Huawei: A Threat To National Security?

https://www.e-ir.info/2013/03/13/huawei-a-threat-to-national-security/

LUCIE KADLECOVA, MAR 13 2013

Chinese Huawei: A Real Threat To National Security?

Introduction

China's economic growth, achieved mainly in the last decade, causes the global community to be flooded not only by inexpensive goods, but also a high number of new Chinese competitors. These come from different market sectors; however, one of the spheres, the Chinese technologies industry, appears to be highly problematic with its exports abroad. In the last few years, a number of foreign governments whose markets are seen as a potential target for Chinese economic expansion have expressed their concern about the safety credibility of technologies manufactured by companies originating from China. In this regard, Huawei Technologies Co. Ltd., China's largest and fastest-growing supplier of telecommunications equipment, has been popular in recent discussion.

Huawei's economic expansion into markets in regions of Africa, Asia, Canada and New Zealand has already achieved success. However, other potentially attractive economies still resist infiltration of Huawei's technologies into their national infrastructure. In India, the company has recently been criticised by the government and the public to be a security threat and a dishonest market competitor. Furthermore, Australia blocked Huawei's attempts to take part in a newly built national broadband system in spring 2012.[1] Nevertheless, the most radical opinion on Huawei's products was expressed by the U.S. representatives who published a report dealing with the company's security credibility in autumn 2012.

Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE[2], published by the Permanent Select Committee on Intelligence on October 8, 2012, is a result of more than a year-long investigation. It was instigated by Huawei's open letter to the U.S. Government in February 2011 denying any security concerns. In order to gain trust in its equipment, the company also requested a formal investigation into its corporate activities.[3] Nevertheless, the investigation brought adverse conclusions, stating that equipment of both Huawei and ZTE represent a risk to the U.S. critical infrastructure and undermines national-security interests.[4] Moreover, according to the report,

"The United States should view with suspicion the continued penetration of the U.S. telecommunications market by Chinese telecommunications companies. U.S. government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including component parts".[5]

The Committee then addressed similar recommendations to government contractors and private-sector entities. Although Huawei immediately denied these conclusions, indicating that they are "dangerous political distractions",[6] and the Chinese Commerce Ministry even warned that the Sino-American economic and trade relations may be hurt by the report,[7] Huawei remains considered a threat to national cyber security by many foreign governments.

Therefore, the goal of this essay is to examine the arguments which are generally discussed in relation to Huawei's expansionist tendencies, and better comprehend the level of risk which the company may possess to governments whose markets it wants to economically penetrate. Are Huawei and its equipment a real threat to national cyber

security of these targeted countries that resist its deeper involvement in their markets? Or, is the critique only a gesture of excuse for their protectionist attempts? An opinion even emerged saying that the situation in which Huawei is being caught in these days suggests Japanese companies that were surpassing the U.S. automobile industry in the 1980s: the decrease of U.S. car producers and penetration of the market by foreign competitors aroused widespread panic in that time.[8]

This essay argues that Huawei can represent an actual risk to the national security of foreign states. The argument is mainly based on the assumption that the Chinese government and military, which are worldwide one of the most active culprits of cyber espionage, possess a decisive influence inside Huawei's headquarters. Although Huawei claims to be a private company free of outer control, diverse indications imply otherwise. The argument is further supported by other clues such as Huawei's unwillingness to clarify its operations.

The argument of the essay will be assessed in five steps. First of all, Huawei's profile and strategy of expansion will be presented. Second, the ties between Huawei and the Chinese government will be examined focusing, for example, on the state's support of the company. Third, the essay will discuss Huawei's lack of transparency followed by an assessment of the vulnerabilities which were exposed in the company's manufactured equipment. Finally, Huawei's questionable respect for international legal obligations will be investigated. The essay will critically evaluate the potential of Huawei to be a threat to national security in the conclusion.

