This PDF is auto-generated for reference only. As such, it may contain some conversion errors and/or missing information. For all formal use please refer to the official version on the website, as linked below.

The Evidence Supporting the Fear of Chinese Telecommunication Providers

https://www.e-ir.info/2012/10/14/the-evidence-supporting-the-fear-of-chinese-telecommunication-providers/

CLEMENT GUITTON, OCT 14 2012

On Monday 8 October 2012 a committee of the U.S. House of Representatives issued strong recommendations against doing business with two Chinese based telecommunication companies; Huawei and ZTE.[1] The two companies are the main Chinese providers of telecommunication equipment. The two first recommendations are that the US 'should view with suspicion the continued penetration of the U.S. telecommunications market by Chinese telecommunications companies', hence targeting every Chinese company; and the second one is that the 'private-sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services'. What evidence did the committee have to issue such recommendations?

Two different types of fears underpin the recommendations against Huawei and ZTE. The first one is the fear of espionage, and the second one is a fear that the companies could use their insight into critical infrastructure to affect consequential damage onto the US if a conflict between theUS and China were to occur.

Information systems play a central role for many 'critical infrastructures'. In general, the term critical infrastructure encompasses hospitals, power grids and other elements of the energy supply chain. There is a fear that it is now possible to conduct cyber attacks on critical infrastructure that would have devastating effects. Some of the fear stems from cases such as the Stuxnet worm, where the virus caused physical damage to thousands of nuclear centrifuges in Iran. However, some academics have also pointed out how the fears may have been grossly exaggerated.[2] There is currently no consensus on the level of insecurity represented by information systems for critical infrastructure.

But there is no accepted definition of critical infrastructure in the US, and this was a particular moot point when debating the Cyber Security Act. Acting against fears that cyber attacks may bring many of these critical infrastructures down, two US Senators Joe Lieberman and Susan Collins proposed the Cyber Security Act 2012. The Act would compel owners of critical infrastructure to apply specific security standards, and to report any breach to a governmental authority. The Act did not pass during the last session of the Congress, and the current Obama administration is now considering an executive order so as to ensure the security of critical infrastructure.[3] An executive order merely further extends existing law, and would be based in this case upon the regulatory authorities that already overview specific industries. The release of the report from the Permanent Select Committee on Intelligence, while potentially unrelated to the executive order, helps construct this perception of the US infrastructure facing a high threat and necessitating government involvement.

The authors of the report, Mike Rogers and Dutch Ruppersberger, do not have evidence that the two Chinese companies engage in either espionage or actions to undermine US critical infrastructure. They reversed the burden of proof, and because the two Chinese companies did not prove their innocence sufficiently, Rogers and Ruppersberger declared them a 'threat'. The authors write that 'the companies failed to provide evidence that would satisfy any fair and full investigation'.[4] An important point for the Committee was the link of Huawei with the Chinese government. According to the assumption of the Committee, Huawei would be much more likely to put backdoors in its equipment to control them if the Chinese government had a say in the company's decision. Here, a backdoor in

the equipment could allow connection onto the network that the equipment supports, and either the stealthy extraction of information or the running of commands to damage the information system. The current CEO and founder Ren Zhengfei has fueled these speculations regarding his background as a former solider in the People's Liberation Army. Huawei 'failed to explain its relationship with the Chinese government'.[5] Similarly, and following the reverse of burden of proof, the authors write 'Huawei failed to answer key questions or provide supporting documentation for its claims to be financially independent of the Chinese government', and 'Huawei failed to provide details of its operations in Iran'.[6]

Bringing evidence of the lack of integrity of Huawei or ZTE's equipment would have required the Committee to carry out a deep technical assessment of their equipment, which they did not do. It is common for telecommunication products to receive security accreditation from other independent companies. While it is possible that these audits miss out on potential backdoors inserted in companies' products, Huawei stated that the US security firm Electronic Warfare Associates has accredited many of its products.[7] This statement came in an open letter that triggered this very investigation by the Permanent Select Committee on Intelligence. In February 2011, Huawei was interested in buying the assets of a US based company that was filing for bankruptcy, 3Leaf. But following pressure from the Committee on Foreign Investment, which reviews deals causing potential threats to 'national security', the company backed away.[8] Following this demonstration of lack of trust, the Chinese firm issued a public statement calling for theUS to investigate the firm. Hence, instead of carrying technical assessments and showing evidence to incriminate the two firms, the two authors repeatedly use the conditional statements and make assumptions about the companies, such as:

