‘Framing’ Chinese hi-tech firms: A political and legal critique

Colin Hawes[*]

Governments in many countries, including the United States, Australia and Canada, have been highly suspicious of the political motives of Chinese business firms seeking to invest in resource industries and infrastructure development overseas. This article uses the case of the Chinese hi-tech firm, Huawei Technologies, to demonstrate the tendency of the United States and other governments to frame their analysis based on unreliable or biased sources and outdated understanding of the Chinese legal and corporate environment. The inevitable results of such misguided framing will be schizophrenic foreign policy decisions, increased international tensions, higher costs for consumers, and retaliation by the Chinese government against international firms doing business in China.

In October 2012, the Permanent Select Committee on Intelligence of the US Congress (the committee) held hearings about two Chinese hi-tech companies, Huawei Technologies and ZTE, and produced a scathing report (the PSC Report), which concluded: ‘Based on available classified and unclassified information, Huawei and ZTE cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States and to our systems.’[1] The report recommended that the US government should block acquisitions, takeovers, or mergers involving Huawei and ZTE, that US government contractors should not use Huawei’s or ZTE’s equipment, including in component parts, and private-sector US telecom firms should be strongly discouraged from buying products from these two companies.[2]

The problem is, virtually all the evidence that the committee relied on to come to this conclusion is either incorrect, misleading, or exaggerated. This article gives just a few examples of these errors: more detailed accounts can be found elsewhere.[3] Our main focus is on Huawei Technologies because it is

* Senior lecturer, Faculty of Law, University of Technology, Sydney. His research focuses on Chinese corporate law and its relationship to culture and politics. He recently published a book titled *The Chinese Transformation of Corporate Culture*, Routledge Press, 2012.

1 M Rogers and D Ruppersberger, ‘Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE’, 8 October 2012, pp vi–vii, at <http://intelligence.house.gov/legislation/committee-reports> (accessed 31 March 2015) (PSC Report). See also videos and transcripts of testimony given at the hearings into this matter at <http://intelligence.house.gov/hearing/investigation-security-threat-posed-chinese-telecommunications-companies-huawei-and-zte-0> (accessed 31 March 2015)..

2 PSC Report, ibid, p vi.

3 The most detailed critical analysis of the PSC Report can be found in E Anderson, *Sinophobia: The Huawei Story*, Kindle Books, 2013, Ch 4. Anderson also collects many of the relevant English-language sources on Huawei’s political challenges, and concludes that there is no convincing evidence of Huawei’s connections with the Chinese military or involvement in any kind of activities that would threaten US national security. For a detailed account of Huawei’s corporate culture, see C Hawes, *The Chinese Transformation of Corporate Culture*, Routledge, Abingdon, UK, 2012, pp 37–43, 117–28. And for balanced

the most successful Chinese hi-tech firm to develop an international market, and it has faced the most serious political and media criticism. But the problems faced by Huawei are shared by its Chinese competitor ZTE, and will stymie any Chinese firm if its business directly or indirectly touches on national security issues.

To point out the inaccuracies in the PSC Report is not to downplay the harmful impacts of cyber-spying or the emerging risks of cyber-warfare. Rather, it is to question the tendency of the United States and other governments to 'frame' their analysis based on unreliable or biased sources and outdated understanding of the Chinese legal and corporate environment, thereby drawing simplistic and erroneous conclusions about Chinese business enterprises. The inevitable result of such framing will be increased international tensions, higher costs for consumers, and retaliation by the Chinese government against American and other international firms doing business in China.

Before offering a critique of the PSC Report's findings about Huawei, the article will first define the concept of framing and briefly introduce some of the typical frames of reference that have been constructed by Chinese commentators, opinion leaders and academics to interpret Chinese government and corporate behaviour, exerting a strong influence on US and other Western government policymakers. We will also note some actions of the Chinese government and military that may have reinforced negative attitudes to Chinese hi-tech firms. In the concluding analysis, the article will argue that negative views of Chinese hi-tech firms represented by the PSC Report and associated academic and media commentary are the inevitable result of a vicious cycle of counter-responses rooted in the very human tendency to frame the 'other' as an actual or potential enemy.

Frames for interpreting China to the West

The concept of framing is a well-known one in the field of communication and media studies. Jim A Kuypers provides a clear definition:

> Framing . . . is the process whereby communicators act — consciously or not — to construct a particular point of view that encourages the facts of a given situation to be viewed in a particular manner, with some facts made more or less noticeable (even ignored) than others . . . [Frames] induce us to filter our perceptions of the world in particular ways.[4]

In their public announcements, politicians frequently seek to 'frame' statements to focus on positive results, whereas their opponents and hostile media commentators will find ways to 'reframe' the analysis to point out the negative impacts of government policies and decisions. Sometimes framing is more sinister, an attempt by law enforcement officials or unprincipled

---

accounts in Chinese about the company, see D Cheng and L Liu, *Huawei zhenxiang* [The Truth about Huawei], Dangdai zhongguo chubanshe, Beijing, 2004; and G Zhang, *Huawei si zhang lian* [The four faces of Huawei], Jingji chubanshe, Guangdong, 2007.

4 See 'Framing Analysis' in *The Art of Rhetorical Criticism*, J A Kuypers (Ed), Pearson, Boston, 2005, p 187.

competitors to cook up false evidence that ensures their opponents will face a guilty verdict or at least be put on the defensive.[5]

But the frames through which people view the world may be adopted unconsciously, resulting from years of acculturation in a specific environment rather than from intentional rhetorical strategies or corrupt practices. As the cultural anthropologist Gregory Bateson put it: 'There may be no explicit verbal reference to the frame, and the subject may have no consciousness of it.'[6] And sociologist Erving Goffman noted the impossibility of doing away with frames altogether: 'It seems we can hardly glance at anything without applying a primary framework, thereby forming conjectures as to what occurred before and expectations of what is likely to happen now.'[7]

All these meanings of framing are relevant for explaining US and other Western governments' publicly stated attitudes towards Chinese hi-tech firms, as we will demonstrate in detail below. Indeed, one of the most influential frames of reference through which foreign governments tend to view China is as a military, economic or sociocultural 'threat'. A brief introduction to the diverse sources of this 'China threat' frame will help to contextualise the case of Huawei Technologies within the broader political discourse.