Huawei's Profile and Strategy of Expansion

Huawei, based in Shenzhen, China, was established by Ren Zhengfei with no more than RMB 21,000 (about US$2,500) in capital in 1987.[9] However, the company soon started its rapid expansion from the mainly rural interior of China to the Chinese rich coast and abroad. Within ten years, its revenues achieved the amount of $250 million. Moreover, Huawei set up its first research and development centre beyond Chinese borders, in India, only twelve years after its establishment.[10] Further expansion followed, and later Huawei became the leader of China's boom of telecommunications infrastructure. Nowadays, the company, whose revenues are $32 billion, employs 140,000 employees with customers in almost 140 countries.[11] This makes Huawei the second largest supplier of network infrastructure after Sweden's Ericsson. A number of experts claims that Mr. Ren's strategy is to use the countryside in order to encircle and finally to capture the cities, and is one of the main reasons of Huawei's success overseas. The company primarily targeted peripheral markets such as those in Africa or South East Asia, undercutting its competitors by 5 % to 15 %.[12] Subsequently, Huawei started moving into more competitive markets in Europe and the USA, encountering diverse opinions on its economic expansion.

One of Huawei's most successful steps forward has been its penetration of the British market. Not only that among its UK customers belong companies such as Sky, O2 or Orange, but Huawei's investments are also welcomed by British government.[13] Nevertheless, Huawei's biggest achievement was the establishment of the 'Cyber Security Evaluation Centre' in Banbury, England, in 2010. It was set up with a fundamental goal – persuade customers and the British government that Huawei's products were reliable. The centre closely cooperates with the Government Communications Headquarters, a British signals intelligence agency, in order to assure the purchasers that the networking equipment, as well as its software, have reliable resistance against possible exploitation by cyber attacks or foreign espionage, including that from China.[14] It seems that the tactic has been convincing enough since the number of Huawei's users in the UK has grown rapidly, and the company has already promised further investments in the country.[15]

However, other competitive and attractive markets overseas see Huawei's operations in their country as a threat to national security rather than a cheap high-quality alternative to other telecommunications companies. The case of the U.S. Report, mentioned previously, is a good example of this. Moreover, in 2010, the Indian government, for instance, slapped a ban on imports of the Chinese company's networking equipment.[16] A similar situation occurred in Australia in early 2012 when Huawei was barred from bidding for cooperation on National Broadband Network, a project worth almost $38 billion. The Australian government stated that the main reason for denying the company access to the contract was security concerns.[17] Huawei's immediate counter offer to provide Australian government with unrestricted access to its codes and hardware in order to assure it of their reliability was

unsuccessful.[18] These are but a few of the most visible cases of Huawei's complications to entering overseas markets or winning a crucial contract. The similarities of these bans show that Huawei is seen by governments as a threat to national cyber security.

Huawei's Relations with the Chinese Government

Huawei's perceived potential to harm the security of foreign countries is based on multiple arguments. The following part of the essay will focus on the most serious one, which may be, however, also the most disputable. In general, a great number of analysts and policymakers consider the allegedly close links between Huawei and the Chinese government as the gravest obstacle when considering economic and trade cooperation with the company. According to these voices, Huawei, and potentially other telecommunications companies, may be used as China's tool for malicious purposes. The Chinese intelligence network is highly sophisticated and active, especially in regards to economic espionage in competitive markets such as that in the USA. Chinese cyber espionage efforts are in the majority of cases based on elaborate technologies. Their main task is to penetrate the cyber defence; perhaps, for instance, by inserting malicious software or hardware components into Huawei's manufactured telecommunications equipment meant to be exported to targeted countries.[19]

As the above mentioned report by the U.S. Congress Committee points out, there are plenty of opportunities where Chinese intelligence agencies could insert malicious components into the company's critical telecommunications equipment and systems. The Chinese government may seek collaboration from the top leaders of the said company.[20] According to experts based outside China, it even seems that current Chinese law may oblige companies such as Huawei to cooperate with China's government and allow them access to their manufacturing under a cloak of national security.[21] Then, it would be very simple for the Chinese intelligence agency to insert malicious implants into the company's manufactured components and systems. Nevertheless, in case the leadership of the company refuses the cooperation, recruitment of technicians in factories by Chinese intelligence agencies would be enough for the malicious purposes.[22] Subsequently, the Chinese intelligence implants would be a useful tool for penetration of targeted national systems and access to their networks containing sensitive economic data.