'[the companies infrastructure] ***could be used*** for spying and other malicious purposes'

'Inserting malicious hardware or software implants into Chinese-manufactured telecommunications components and systems headed for U.S. customers ***could*** allow Beijing to shut down or degrade critical national security systems in a time of crisis or war'

'Malicious Chinese hardware or software implants ***would*** also be a potent espionage tool for penetrating sensitive U.S. national security systems' [emphasis added]

These assumptions, that lacked evidence, serve to construct the fear and the mistrust against the two companies, but do not show any grounds. Huawei responded to the accusations following this argument, stating that despite their 'best effort' to cooperate, the Committee based their report on rumors and speculations.[9] On the other hand, ZTE was more bold and stated that the Committee should now check most of US telecommunication companies, which use components mostly originating from China.[10]

The US is not the only country to display fear of Chinese companies. In March 2012 Australia blocked Huawei from bidding for the construction of its national broadband network, citing concerns of the Chinese companies 'stealing' information . Similarly, in October 2012, following the release of the US report, Canada also tried to block Huawei from bidding onto one of its government communication network.[11] Despite this growing atmosphere of mistrust, not all countries turned their back on the Chinese firm. The UK Prime Minister, David Cameron, had for instance declared it was 'open for business' when he met with Ren Zhengfei, Huawei's CEO.[12] Other incidents of espionage seemingly involving the Chinese government have informed this atmosphere of mistrust, such as operation Aurora or GhostNet. The incident of mistrust begets the question: how do other telecommunication companies behave, in comparison with Huawei and ZTE?

Another interesting case study is how the US-based firm Cisco, the world largest producer of computer network, behaves in China. The Chinese allegedly use Cisco products to build the Golden Shield Project, also known as the Great Firewall of China. In 2011, two complaints were filed against Cisco for helping the Chinese government to catch internal dissidents to its regime. The Chinese arrested and questioned the political writers Du Daobin, Zhou Yuanzhi and Liu Xianbin allegedly thanks to using tailor made Cisco systems.[13] One of the key pieces of evidence pointing to the involvement of Cisco is a presentation, available online, that details the potential use of Cisco products for the Golden Shield Project as being: '[to] stop network related crimes, [to] guarantee the security and services of

public network, and [to] combat "Falun Gong" evil religion and other hostiles'.[14] Cisco acknowledged its involvement in selling Chinese products but it claimed it acted while complying with US export rules, and denied that they customized them to help them catch dissidents.[15] They also noted:

Equipment supplied to China is the same equipment we provide worldwide, which includes industry-standard network management capabilities which are the same as those used by public libraries in the U.S. that allow them to block inappropriate content for children.

Huawei held the same argument about its own equipment, but it appeared to have 'failed' to convince the Committee. Cisco, Huawei and ZTE are not the only telecommunication companies to be engrained in political tensions for espionage. Another US based telecommunication provider, AT&T, is currently fighting its involvement in court in wireless taping programs that would have occurred under the Bush administration.[16] However, the court and government officials are reluctant to release any information, as they claim it could affect 'national security'.

The lack of evidence released in all four cases impedes on making an informed decision about the reality of the threat. It confuses users, business owners and government officials, and creates an atmosphere of mistrust that does not help resolve cyber security issues. As more cooperation is required to enhance cyber security on all levels, governments should hence refrain from creating fears based on an entity's failure to demonstrate that they are not guilty. Instead, they should base their argument on evidence proving that they are, whilst still promoting an exchange of information, but not complete exclusion of businesses merely based on the origin of the mother company.

—

Clement Guitton *is a PhD candidate in War Studies at King's College London. He previously worked at the International Telecommunication Union, a United Nations specialised agency, and holds two masters, one in international relations and one in electrical engineering.*

Bibliography

Brito, Jerry, and Tate Watkins. "Loving the Cyberbomb? The Danger of Threat Inflation in Cybersecurity Policy." *Mercatus Center – George Mason University* (2011).

Chandler, Mark. "Cisco Supports Freedom of Expression, an Open Internet and Human Rights." Cisco, http://blogs.cisco.com/news/cisco-supports-freedom-of-expression-an-open-internet-and-human-rights/.

Cisco Systems. "Overview of the Public Security Sector." Wired, http://www.wired.com/images_blogs/threatlevel/files/cisco_presentation.pdf.