(1) The 'China threat' frame

Chengxin Pan has provided a detailed analysis of recent representations of the 'China threat', demonstrating the broad range of sources — from scholarly works and government documents to popular culture and mass media — that have viewed China's 'rise' over the past three decades as a precursor to conflict with Western powers, especially with the United States.[8] Pan cites typical headline-grabbing book titles, including Bernstein and Munro's *The Coming Conflict with China* and Peter Navarro's *The Coming China Wars*; and numerous media headlines painting an overwhelmingly negative picture of China. 'Job Losses: Made in China', and 'Tracing a Poison's Global Path Back to China' are standard examples.[9] Even academics with less inflammatory views often make statements such as: 'China would almost certainly use its wealth to build a mighty military machine',[10] and 'China [is] a gathering multi-dimensional threat'.[11]

Pan notes that there are often links between the more hawkish 'China threat' advocates and the American 'military industrial complex', with some key US foreign policy think tanks either funded by the military or headed by former military personnel.[12] Pan and others have argued that the US military has a vested interest in talking up the potential military challenge from China

5 See *Merriam-Webster Dictionary*, 'frame', at <http://www.merriam-webster.com/dictionary/frame> (accessed 31 March 2015) .

6 G Bateson, *Steps to an Ecology of Mind*, Intertext Books, London, 1972, p 187.

7 E Goffman, *Frame Analysis: An Essay on the Organization of Experience*, Harvard University Press, Cambridge, 1974, p 38.

8 C Pan, *Knowledge, Desire and Power in Global Politics: Western Representations of China's Rise*, Edward Elgar, Cheltenham, UK, 2012.

9 Ibid, p 24.

10 J J Mearsheimer, *The Tragedy of Great Power Politics*, WW Norton, New York, 2001, cited in Pan, ibid, p 28.

11 S Halper, 'Wrongly Mistaking China' (2007) 40(1) *The American Spectator* 20, cited in ibid.

12 Pan, above n 8, pp 72–6.

in order to justify increased investment in major weapons systems and defence contracts, especially since the previous threat from the Soviet Union has diminished.[13] Likewise, many US congressmen and senators represent districts where defence industry contracts are vital to the local economy (and to political candidates' re-election efforts). They will have an in-built tendency to support any perspective on China that sees increased defence spending as vital to the US national interest.[14]

Added to the potential military 'threat' are equally powerful fears about China's growing economic might, and resentment about the perceived loss of jobs to 'China' due to unfair competition and alleged currency manipulation. One estimate by a group of US senators claimed that China's 'undervalued currency' had contributed to the loss of '2.6 million [American] manufacturing jobs'.[15]

Finally, one should not underestimate the longstanding hostility towards Communism and authoritarian governments that drove the United States and its allies into the Cold War and still provokes the ire of many politicians, especially in the United States. Any direct or indirect involvement of the Chinese Communist Party (CCP) in commercial investment overseas would raise 'red flags' with such politicians, who are constantly vigilant about Communist attempts to infiltrate and undermine societies in the 'free world'.[16]

In Australia, similar fears have been expressed about China's rise, especially the risks of Australia being drawn into a regional conflict between China and its Asian neighbours. Influential think tanks like the Australian Strategic Policy Institute have called for greater military spending and closer cooperation with the United States to prepare for this 'threat'.[17] There is also frequent media commentary about Chinese corporations buying up Australian agricultural land, pushing up food prices for consumers and potentially threatening Australia's food security; and claims that Chinese property investors are inflating house prices to unaffordable levels in Sydney and Melbourne.[18]

Part of this discourse may be based on fear of the unknown or anti-Asian bias, as occurred when Japanese investors bought up great swathes of

13 Ibid, pp 74–5; and for a historical analysis of 'invented' justifications for US military spending, cf I Hossein-Zadah, *The Political Economy of US Militarism*, Palgrave Macmillan, New York, 2006.

14 Ibid, pp 71–2.

15 Ibid, p 27.

16 See, eg, comments about Huawei and 'Communist China' by Congressman Thaddeus McCotter, 'Communist China and CFIUS: "Dropping the Shark"', 3 October 2007, at <http://archive.redstate.com/blogs/rep_thaddeus_mccotter/2007/oct/18/communist_china_and_cifus_dropping_the_shark> (accessed 31 March 2015)

17 See C McGrath, 'Australia urged to up defence spending to meet threat from rising power China', *ABC News*, 11 June 2014, at <http://www.abc.net.au/news/2014-05-30/call-for-review-of-australian-defence-spending/5487968>; and M Dal Santo, 'Is a powerful China a threat to Australia?', *The Drum*, 27 May 2014, at <http://www.abc.net.au/news/2014-05-27/dal-santo-us-alliance-could-be-our-china-fail-safe/5477528> (accessed 31 March 2015).

18 See A White, 'China land grab hidden by "corporate veil"', *The Australian*, 29 October 2013; and M Janda, 'Chinese buyers to invest $44b in Australian real estate: analysts', *ABC News*, 5 March 2014, at <http://www.abc.net.au/news/2014-03-05/chinese-buyers-to-invest-44-billion-dollars-in-australian-real-/5300494> (accessed 31 March 2015).

Australian real estate during the 1980s.[19] But it may also result from US pressure. In the telecommunications industry, for example, the Singaporean-controlled company SingTel was temporarily blocked from taking over Optus in 2001, as US regulators were concerned about military technology on satellites owned by Optus getting into foreign (ie, Singaporean) hands. Because the technology was manufactured in the United States, it required approval from the US State Department to 'export' it to another country. Eventually the approval was given after SingTel gave undertakings to safeguard any sensitive military information carried on the Optus satellites.[20]

With this combination of popular fears about China's rise and external pressure not to jeopardise the key US strategic relationship, it is no surprise that the Australian government would prevent Chinese firms like Huawei from bidding to supply the Australian National Broadband Network.[21]

Of course, these fears about the rise of China are not entirely groundless. Double digit annual increases in China's military spending budget have been frequent over the past decade, even if the total amount still falls far short of US military budget levels; and there are plenty of 'hawks' in the Chinese defence establishment who openly declare that the United States and its Asian allies are China's main adversaries.[22] China has territorial disputes with most of those allies, including especially Japan, Taiwan and the Phillipines, and these disputes frequently erupt into political rows and threatening gestures.[23] There is certainly an element of what Pan calls 'mutual responsiveness', with China's military build-up resulting from its fear of US 'containment', and correspondingly inflamed US suspicion of China's motives.[24]

Whatever the fundamental causes of this increased mutual suspicion, it has led to a situation where the US government's own official defence reports have concluded: 'Of the major and emerging powers, China has the greatest potential to compete militarily with the United States.'[25] The congressmen on the Permanent Select Committee on Intelligence would surely have consciously or unconsciously been influenced by these widespread negative

19 See a historical account by A Rix, *The Australia-Japan Political Alignment: 1952 to the Present*, Routledge, London, 1999, p 108. For a critique of the similar US perspective on Japanese investment, see D Boaz, 'Yellow Peril Reinfects America', CATO Institute Commentary, 7 April 1989, at <http://www.cato.org/publications/commentary/yellow-peril-reinfects-america> (accessed 31 March 2015).