It is crucial, however, to mention that there has been no specific evidence that Huawei has or would actually cooperate with the Chinese government. Moreover, Huawei claims that it would not have any ties to the government in general.[23] On the other hand, a lot of industry analysts believe that there exists proof suggesting otherwise. As an example, they point to the past of Mr. Ren, the founder of Huawei. Ren Zhengfei attended the Chongqing University of Civil Engineering and Architecture in the 1960s.[24] After his graduation he worked as a civil engineer until 1974, when he decided to accept a job in the military's Engineering Corps. He became a member of Chinese army there and cooperated on the construction of the Liao Yang Chemical Fiber Factory. Subsequently, he was offered a post of Technician, Engineer and Deputy Director, which did not, however, include any military rank. As a result of his bright career, he was invited to the National Congress of the Communist Party of China in 1982. He was retired from the Chinese military in 1983 and, after being discontent with his job, he decided to establish Huawei in 1987.[25] Nevertheless, Mr. Ren's personal and professional links, which he developed during his career in the People's Liberation Army, can continue to these days and may influence Huawei's contracts overseas.

Besides Mr. Ren's military career, there are still other reasons to maintain the suspicion of Huawei's close relations with the Chinese government and army. One of them is the supposed financial support from the government following the proclamation of Huawei as a 'national champion'. As the*2011 Report to Congress of the U.S.-China Economic and Security Review Commission* outlines, there are diverse types of ownership in China, depending on the latitude of the control which the state executes. Moreover, it is difficult to quantify the extent of the state's influence on the company. The report continues by claiming that Huawei belongs among those companies which assert to be private even though they are actually influenced by the state's power whilst enjoying special market privileges.[26] It cannot be ignored that Huawei works within one of China's main strategic sectors, which the government cherishes as the centre of China's national interests. In these sectors, the dominating 'national champions' enjoy special favouritism such as favourable commercial loans, market support and tax programmes.[27] With respect to Huawei's proclamation that the company resides in the Shenzhen Special Economic Zone, which secures that it operates within a market economy,[28] doubts about its financial independence from China's government remain.

Lastly, regarding the supposed links between Huawei and the Chinese government and military, the company acknowledges that the Chinese Communist Party keeps an internal Party Committee within Huawei's organizational structures.[29] This fact is of particular concern for foreign governments whose markets are Huawei's potential customers. Due to this Party Committee, the Chinese government could exercise its influence on the leadership of the company. Huawei's argument of defence is that all Chinese business institutions must keep a Party apparatus within its structures. This may be legitimate only if the company provides the public with more information regarding the members of the Committee or its job sheet.[30]

Lack of Transparency

The lack of cooperation, together with an unwillingness to share more data on the company's structures or decision-making procedures, are the second most commonly stated arguments by critics worried about allowing Huawei to enter their markets. Their line of reasoning can be illustrated by the two following examples. Firstly, Huawei claims to be a private, employee-owned company. The shares of the company are allocated solely to Chinese employees of Huawei, which is justified by the prevailing legal issues in China where the company resides.[31] This discrimination towards non-Chinese employees from participating in the company's stocks undermines Huawei's claims to be truly an employee-owned entity. Subsequently, this fact can arouse doubts about the structure of the company's ownership, which has happened in the case of the U.S. Congressional Committee investigation conducted in 2012. Huawei refused when asked to provide, for instance, a list of the ten largest shareholders of the company.[32] Therefore, Huawei's customers still cannot be really sure who actually controls the company. Huawei claims that 1.42 % of the shares belong to Mr. Ren and the rest are held by employees. Their participation in the stock is moderated by a shareholder's union that is administered by an elected committee. The question remains what the powers of this decision-making apparatus are and who sits on it, since the company again does not want to provide any further information.[33]

