. When national security is not involved, the private sector should take the lead on how best to respond to cyber and intellectual property threats. These will vary by sector and by company and should not be evaluated at the level of national policy.

Beyond the U.S., American telecom and computer systems are connected to those of our military allies. Huawei has done considerable business in Britain, for example. Do the operations of Chinese telecoms in countries that are U.S. allies constitute an indirect threat to the U.S.? If so, what is the best way to meet this threat?

The question has multiple dimensions, and answering it will require extensive coordination within the Administration and with Congress:

1. Huawei, ZTE, and other Chinese telecoms should not be permitted to conduct business in areas deemed truly vital for American national security. This prohibition is derived in part from the nature of telecommunications and should not be expanded.

2. Most Chinese companies should be welcomed to trade with and invest in the U.S.

3. It would be valuable to extend the House Intelligence Committee's work to the matter of Chinese telecom business with American allies. Such an extension could be led by the Department of Defense and coordinated with multiple branches of government.

Proceed with Care. Huawei and ZTE exist at the discretion of the Chinese government. Therefore, it is necessary for American companies and policymakers to be very cautious in dealing with them. Similar care should be exercised to ensure that national security restrictions in telecom are not extended to industries where they do not belong and where they would unjustifiably interfere with free enterprise.

*—**Derek Scissors, PhD**, is Senior Research Fellow in Asia Economic Policy in the Asian Studies Center at The Heritage Foundation. **Steven Bucci, PhD**, is Senior Research Fellow in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.*

David Inserra, a Research Assistant in the Allison Center, contributed to this report.

7. Derek Scissors, "Chinese Outward Investment: Acceleration Features the U.S.," Heritage Foundation *Issue Brief* No. 3656, July 9, 2012, http://www.heritage.org/research/reports/2012/07/chinese-foreign-investment-outward-investment-acceleration-features-the-us.