20 K Morrison, 'US Spies in the Sky Stall Bid for Optus', *Sydney Morning Herald*, 15 June 2001; and A Hyland, 'Optus Stoush Leaves Singapore Smarting', *Australian Financial Review*, 2 August 2003.

21 See S McDonell, 'China criticises Government's decision to uphold NBN ban on telco Huawei', *ABC Lateline*, 30 October 2013, at <http://www.abc.net.au/news/2013-10-29/china-angered-by-decision-uphold-nbn-ban-on-huawei/5056588> (accessed 31 March 2015). Ironically, one of the main beneficiaries of this decision has been SingTel Optus, which has received the contracts to operate the Network's two satellites: see National Broadband Network Co, *2013–14 Annual Report*, p 38.

22 Dal Santo, above n 17.

23 N Bisley and B Taylor, 'Conflict in the East China Sea: Would ANZUS Apply?', UTS Australia-China Relations Institute Research Paper, November 2014, pp 12–15.

24 Pan, above n 8, pp 17–18.

25 US Department of Defense, *Quadrennial Defense Review Report*, Washington DC, 6 February 2006, p 29; cited in Pan, above n 8, p 26.

perceptions of China when they were asked to investigate the expansion of Chinese hi-tech firms overseas.

(2) Other frames: 'China Opportunity' and ambivalence

Contrasted with the 'China threat' discourse is what Pan calls the 'China opportunity' paradigm. This perspective combines an optimistic expectation that China will open access to its enormous consumer market, with the hope that opening up will lead to closer integration with the international community, and ultimately perhaps democratic political reform.[26] For those who adopt this frame, the accession of China to the WTO in 2001 and its greater involvement in global institutions are important milestones on the way to China becoming a 'responsible stakeholder on the world stage'.[27] Clearly advocates of this perspective would also strongly support free trade and globalisation. Samuel Berger, the national security adviser under Bill Clinton, expressed this point clearly: 'Just as North American Free Trade Agreement membership eroded the economic base of one-party rule in Mexico, WTO membership . . . can help do the same in China.'[28]

Seen from today's perspective, with one-party rule still firmly ensconced in China, such optimism about political reform may appear misguided. But the economic argument for promoting open trade with China is still very influential in government and business circles. The more sophisticated observers of China therefore tend to adopt an ambivalent attitude, or 'bifocal lens', that remains wary of the potential Chinese 'threat' while simultaneously promoting economic engagement and hoping for continuing reform and even 'regime change' in the future.[29] Difficulties emerge, however, when these various frames are brought into conflict with each other, as when a Chinese hi-tech firm seeks to sell its products to US telecom firms or foreign governments, or to acquire technology from overseas.

Deconstructing the PSC Report: The case of Huawei

Huawei is a highly successful communications technology firm, with its core business focused on internet and telephone network hardware. It has business operations or sales in over 170 countries, supplying some of the world's largest telecom and internet service providers, and over half of its revenues come from outside China.[30] The main challenge Huawei faces is that it has effectively been excluded from much of the US telecom market, one of the largest in the world. Other nations like Australia, India and Canada have also prevented Huawei from bidding on major government contracts including the Australian National Broadband Network, or selling equipment to state-controlled telecom firms, citing 'national security' concerns.[31] But are these concerns justified based on the available evidence?

---

26 Pan, above n 8, pp 31–8.
27 Ibid, p 37.
28 Ibid, p 37.
29 Ibid, pp 38–9.
30 See information about the company on Huawei's website at <http://www.huawei.com/en/about-huawei/corporate-info/index.htm> (accessed 31 March 2015).
31 For Australia, see McDonell, above n 21; for India, see M Srivastava and M Lee, 'India Said

Assisting America's enemies? Huawei or Hua-Mei?

The most serious allegation that emerged in the controversy leading up to the PSC Report was that Huawei assisted America's enemies by providing them with sophisticated communications hardware that can be used in defensive weapons systems. Since 2010, US senators have publicly accused Huawei of supplying Saddam Hussein's regime in Iraq in the late 1990s, and the Taliban in Afghanistan.[32] These allegations are untrue.

After the Americans started enforcing a no-fly zone in Iraq in the 1990s, there were several media reports claiming that Huawei's communications equipment had been installed as part of the Iraqi air defence network, thereby threatening American lives.[33] But those reports were incorrect, because the actual name of the company involved was Hua-Mei (which translates as China-America). This was a joint venture between an American firm and a company controlled by Chinese military personnel called Galaxy New Technology.[34] Huawei had nothing to do with this joint venture or its equipment at all: it was just a misreading of the name Hua-Mei by some careless reporters! Unfortunately, the same mistake was still being repeated 10 years later in a letter by US senators to the US Congress, demanding that Huawei be blocked from the US market due to its alleged 'collaboration' with America's enemies.[35] As for Huawei supposedly supplying equipment to the Taliban in Afghanistan, that turned out to be pure speculation as well.[36]

Because the allegations about Huawei in Iraq and Afghanistan were clearly false, the PSC Report itself did not include them, but neither did it correct the errors that had been publicly aired by US Senators. Instead, the PSC Report

---

to Block Orders for ZTE, Huawei Technologies Telecom Equipment', *Bloomberg*, 30 April 2010, at <http://www.bloomberg.com/news/2010-04-30/india-said-to-block-china-s-huawei-zte-from-selling-phone-network-gear.html> (accessed 31 March 2015); and for Canada, see S Chase, 'Ottawa set to ban Chinese firm from telecommunications bid', *The Globe and Mail*, 10 October 2012, at <http://www.theglobe andmail.com/news/politics/ottawa-set-to-ban-chinese-firm-from-telecommunications-bid/article4600199/> (accessed 31 March 2015).