Secondly, Huawei is reluctant to release deeper information concerning its Board of Directors and its members. This is crucial since the decision-makers sitting on the Board possess key authority and may possibly have ties to the Chinese government. In this regard, Mr. Ren's succession has been discussed recently. Since the company declares that it urges corporate-governance reforms, it was expected that one of Ren's closest co-workers, possibly a member of the Board of Directors, would be his heir. The contrary seems to be true because Mr. Ren wants his son, Ren Ping, to take over his position in Huawei's leadership.[34] This event is publicly perceived as a step backward rather than an attempt for a trouble-free takeover.

Therefore, it appears that Huawei is trying to preserve its culturally Chinese character while also trying to expand into Western markets that have a different value system. The obstacles become more apparent when customers request broader transparency, which they have lacked so far. The deficit of more detailed internal information undermines Huawei's credibility.

Controversy About Vulnerabilities

The third concern of Huawei's critics is a potential threat posed to customers by alleged vulnerabilities of the company's manufactured equipments. Since at least part of Huawei's components may be used in the telecommunications supply chain, it is of high importance for national security that the amount of vulnerabilities is as marginal as possible. However, it can appear that the quantity found in Huawei's products might cause serious threat to the national critical infrastructure of the customers, eroding the necessary trust in the company.

A reported study by cyber expert Felix Lindner illustrates the issues of vulnerabilities in the case of Huawei. Lindner's analysis focused on the company's routers, discovering multiple vulnerabilities. According to Lindner, it was five times easier to find a weak place in a router manufactured by Huawei than in the one by Cisco; he also pointed out that the vulnerabilities were probably a consequence of poor coding, rather than an endeavour of espionage.[35] According to some critical experts from the U.S. government, Huawei's vulnerabilities, and its seemingly poor security procedures, simply cover purposely-built backdoors. These might be possibly used in future attacks to infiltrate targeted systems, install malicious software, and spy on sensitive information such as

technologies or trade secrets.[36] This argument is strengthened by the Chinese reputation as a regime that represents a highly active threat of espionage to many foreign countries.[37] On the other hand, Huawei's defenders argue it is unlikely that the company would provide customers with equipment containing a backdoor which would be detected in an attack. This behaviour would subsequently culminate in total loss of purchasers' confidence in the company.[38]

Therefore, any unified opinion on the issue of vulnerabilities in Huawei's equipment has not been expressed so far. The only fact which is commonly acknowledged is the lack of transparency regarding security concerns. Felix Lindner illustrated this by arguing that Huawei, for instance, does not publish any security advisories and does not operate a contact that customers could use to report a security vulnerability.[39]

Questionable Respect for International Legal Obligations

Critics of Huawei also highlight that the company does not respect the political and legal rules of those countries whose markets it is about to target. This is not necessarily a threat to national security, but it undermines Huawei's image of a respectable business entity. As examples of this behaviour, two cases are discussed most frequently: Huawei's contracts with Iran, and the company's disregard for intellectual property rights.

Firstly, Huawei refuses accusations that it does trade with the Iranian government, which is currently under international sanctions. The company claims that it is determined to limit its future operations in Iran, but fails to provide the public with any detailed information about its contracts there. Huawei even states that it plans to respect its current contracts with Iranian customers.[40] This behaviour results in the fact that international society sees Huawei's business interests as suspicious.

Secondly, Huawei's official open letter to the U.S. Congressional Committee claims that it had applied for more than 49,000 patents in total, and had been awarded almost 18,000 of them by the end of 2010. It also states that besides their own innovation research, it buys licences to access other patent technologies. The company was said to have paid $222 million in licensing fees in 2010 alone.[41] Although these numbers may indicate that Huawei has recently been one of the most productive sources of intellectual property worldwide, it becomes impossible not to avoid rumours and accusations of stealing intellectual property from other technological developers. Huawei often builds its defence on the broad expansion of research and development centres, but again fails to provide any deeper information.[42]

Huawei's business in Iran and supposed disregard for the intellectual property rights of other entities exemplifies why foreign governments think the company does not respect international legal obligations and business standards. This subsequently casts a shadow upon its requests for deeper cooperation in overseas markets.