Hansen, Lene, and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School."*International Studies Quarterly* 53, no. 4 (2009): 1155-75.

Hu, Ken. "Huawei Open Letter." 2011.

Huawei. "Statement Regarding Hpsci's Report." Huawei, http://www.huawei.com/en/about-huawei/newsroom/press-release/hw-194454-hpsci.htm.

Kravets, David. "Supreme Court Terminates Warrantless Electronic Spying Case." *Wired*, 10 September 2012.

Little, Morgan. "Executive Order on Cyber Security Builds Steam Amid Criticisms." *LA Times*, 2 October 2012.

Pfanner, Eric. "Chinese Telecom Firm Finds Warmer Welcome in Europe." *The New York Times*, 10 October 2012.

Reuters. “Australia’s Block of Huawei Is Part of Wider Concern.” *Reuters*, 28 March 2012.

———. “Huawei Backs Away from 3leaf Acquisition.” *Reuters*, 19 February 2011.

———. “Huawei Faces Exclusion from Planned Canada Government Network.” *Reuters*, 9 October 2012.

Rogers, Mike, and Dutch Ruppersberger. “Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and Zte “, 60. Washington, D.C.: U.S. House of Representatives, 2012.

Schmidt, Michael S., Keith Bradsher, and Christine Hauser. “U.S. Panel Cites Risks in Chinese Equipment.”*The New York Times*, 8 October 2012.

Wee, Sui-Lee. “Insight: Cisco Suits on China Rights Abuses to Test Legal Reach.” *Reuters*, 8 September 2011.

ZTE. “Zte’s Equipment Is Safe and Poses No Threat to Us Telecommunications Infrastructure.” http://wwwen.zte.com.cn/en/press_center/news/201210/t20121009_358022.html.

—

[1] Michael S. Schmidt, Keith Bradsher, and Christine Hauser, “U.S. Panel Cites Risks in Chinese Equipment,”*The New York Times*, 8 October 2012.

[2] Jerry Brito and Tate Watkins, “Loving the Cyberbomb? The Danger of Threat Inflation in Cybersecurity Policy,” *Mercatus Center – George Mason University* (2011); Lene Hansen and Helen Nissenbaum, “Digital Disaster, Cyber Security, and the Copenhagen School,” *International Studies Quarterly* 53, no. 4 (2009).

[3] Morgan Little, “Executive order on cyber security builds steam amid criticisms,” *LA Times*, 2 October 2012.

[4] Mike Rogers and Dutch Ruppersberger, “Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE ” (Washington, D.C.: U.S. House of Representatives, 2012), v.

[5] Ibid., 21.

[6] Ibid., 27-32.

[7] Ken Hu, “Huawei Open Letter,” (2011).

[8] Reuters, “Huawei backs away from 3Leaf acquisition,” *Reuters*, 19 February 2011.

[9] Huawei, “Statement regarding HPSCI’s report,” Huawei, http://www.huawei.com/en/about-huawei/newsroom/press-release/hw-194454-hpsci.htm.

[10] ZTE, “ZTE’s Equipment is Safe and Poses no Threat to US Telecommunications Infrastructure,” http://wwwen.zte.com.cn/en/press_center/news/201210/t20121009_358022.html.

[11] Reuters, “Huawei faces exclusion from planned Canada government network,” *Reuters*, 9 October 2012.

[12] Eric Pfanner, “Chinese Telecom Firm Finds Warmer Welcome in Europe,” *The New York Times*, 10 October 2012.

[13] Sui-Lee Wee, “Insight: Cisco suits on China rights abuses to test legal reach,” *Reuters*, 8 September 2011.

[14] Cisco Systems, "Overview of the Public Security Sector," Wired, http://www.wired.com/images_blogs/threatlevel/files/cisco_presentation.pdf.

[15] Mark Chandler, "Cisco Supports Freedom of Expression, an Open Internet and Human Rights," Cisco, http://blogs.cisco.com/news/cisco-supports-freedom-of-expression-an-open-internet-and-human-rights/.

[16] David Kravets, "Supreme Court Terminates Warrantless Electronic Spying Case," *Wired*, 10 September 2012.

About the author:

Clement Guitton is a PhD candidate in War Studies at King's College London. He previously worked at the International Telecommunication Union, a United Nations specialised agency, and holds two masters, one in international relations and one in electrical engineering.