32 Iraq and Afghanistan are not mentioned in the PSC Report, doubtless because the evidence of Huawei's alleged wrongdoing in those countries cannot stand up to scrutiny, but several US government officials have publicly made unsubstantiated allegations, for example, eight Republican Senators sent an open letter to various government departments and media organisations in 2010 claiming that 'Huawei sold communications technology to Saddam Hussein's regime . . . and it also supplied the Taliban before its fall'. See Sen J Kyl et al, 'Letter Requesting Information on Huawei', 18 August 2010, United States Senate, Washington, at <http://www.docstoc.com/docs/51224083/20100818-letter-to-Geithner_-Locke_-Clapper_-and-Johnson> (accessed 31 March 2015).

33 Anderson, above n 3, pp 991–1000. See, eg, K Motz and J Richie, *'Technology Two-Timing', The Asian Wall Street Journal*, 19 March 2001, at <http://www.iraqwatch.org/suppliers/techno-2time.htm> (accessed 31 March 2015)

34 The involvement of HuaMei is described in a report by the US Government Accountability Office, 'Export Controls: Sale of Telecommunications Equipment to China', NSIAD-97-5, 13 November 1996, at <http://www.gao.gov/products/NSIAD-97-5> (accessed 31 March 2015). The American firm claimed it had no idea its Chinese partner was connected to the military, but it should have known because the CEO of the company was an officer in the People's Liberation Army and her husband was a Chinese general! Anderson, above n 3, pp 1184–1230, gives a detailed account of this debacle.

35 Kyl, above n 32.

36 Anderson, above n 3, pp 1232–50.

implies that other abuses may have occurred, concluding that Huawei 'did not provide evidence to support its claims that it complies with all international sanctions regimes'.[37]

The only evidence of Huawei's 'collusion' with America's 'enemies' in the PSC Report related to Iran. The Congressional Committee expressed doubts about Huawei's claim that it had voluntarily suspended signing new contracts in Iran to comply with international sanctions imposed since 2010.[38] Huawei certainly has been a major player in Iran in the past, selling its hardware to upgrade the country's phone and internet networks.[39] But Huawei's competitors like Ericsson and Nokia Siemens Networks have been just as active in Iran, selling similar kinds of equipment. Does that make these European multinationals a threat to US national security too?[40] The PSC Report fails to note that Huawei was only one of several multinational firms helping to upgrade Iran's telephone and internet networks over the past decade.

This kind of 'framing' — attempting to cast Huawei in the most negative light through selective presentation of evidence and failure to correct prior misinformation — is a feature that runs through the entire PSC Report. It is particularly evident in the discussion of Huawei's alleged ties to the Chinese military and government.

Military ties?

The claim that Huawei has close ties to the military, repeated several times in the PSC Report, also turns out to be speculation based on very shaky foundations.[41] It is true that Huawei's CEO Ren Zhengfei was once a relatively low-ranking officer in the Chinese military engineering corps.[42] But he left the army in 1983, and a few years later in 1987 set up a private business selling simple telephone exchange switches imported from Hong Kong, which later grew into Huawei.[43] There is no convincing evidence that Ren Zhengfei maintained any close connections with the Chinese military or that the military has been involved in or exercised any influence over Huawei's business.

The story about Huawei's military ties appears to have been sparked by a

37 PSC Report, above n 1, p 32.

38 For references to Iran, see the PSC Report, ibid, pp 32–3.

39 For contrasting reports on Huawei's operations in Iran, see S Stecklow, F Fassihi and L Chao, 'Chinese Tech Giant Aids Iran', *The Wall Street Journal*, 27 October 2011, at <http://online.wsj.com/news/articles/SB10001424052970204644504576651503577823210> (accessed 31 March 2015); and Huawei Technologies, 'Statement Regarding Inaccurate and Misleading Claims about Huawei's Commercial Operations in Iran', 4 November 2011, at <http://pr.huawei.com/en/news/hw-104191.htm#.U-xfk02KCM8> (accessed 31 March 2015)

40 For Nokia Siemens Networks, see C Rhoads and L Chao, 'Iran's Web Spying Aided By Western Technology', *Wall Street Journal*, 22 June 2009; for Ericsson, see S Stecklow, 'Exclusive: Ericsson helps Iran telecoms, letter reveals long-term deal' *Reuters*, 20 November 2012, at <http://www.reuters.com/article/2012/11/20/us-iran-ericsson-idUSBRE8AJ0IY20121120> (accessed 31 March 2015).

41 PSC Report, above n 1, pp 13–14, 21–2, 24–5.

42 Ibid, p 24.

43 See Zhang, above n 3, pp 23–4, 135, 223–4.

reporter from the news weekly *Far Eastern Economic Review*, who visited Huawei's Shenzhen manufacturing facility back in 2000. He claimed to have come across three large telephone exchange switches in Huawei's shipping warehouse addressed to the telecom bureau of the People's Liberation Army (PLA).[44] Unfortunately the article did not provide any photographic evidence to back up this arresting claim, or any details of the equipment's specifications. The only other hard evidence was a comment by Huawei's Senior Vice President Fei Min that the company did sell some standardised equipment to the Chinese military, but it made up less than 1% of the company's overall sales.[45] From this, the reporter concluded that Huawei was a 'military-backed company'.[46]

Such a speculative news article would normally have disappeared quickly, but it gained a new lease of life in an influential 2005 report by the RAND Corporation with the imposing title 'A New Direction for China's Defense Industry'.[47] The RAND report claimed that Huawei was part of a new 'digital triangle' between the Chinese state, military and commercial IT industry, and that 'Huawei maintains deep ties with the Chinese military, which serves a multi-faceted role as an important customer, as well as Huawei's political patron and research and development partner'.[48] Unfortunately, the only named source cited for these assertions is the same *Far Eastern Economic Review* article from 2000 — which even at face value does not support such wide-ranging conclusions about 'deep ties', military patronage or R&D partnerships.[49]

Many of the media reports and government committees that continue to raise these allegations about Huawei's 'military ties' cite this RAND Report without questioning the paucity of its source material.[50] It is even relied on in the PSC Report as the main 'evidence' by 'many analysts' of Ren Zhengfei's continuing military connections.[51] The case for Huawei's military ties must be

44 B Gilley, 'Huawei's Fixed Line to Beijing', *Far Eastern Economic Review*, 28 December 2000, p 94.

45 Ibid, p 96. The reporter also cited unnamed 'foreign analysts' and a Russian assistant manager at Huawei's Moscow office to back up his claims of Huawei's 'military ties'! Huawei has never denied that one of its customers is the Chinese military, but has consistently maintained that such military sales have never made up more than 1% of its overall sales. With the growth of its overall business, sales to the Chinese military now make up only 0.1% of its overall sales, according to statements provided by Huawei to the PSC: see PSC Report, above n 1, p 34.