Conclusion

This essay has examined whether Huawei, the second largest telecommunication company in the world, is a real threat to the national security of other countries as it has recently been proclaimed by several overseas governments. The study focused on four broad arguments which are discussed most often in regard to this issue. These are the level of links between Huawei and the Chinese government and army, the company's reluctance to share concrete information on its structure and decision-making, its poor security practices, and its respect for international legal and political standards.

The examination of all arguments revealed that, although there is no clear proof that Huawei directly cooperates with Chinese communist regime, the circumstantial evidences suggests that Huawei's operations are of high concern to foreign governments and their national security. Furthermore, this outcome is supported by other potentially dangerous detections, such as the significant number of vulnerabilities in the company's equipment. Huawei's unwillingness to provide the public with more information on its structures, leadership or market operations simply further undermines the image of a respectable and trustworthy company. For all these reasons, Huawei is more likely to be seen as a threat to national security rather than a victim of a foreign state's protectionism.

Huawei may gain trust by establishing other Cyber Security Evaluation Centres, such as it did in the UK in 2010. Nevertheless, it is probable that it would not be an adequately satisfying solution for all potential customers and their critical telecommunications infrastructure. Other possible solutions for winning the trust of overseas governments would certainly be Huawei's broader openness, transparency and responsiveness for international legal obligations.

Bibliography

Anderson, Richard. 'Huawei Technologies: Controversial Success Story.' *BBC*, 12 September 2012. Accessed 26 November 2012. http://www.bbc.co.uk/news/business-19568465.

Backaler, Joel. 'Viewpoint: Why Chinese Firms Buy Western Rivals.' *BBC*, 28 February 2012. Accessed 27 November 2012. http://www.bbc.co.uk/news/business-17197907.

Constantin, Lucian. 'Hackers Reveal Critical Vulnerabilities in Huawei Routers at Defcon.' *Computer World*, 30 July 2012. Accessed 30 November 2012. http://www.computerworld.com/s/article/9229785/Hackers_reveal_critical_vulnerabilities_in_Huawei_routers_at_Defcon.

Gorman, Siobhan and Paul Mozur. 'China Warns Huawei Report Could Harm U.S.-China Relations.'*The Wall Street Journal*, 9 October 2012. Accessed 1 December 2012. http://online.wsj.com/article/SB10000872396390443982904578046530208663580.html.

Hesseldahl, Arik. 'Why America Is Really Worried about Huawei.' *All Things*, 8 October 2012. Accessed 1 December 2012. http://allthingsd.com/20121008/why-america-is-really-worried-about-huawei/?KEYWORDS=Huawei.

Kang, Cecilia. 'Huawei's U.S. Competitors among Those Pushing for Scrutiny of Chinese Tech Firm.'*Washington Post*, 11 October 2012. Accessed 30 November 2012. http://www.washingtonpost.com/business/technology/huawei s-us-competitors-among-those-pushing-for-scrutiny-of-chinese-tech-firm/2012/10/10/b84d8d16-1256-11e2-a16b-2c110031514a_story.html.

Ken Hu. *Huawei Open Letter*. The Wall Street Journal. Undated (2011). Downloaded 27 November 2012. http://online.wsj.com/public/resources/documents/Huawei20110205.pdf.

Kroft, Steve and Graham Messick. 'Huawei Probed Security, Espionage Risk.' *CBS News*, 7 October 2012. Accessed 30 November 2012. http://www.cbsnews.com/8301-18560_162-57527441/huawei-probed-for-security-espionage-risk/?tag=currentVideoInfo;videoMetaInfo.

Lee, John. 'The Other Side of Huawei.' *Business Spectator*, 30 March 2012. Accessed 27 November 2012. http://www.businessspectator.com.au/bs.nsf/Article/Huawei-CCP-China-NBN-broadband-pd20120330-SV8JB?OpenDocument&emcontent_spectators.