46 Ibid, p 94.

47 E S Medeiros, R Cliff, K Crane and J C Mulvenon, 'A New Direction for China's Defense Industry', RAND Corporation, Arlington, VA, 2005 (RAND Report).

48 Ibid, p 218.

49 Ibid, pp 219–21 nn 17–20. The report also refers to some unnamed 'interviewees' in Beijing, which is a long distance from Huawei's headquarters in Shenzhen.

50 For example, J Dean, 'Outside of US, Few Fear Huawei', *Wall Street Journal*, Asian edition, 22 February 2008, at <http://online.wsj.com/news/articles/SB120359554277582713> (accessed 31 March 2015); and Tech Law Journal, '3Com Huawei transaction to be reviewed by CFIUS', *Tech Law Journal*, 9 October 2007, at <http://www.techlawjournal.com/topstories/2007/20071009b.asp> (accessed 31 March 2015).

51 PSC Report, above n 1, pp 13, 48 nn 40–41.

extremely weak if this is the best evidence that a well-funded US government committee can dig out.[52]

Government ties?

What about ties to the Chinese government? The PSC Report expressed grave concern about the fact that Huawei has a Chinese Communist Party (CCP) Branch within the firm, and that Huawei's ownership is not clear. They also pointed out that Ren Zhengfei has been a CCP member since the early 1980s and once attended a meeting of the CCP's National Party Congress in 1982, when he was still in the PLA.[53] They treated this as evidence that Huawei is being controlled and influenced by the Chinese government behind the scenes.[54]

One major problem with this argument is that there are over 80 million CCP members in China, and every large business firm registered in China must set up a CCP Branch if requested by employees, as stated in the PRC Company Law.[55] Even American corporations like Walmart and Motorola have set up CCP Branches in their Chinese subsidiaries. Does this mean that Walmart and Motorola are being controlled by the Chinese government?[56]

Moreover, the CCP's Charter makes it clear that the main role of the CCP within non-state controlled business firms is to:

> provide guidance to the enterprise in observing the laws and regulations of the state, exercise leadership over the trade union, . . . rally the workers and office staff, safeguard the legitimate rights and interests of all stakeholders and stimulate the healthy development of the enterprise.[57]

The CCP Charter also specifically distinguishes between the role of the Party in state-controlled enterprises and 'non-public' (ie, private) enterprises. In state-controlled enterprises, the CCP Committees should 'participate in making final decisions on major questions in the enterprise', but that is not part of their function in non-public enterprises.[58]

One Walmart employee and CCP branch member explained: 'Our Branch Party Secretary told me that a major criterion for evaluating Party members' progress is whether we have helped to increase sales at the Walmart stores where we work.'[59] Ren Zhengfei made a similar remark in a 2008 speech to Huawei's CCP branch members: 'You are extremely important mentors within

52 Ibid, p 10, also refers to a 'classified annex' that the writers claim contains much more evidence against Huawei, but this (conveniently?) cannot be published due to 'national security concerns'.

53 Ibid, p 23.

54 Ibid, pp 13, 22–4.

55 See PRC Company Law Art 19.

56 For more details on the role of the Communist Party Committees in corporations in China, including foreign corporations like Walmart, see C Hawes, 'Interpreting the PRC Company Law through the Lens of Chinese Political and Corporate Culture' (2007) 30(3) *UNSWLJ* 813 at 816–19.

57 CCP Charter Art 32, at <http://www.idcpc.org.cn/english/cpcbrief/constitution.htm> (accessed 31 March 2015).

58 CCP Charter Art. 32.

59 J Min, W Zheng and Z Jianhua, 'Zhonggong shouci zai woermafendianjianli dang zuzhi' [CCP sets up Party organisations within Walmart for the first time], *Xinhua News Agency*,

our company . . . and your role is to help your colleagues to realize that . . . they chose a life of hard work and struggle, because firms like ours without any established history can only survive if we work a bit harder than everyone else'.[60] While Huawei does not spell out the role of its CCP Committee in detail, published statements by other privately controlled firms have made it clear that the CCP supports rather than controls the management. For example, Mme Lu Jun, the first Party Secretary of the privately controlled Mengniu Dairy Group, stated that the Party organisation within Mengniu has three main tasks: (1) to motivate the employees so that they become more productive; (2) to regularly survey employees to find out what issues they are concerned with and to seek their rational suggestions for improvements to the firm's processes; and (3) to investigate and root out corruption among the firm's employees.[61] Clearly the CCP branches within privately controlled Chinese firms today are more like employee motivation associations assisting the management to improve firm performance rather than the overtly political organisations of the past.[62]

Setting aside Huawei's Communist Party Committee for the moment, does the firm's ownership structure itself conceal Chinese government control? It's true that Huawei's structure is somewhat complicated, but a careful examination shows that the firm is owned by its employees and controlled by its management.

Ownership questions

Part of the complexity stems from Huawei's history as a private business in China, where private enterprises faced discrimination until very recently.[63] Back in the 1980s and early-1990s, Huawei's only customers were the big Chinese state-owned telecom firms (in fact there was only one firm, China Telecom, until the industry was partly deregulated in the late-1990s).[64] Huawei had to do business with the local branches of China Telecom all over China, and the only way to compete with state-owned equipment manufacturers was by giving long-term incentives to China Telecom officials and employees. Huawei set up a whole series of joint venture subsidiaries with local telecom branches where the China Telecom branch would agree to buy Huawei's equipment, but it would be sold through the joint ventures, and the

---

26 August 2006, at <http://www.ln.xinhuanet.com/ztjnl2007-08/26/content_11295101.htm> (accessed 31 March 2015). Hawes, above n 56, at 818–19.

60 Z Ren, 'Jinqi zai canjia gongsi youxiu dangyuan zuotanhui shi fayan' [Speech given while participating in a recent symposium for Huawei's outstanding Party members], 2008, copy on file with author.