Liu Jin. 'China: Pushing Ahead of the Cyberwarfare Pack.' *Stratfor*, 2 March 2009. Accessed 28 November 2012. http://www.stratfor.com/sample/analysis/china-pushing-ahead-cyberwarfare-pack.

Maloof, Michael. 'China Tech Company Brags: We Hacked U.S. Telecoms.' *WND*, 14 June 2012. Accessed 30 November 2012. http://www.wnd.com/2012/06/china-tech-company-admits-hacking-u-s-telecoms/.

Medeiros, Evan S., Roger Cliff, Keith Crane and James C. Mulvenon. *A New Direction for China's Defense Industry*. The RAND: Santa Monica, Pittsburgh, 2005. Downloaded 30 November 2012. http://www.rand.org/pubs/monographs/2005/RAND_MG334.pdf.

Menn, Joseph. 'White House-ordered Review Found No Evidence of Huawei Spying.' *Reuters*, 18 October 2012. Accessed 30 November 2012. http://www.reuters.com/article/2012/10/18/us-huawei-spying-idUSBRE89G1Q920121018.

Paganini, Pierluigi. 'Huawei – Symantec, Broken Join Venture and the Fear on Chinese Firms.' *Security Affairs*, 27 March 2012. Accessed 27 November 2012. http://securityaffairs.co/wordpress/3666/intelligence/huawei-symantec-broken-join-venture-and-the-fear-on-chinese-firms.html.

Paganini, Pierluigi. 'The Nightmare Backdoor, Reflections on the Case Huawei.' *Security Affairs*, 6 January 2012. Accessed 27 November 2012. http://securityaffairs.co/wordpress/1377/cyber-crime/the-nightmare-backdoor-reflections-on-the-case-huawei.html.

Roberts, Paul. 'U.S. Investigators Will Call for Ban on Huawei, ZTE over Spying Concerns.' *Naked Security*, 8 October 2012. Accessed 26 November 2012. http://nakedsecurity.sophos.com/2012/10/08/ban-huawei-zte-spying/.

Rogers, Mike, and Ruppersberger, Dutch. *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*. U.S. House of Representatives, 8 October 2012. Downloaded 26 November 2012. http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf.

Saarinen, Juha. 'Analysis: Who Really Owns Huawei?.' *IT news*, 28 May 2010. Accessed 27 November 2012. http://www.itnews.com.au/News/175946,analysis-who-really-owns-huawei.aspx.

Vaas, Lisa. 'National Security Threat or not? Huawei Offers Australia Unrestricted Access to Code.' *Naked Security*, 25 October 2012. Accessed 26 November 2012. http://nakedsecurity.sophos.com/2012/10/25/huawei-australia/.

'China's Huawei Barred from Australia Broadband Deal.' *BBC*, 26 March 2012. Accessed 27 November 2012. http://www.bbc.co.uk/news/business-17509201.

'China's Huawei Feels U.S. Pressure on Iran Business Ties.' *BBC*, 5 January 2012. Accessed 26 November 2012. http://www.bbc.co.uk/news/business-16420380.

'China: Huawei Partner Tried to Sell Embargoed U.S. Technology to Iranian Company.' *Stratfor*, 25 October 2012. Accessed 28 November 2012. http://www.stratfor.com/sample/situation-report/china-huawei-partner-tried-sell-embargoed-us-technology-iranian-company.

'Huawei and ZTE Pose Security Threat Warns U.S. Panel.' *BBC*, 8 October 2012. Accessed 26 November 2012. http://www.bbc.co.uk/news/business-19867399.

'Huawei and ZTE Deny U.S. Spying Charges at Hearing.' *BBC*, 14 September 2012. Accessed 26 November 2012. http://www.bbc.co.uk/news/business-19595778.

'Huawei to Invest £1.3bn in Growing Its UK Business.' *BBC*, 11 September 2012. Accessed 26 November 2012. http://www.bbc.co.uk/news/business-19556817.