61 X Sun and Z Zhang, *Mengniu neimu* (Mengniu: the inside story), 3rd ed, Peking University Press, Beijing, 2008, pp 263–4.

62 Hawes, above n 56, at 816–19.

63 For discrimination against private enterprises in China, see S Lin and S Song (Eds), *The Revival of Private Enterprise in China*, Ashgate, Aldershot, UK, 2007, p 36; and J Zeng, *State-Led Privatization in China*, Routledge, Abingdon, UK, 2013, pp 133–4. A more nuanced account is provided in Y Xu, 'Financing of Private Enterprises and Deepening Financial Reform' in *Private Enterprises and China's Economic Development*, S Lin and X Zhu (Eds), Routledge, Abingdon, UK, 2007, pp 51–73.

64 S Y Guan, *China's Telecommunications Reforms: From Monopoly towards Competition*, Nova Science Publishers, New York, 2003, pp 18–39.

profits would be shared with China Telecom officials and employees.[65] This was not illegal at the time, though certainly a legal grey area.[66] But in the late 1990s, the government restructured the telecom service providers to remove China Telecom's monopoly and create a market-oriented system, so Huawei bought out all the joint ventures and adopted more orthodox marketing and sales methods instead.[67]

China Telecom staff and officials never owned shares in Huawei Technologies itself; they only had ownership interests in Huawei's joint venture subsidiaries. Instead, Huawei's shares were initially owned directly by its employees, with the company's senior managers holding the majority of shares.[68] This was a clever way of retaining employees, because most of their salary came from the profits on their shares, and if they left the firm, they would forfeit their shares. Many employees called these shares 'golden handcuffs', as they were worth a lot, but they tied people to the firm.[69] The problem was, once Huawei expanded very quickly and hired thousands more employees, it became impossible for senior management to retain control with their regular shares. This is because the PRC Company Law requires a company with more than 50 shareholders to give each shareholder one vote per share.[70]

So as part of Huawei's restructuring in the late 1990s, the firm set up an employee investment fund to acquire Huawei's shares from its employees. In return, the employees were allotted units in the fund instead of shares, which did not give them direct voting power but allowed them to share in the company's profits.[71] The investment fund was controlled by an employees' representative commission, which cast votes in shareholder meetings on behalf of the employees, but the CEO Ren Zhengfei had a veto over any decisions made by the fund, including who would be appointed to Huawei's board.[72] The employees' representative commission currently consists of 51 members, the majority of whom are senior managers of the firm. This means that even though there are currently about 84,000 Huawei employees who hold units in the investment fund that owns Huawei's shares, the firm is still

65 Cheng and Liu, above n 3, pp 76–8, 104–9; and for further details, see Y Wang, *Langxing guanli zai Huawei* [Wolf-style management at Huawei], Wuhan University Press, Hubei, 2007, pp 283–6.

66 Zeng, above n 63, p 27.

67 G Li, 'Can the PRC's New Anti-Monopoly Law Stop Monopolistic Activities? Let the PRC's Telecommunications Industry Tell You the Answer' (2009) 33(7) *Telecommunications Policy* 361; Zhang, above n 3, pp 8, 38, 55.

68 Wang, above n 65, pp 101–2; Cheng and Liu, above n 3, p 110.

69 Cheng and Liu, above n 3, p 116.

70 With more than 50 shareholders, a company must normally be formed into a joint stock company, which stipulates one vote per share: see PRC Company Law Arts 79, 104. With less than 50 shareholders, a company can be formed as a limited liability company (LLC), which allows flexibility in the way voting rights are divided up among shareholders: PRC Company Law Arts 24, 43. The PRC Company Law was first introduced in 1994, and Huawei was restructured from an employee-owned collective to a registered limited liability company in 1997: see PSC Report, above n 1, pp 15–16.

71 The PSC Report gives a very useful detailed summary of Huawei's employee share ownership program based on information provided by the firm: PSC Report, above n 1, pp 15–20.

72 Ren's veto will last until 31 December 2018: PSC Report, above n 1, p 20.

effectively controlled by its senior management.[73]

This ownership structure is certainly unorthodox, but was designed to get around the inflexible rules on share voting in the Company Law.[74] It wasn't done to hide the 'true' owners of Huawei. But the PSC Report seems to think that somewhere in this structure government control is lurking.[75] In the end, however, the PSC Report was only able to make a weak finding that Huawei was not completely forthcoming about its relationship networks with Chinese government ministries, which is a long way from establishing Chinese government influence over the firm.[76]

Intellectual property infringements?

Finally, the PSC Committee was clearly seeking to frame Huawei in the worst possible light when they alleged that the firm was a serial IP infringer, stealing ideas from its US competitors.[77] Why was this relevant to US national security? Because, they said, it tested whether Huawei was a 'good corporate actor' and could be trusted with sensitive US communications infrastructure contracts.[78] This is another problematic argument, as it ignores the fact that the two main IP lawsuits brought against Huawei by Cisco and Motorola were both settled out of court.[79] While the Cisco suit appears to have had merit, the Motorola suit was much less clear-cut, and a single example of infringement dating from 2003 is hardly evidence of 'serial' infringement.

Moreover, virtually all multinational hi-tech firms have been sued for IP infringement or unfair competition by their competitors or by governments, including Apple, Samsung, Microsoft, Intel and others. Some have even been found liable in IP or anti-trust lawsuits in international and US courts.[80] Does that mean these firms are also too dishonest to be permitted to bid on US government contracts?[81]

Fear of technological 'back doors'

Despite the lack of hard evidence against Huawei and ZTE, the PSC Report's main concern is that somehow the Chinese government or military will

73 Information about the employees' representative commission and the number of employee unit holders is taken from Huawei's *2013 Annual Report*, pp 108–9.

74 Huawei gave this explanation in materials cited in the PSC Report, above n 1, pp15–16.

75 PSC Report, above n 1, pp 14, 21–2. The only solid criticism that the PSC Report could make was that Huawei is not controlled by its shareholders but by its senior executives, but this is no secret and does not prove any government control over the firm.

76 PSC Report, above n 1, p 22.

77 Ibid, pp 31–2.

78 Ibid, p 11.

79 See the detailed analysis of these disputes in Anderson, above n 3, at 1320–1585.

80 See, eg, Anon, 'Samsung ordered to pay Apple $120m for patent violation', *The Guardian*, 3 May 2014; C Arthur, 'Microsoft loses EU anti-trust fine appeal', *The Guardian*, 28 June 2012.

81 Some scholars have also noted that most countries go through a period of development when they feel the need to breach intellectual property rights in order to catch up with more developed nations. Only after reaching a certain stage of prosperity and technological advancement do they then seek to enforce intellectual property laws vigorously. This occurred in both the United States and Japan, for example. See D S Ben-Atar, *Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power*, Yale University Press, 2004.

persuade or force these two companies to insert 'malicious hardware or software implants' into telecom components or systems sold in the United States, resulting in potential disruption of critical communications systems, loss or theft of confidential data, and foreign government control over US critical infrastructure.[82] But this fear ignores the complexity of the supply chain for these multinational hi-tech firms, whose products typically contain advanced technological components assembled in over 20 different countries, all of which would require adjusting to be compatible with any 'malicious' implants.[83] Due to these insurmountable technical challenges, Chinese and other foreign cyber-hackers have found it easier to infiltrate foreign government and corporate networks at the user end rather than the manufacturing end, and this has occurred despite the fact that most of the victims were not using Huawei's or ZTE's equipment.[84] There is no evidence that excluding these two Chinese firms from the US and other markets will help to prevent such cyber attacks from occurring in the future. Doing so will only give a false sense of security to American and international consumers.

Reasons for suspicion? Locating the Huawei investigation within the broader geopolitical and theoretical framework

If the evidence against Huawei is so thin, why are the US government and some of its allies so suspicious of this company? Why are they not celebrating the great success of this Chinese private enterprise that has proved it can compete with the best in the world? There are several factors, which we can divide into two main categories: (1) the impact of Huawei's own behaviour and that of the Chinese military and government; (2) distorted frames adopted by the US government and the international media when viewing Huawei's behaviour.

(1) Contextualising Chinese private hi-tech firm behaviour

Looking at Huawei's actions first, the only way to succeed as a private telecom equipment firm in China during the 1980s and '90s was to build business alliances with local state-owned telecom officials, and even though these joint ventures were sold off in the late 1990s, Huawei's restructuring into an employee investment fund ownership system then created a kind of black box, allowing outsiders to speculate that it was hiding something about its ownership. While the structure was adopted to allow Huawei's senior management to maintain control while complying with the PRC Company

82 PSC Report, above n 1, pp 2–3.

83 P Rossi, 'Huawei's End-to-end Assurance System', talk given at a University of Technology Sydney workshop on 'Cloud Computing, Cyber Security and Privacy Protection in China: Legal and Political Issues', 12 June 2014. Note also that US firms producing internet equipment for the US market, such as Cisco Systems, also manufacture some of their products and components in China: see Cisco Systems, '*Gongsi jieshao*' (Introducing the Company), at <http://www.cisco.com/web/CN/aboutcisco/company_overview/about_company_overview_overview.html> (accessed 31 March 2015).

84 For details of some of these cyber attacks, see n 94 below.

Law, it has created the perception that Huawei is not transparent, which plays into fears that the firm may be engaged in covert activities.

Huawei also downplayed the fact that the firm has a Communist Party branch, saying that the Party has no influence over management decisions.[85] Depending how 'management' is defined, this may be true, but Huawei should explain more clearly what the CCP does in the firm, who Huawei's leading CCP representatives are, and how they interact with the firm's senior management. It is not difficult to find out from a brief web search that Huawei's CCP Branch Secretary is Zhou Daiqi, who is listed in the firm's *2013 Annual Report* as Chief Ethics and Compliance Officer and a member of the Audit Committee.[86] Neither his CCP role nor that of Huawei's CCP Committee are mentioned in the firm's *Annual Reports* and it is not clear how Zhou's role as CCP Secretary interacts with his other executive responsibilities. Other large private Chinese business firms include information about their CCP branches on their Chinese-language websites or in published profiles, including detailed descriptions of the CCP Committee's activities within the firm, and there is no reason why Huawei should not do likewise.[87] Having said this, the PRC Company Law and associated corporate governance principles do not provide any rules about how to disclose the CCP's presence within Chinese-registered corporations, and firms are essentially left to judge for themselves whether or not they should publicise the work of their CCP Committees. Not surprisingly, most choose to say very little, in case they unwittingly breach laws about revealing 'state secrets'.[88] The Chinese government needs to provide more guidance to privately controlled business firms on what they can disclose about their CCP Committees so that their opaqueness is not seen as suspicious evasiveness.

Huawei has also been so desperate to expand internationally that it has sold its equipment in several countries that may not be enemies of the United States but are certainly not allies, such as Sudan and Yemen.[89] Though Huawei's interests are purely commercial, they should have realised the US government

85 PSC Report, above n 1, p 14.

86 See 'Huawei dangwei shuji Zhou Daiqi: guojihua tui Shenqi tisheng jingzhengli' (Huawei's Party Secretary Zhou Daiqi declares: Internationalization has pushed Shenzhen's business firms to increase their competitiveness), *Shenzhen tequ bao*, 23 November 2011, at <http://tech.southcn.com/t/2011-11/23/content_33696313.htm> (accessed 16 January 2015). Zhou's role as Communist Branch Secretary is not mentioned in Huawei's Annual Reports or on its Chinese or English-language websites.

87 See, eg, the website of the electrical instrument manufacturer Zhengtai Group (CHINT), '*Dangjian gongzuo*' (Party Building Work), at <http://www.chint.com/partybuilding?sitePageId=49> (accessed 31 March 2015); and the Tengen (Tianzheng) Group, '*Wenming chuangjian*' (Building a Civilized Firm), at <http://www.tengen.com.cn/sm2111111250.asp> (accessed 31 March 2015). Cf, the description of Mengniu Dairy Group's Party Committee in Sun and Zhang, above n 61, pp 263–4.

88 This was the reason given by ZTE to the Permanent Select Committee on Intelligence for requesting that the list of ZTE's CCP Committee members be kept classified: see PSC Report, above n 1, p 40.