'The Company that Spooked the World.' *The Economist*, 4 August 2012. Accessed 26 November 2012. http://www.economist.com/node/21559929.

'The Long March of the Invisible Mr Ren.' *The Economist*, 2 June 2012. Accessed 26 November 2012. http://www.economist.com/node/18771640.

'Who's Afraid of Huawei?.' *The Economist*, 4 August 2012. Accessed 26 November 2012. http://www.economist.com/node/21559922.

2011 Report to Congress of the U.S.-China Economic and Security Review Commission. U.S. Government: Washington, November 2011. Downloaded 30 November 2012.

http://www.uscc.gov/annual_report/2011/annual_report_full_11.pdf.

[1] 'The Company that Spooked the World', *The Economist*, http://www.economist.com/node/21559929, accessed 26 November 2012. [2] ZTE is the second-largest Chinese telecommunications company after Huawei. [3] Ken Hu, *Huawei Open Letter*, The Wall Street Journal, http://online.wsj.com/public/resources/documents/Huawei20110205.pdf, downloaded 27 November 2012. [4] Rogers and Ruppersberger, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, U.S. House of Representatives, p. vi, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf, downloaded 27 November 2012. [5] Ibid., p. 45. [6] 'Huawei and ZTE Pose Security Threat Warns U.S. Panel', *BBC*, http://www.bbc.co.uk/news/business-19867399, accessed 26 November 2012. [7] Gorman and Mozur, 'China Warns Huawei Report Could Harm U.S.-China Relations', *The WSJ*, http://online.wsj.com/article/SB10000872396390443982904578046530208663580.html, accessed 1 December 2012. [8] Kang, 'Huawei's U.S. Competitors among Those Pushing for Scrutiny of Chinese Tech Firm',*Washington Post*, http://www.washingtonpost.com/business/technology/huaweis-us-competitors-among-those-pushing-for-scrutiny-of-chinese-tech-firm/2012/10/10/b84d8d16-1256-11e2-a16b-2c110031514a_story.html, accessed 30 November 2012. [9] Ken Hu, *Huawei Open Letter*, The Wall Street Journal, http://online.wsj.com/public/resources/documents/Huawei20110205.pdf, downloaded 27 November 2012. [10] Anderson, 'Huawei Technologies: Controversial Success Story', *BBC*, http://www.bbc.co.uk/news/business-19568465, accessed 26 November 2012. [11] 'Who's Afraid of Huawei?', *The Economist*, http://www.economist.com/node/21559922, accessed 26 November 2012. [12] 'The Company that Spooked the World', *The Economist*, http://www.economist.com/node/21559929, accessed 26 November 2012. [13] Anderson, 'Huawei Technologies: Controversial Success Story', *BBC*, http://www.bbc.co.uk/news/business-19568465, accessed 26 November 2012. [14] 'The Company that Spooked the World', *The Economist*, http://www.economist.com/node/21559929, accessed 26 November 2012. [15] 'Huawei to Invest £1,3bn in Growing Its UK Business', *BBC*, http://www.bbc.co.uk/news/business-19556817, accessed 26 November 2012. [16] Vaas, 'National Security Threat or not? Huawei Offers Australia Unrestricted Access to Code', *Naked Security*, http://nakedsecurity.sophos.com/2012/10/25/huawei-australia/, accessed 26 November 2012. [17] 'China's Huawei Barred from Australia Broadband Deal', *BBC*, http://www.bbc.co.uk/news/business-17509201, accessed 27 November 2012. [18] Vaas, 'National Security Threat or not? Huawei Offers Australia Unrestricted Access to Code', *Naked Security*, http://nakedsecurity.sophos.com/2012/10/25/huawei-australia/, accessed 26 November 2012. [19] Rogers and Ruppersberger, 'Investigative Report …', pp. 2–4, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf, downloaded 27 November 2012. [20] Ibid., 2–3. [21] Kroft and Messick, 'Huawei Probed for Security, Espionage Risk', *CBS News*, http://www.cbsnews.com/8301-18560_162-57527441/huawei-probed-for-security-espionage-risk/?tag=currentVideoInfo;videoMetaInfo, accessed 30 November 2012. [22] Rogers and Ruppersberger, 'Investigative Report …', pp. 2–3, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf, downloaded 27 November 2012. [23] Ibid., p. 13. [24] 'The Company that Spooked the World', *The Economist*, http://www.economist.com/node/21559929, accessed 26 November 2012. [25] Ken Hu, *Huawei Open Letter*, The Wall Street Journal, http://online.wsj.com/public/resources/documents/Huawei20110205.pdf, downloaded 27 November 2012. [26] *2011 Report to Congress of the U.S.-China Economic and Security Review Commission* , U.S. Government, p. 47, http://www.uscc.gov/annual_report/2011/annual_report_full_11.pdf, downloaded 30 November 2012. [27] Lee, 'The Other Side of Huawei', *Business Spectator*, http://www.businessspectator.com.au/bs.nsf/Article/Huawei-CCP-China-NBN-broadband-pd20120330-SV8JB?OpenDocument&emcontent_spectators, accessed 27 November 2012. [28] Ken Hu, *Huawei Open Letter*, The Wall Street Journal, p. 4, http://online.wsj.com/public/resources/documents/Huawei20110205.pdf, downloaded 27 November 2012. [29] Rogers and Ruppersberger, 'Investigative Report …', pp. 22–23, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf, downloaded 27 November 2012. [30] Ibid, p. 23. [31] Saarinen, 'Analysis: Who Really Owns Huawei?', *IT news*, http://www.itnews.com.au/News/175946,analysis-who-really-owns-huawei.aspx, accessed 27 November 2012. [32] Rogers and Ruppersberger, 'Investigative Report …', pp. 14–15, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf, downloaded 27

November 2012. [33] 'The Long March of the Invisible Mr Ren', *The Economist*, http://www.economist.com/node/18771640, accessed 26 November 2012. [34] Ibid. And 'The Company that Spooked the World', *The Economist*, http://www.economist.com/node/21559929, accessed 26 November 2012. [35] Menn, 'White House-ordered Review Found No Evidence of Huawei Spying', *Reuters*, http://www.reuters.com/article/2012/10/18/us-huawei-spying-idUSBRE89G1Q920121018, accessed 30 November 2012. [36] Ibid. [37] Maloof, 'China Tech Company Brags: We Hacked U.S. Telecoms', *WND*, http://www.wnd.com/2012/06/china-tech-company-admits-hacking-u-s-telecoms/, accessed 30 November 2012. [38] Paganini, 'The Nightmare Backdoor, Reflections on the Case Huawei', *Security Affairs*, http://securityaffairs.co/wordpress/1377/cyber-crime/the-nightmare-backdoor-reflections-on-the-case-huawei.html, accessed 27 November 2012. [39] Constantin, 'Hackers Reveal Critical Vulnerabilities in Huawei Routers at Defcon', *Computer World*, http://www.computerworld.com/s/article/9229785/Hackers_reveal_critical_vulnerabilities_in_Huawei_routers_at_Defcon, accessed 30 November 2012. [40] 'China's Huawei Feels U.S. Pressure on Iran Business Ties', *BBC*, http://www.bbc.co.uk/news/business-16420380, accessed 26 November 2012. And Rogers and Ruppersberger, 'Investigative Report …', pp. 32–33, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf, downloaded 27 November 2012. [41] Ken Hu, *Huawei Open Letter*, The Wall Street Journal, http://online.wsj.com/public/resources/documents/Huawei20110205.pdf, downloaded 27 November 2012. [42] Anderson, 'Huawei Technologies: Controversial Success Story', http://www.bbc.co.uk/news/business-19568465, accessed 26 November 2012. And Rogers and Ruppersberger, 'Investigative Report …', pp. 31, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf, downloaded 27 November 2012. —

Written by: Lucie Kadlecova
Written at: King's College London
Written for: Dr Thomas Rid
Date written: 12/2012