89 See Huawei's website at <http://www.huawei.com/worldwide/index.htm> and <http://www.huawei.com/en/about-huawei/publications/communicate/hw-087875.htm> (accessed 31 March 2015). We also mentioned Iran, but as noted, Huawei was only one of several multinationals doing business in Iran.

would be suspicious about what they are doing there. This is especially true because Huawei's commercial interests have often coincided with Chinese government interests in promoting overseas investment and building alliances to secure access to natural resources. Indeed, having discriminated against Huawei for many years,[90] once the firm started expanding overseas and became highly profitable, the Chinese government wanted to share in the glow of its success as a world-leading Chinese business. They started assisting Huawei by granting its foreign customers access to Chinese state bank loans and guarantees — a practice that the US frowns on but is common in many other countries that have export development banks, such as Canada and Australia.[91] Huawei's CEO was also invited to join other leading Chinese business executives on several 'team China' overseas trade missions.[92] This gave Huawei market leverage in many developing countries, but redoubled suspicion in the minds of US Congressmen that the company was just a tool of the Chinese government.[93]

More importantly, there is little doubt that elements of the Chinese military have engaged in extensive cyber-spying against the United States and other governments and against many multinational companies. For example, the US Attorney-General recently brought criminal charges against five Chinese military personnel involved in a special unit within the People's Liberation Army which, according to the indictment, hacked into foreign firms' computer systems and stole huge amounts of sensitive commercial and technical information that would benefit Chinese competitors.[94]

Private Chinese companies like Huawei and ZTE are not involved in these activities, and despite the extensive US Congressional Committee investigation, no evidence was uncovered to suggest that they have taken part in any hacking activities whatsoever. The most that the PSC Report could say was: 'It appears that under Chinese law, ZTE and Huawei would be obligated to co-operate with any request by the Chinese government to use their systems or access them for malicious purposes under the guise of state security'.[95] In other words, they are potentially, rather than actually, guilty.

Finally, according to the PSC Report, Huawei has consistently acted in an evasive manner, failing to fully answer questions or provide sufficient documentation to back up its assertions about the independence of its

90 Zhang, above n 3, Ch 7, gives a detailed account of Huawei's difficult struggle to compete with heavily subsidised state-owned Chinese telecom equipment manufacturers in the early 1990s.

91 Cheng and Liu, above n 3, pp 103, 284–7; see also Huawei's evidence as recorded in the PSC Report, above n 1, p 28. For typical examples of how government export development banks assist corporations in other countries, see the websites of Canada's Export Development Corporation at <http://www.edc.ca/EN/About-Exporting/Trade-Links/Pages/financing.aspx> (accessed 31 March 2015); and Efic in Australia, at <http://www.efic.gov.au/export-community/Pages/bankingandfinance.aspx> (accessed 31 March 2015).

92 Cheng and Liu, above n 3, p 285.

93 PSC Report, above n 1, p 29.

94 See Department of Justice, 'US Charges Five Chinese Military Hackers for Cyber Espionage Against US Corporations and a Labor Organization for Commercial Advantage', 19 May 2014, at <http://www.justice.gov/opa/pr/2014/May/14-ag-528.html> (accessed 31 March 2015).

95 PSC Report, above n 1, p 3.

business, and many of the documents it did provide were 'unsigned copies' or otherwise incomplete.[96] Here Huawei was well and truly 'framed' by the Congressional Committee, in the sense of setting a trap to ensure the firm would appear suspicious. After several lengthy meetings between Huawei executives and Committee staff in 2011–12, at which Huawei responded to numerous questions about its business and provided various documents, the committee followed up with a letter to Ren Zhengfei in June 2012 asking for 'clarifications' along with supporting documentation.

For example, the committee asked for details of 'every contract for goods and services' that Huawei or its subsidiaries had been a party to in the United States, including details of the type of goods, price, quantity and location; and copies of all recommendations provided to Huawei by international management consultants in the past 15 years.[97] Also, details of all Huawei's meetings or interactions with 10 different Chinese government ministries over the past 5 years, plus details of a tax investigation of Huawei by the Chinese government that occurred in 1999 (13 years earlier!), including the 'date, time and location of all meetings between government officials and Huawei officials during the course of the investigation'.[98] Several other requests for clarifications were impossibly vague, such as: 'Has Huawei ever been ordered by the Chinese government to perform a task or seek information on behalf of the government?' and 'Has a Huawei employee, whether with the consent of supervisors or not, ever attempted to obtain private information from an individual, company or government through Huawei's network or equipment? . . . Please provide all documents relating to these incidents'.[99]

All responses and documents had to be submitted, along with English translations, within 3 weeks.[100] For Huawei to have responded fully to this request would have meant providing thousands of pages of documents, most of which would need to be translated from Chinese, many involving commercially sensitive issues that no company would publicly disclose.

Having placed this immense disclosure burden on Huawei with its improbably tight deadline and vague parameters, the committee could easily conclude that Huawei was 'evasive' and 'unresponsive' to some of its questions, and this 'lack of cooperation' by Huawei is a major theme repeated throughout the PSC Report.[101]

Distorting frames for viewing Huawei: Preconceived perceptions among foreign governments and international commentators

While certainly Huawei's behaviour and that of the Chinese government/military may have contributed to foreign government suspicion of

96 Ibid, pp v, 9, 12–13, 14–15.
97 For the letter requesting clarification and documents, see <http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/HuaweiRenZhengfe12JUNE2012.pdf> (accessed 31 March 2015).
98 Ibid.
99 Ibid.
100 Ibid.
101 PSC Report, above n 1, pp v, 9, 12–13, 14–15.

the firm, there is no doubt that many US and Australian policymakers have general perceptions about China that are influenced by the 'China threat' discourse. They will tend to interpret any evidence about Chinese hi-tech firms in the most negative light, and downplay evidence that contradicts their preconceived notions. We showed how the 'China threat' discourse has been strongly advocated by high profile think tanks with ties to the US 'military industrial complex', and supported by politicians with a vested interest in sustaining defence industry jobs in their electoral districts. A typical example directly relevant to Huawei's case is the RAND report, on which many of the conclusions about Huawei's and ZTE's 'military and government ties' were based. This report was commissioned by the US Air Force,[102] and in writing it the RAND Corporation would be especially keen to adopt a hard line stance on China, as one of their previous reports for the US National Intelligence Council was rejected by then CIA Director George Tenet for failing to depict China as a 'clear and present danger'.[103]

The members of the Permanent Select Committee on Intelligence, who passed judgment on Huawei and ZTE, would also have been influenced by the CIA's long history of covert collaboration with US hi-tech business corporations. An early example was ITEK Corporation, which produced the first high resolution camera for use in the CIA's top secret spy satellite program in the early 1960s. Jonathan Lewis describes how ITEK had to create various front businesses to justify raising capital from investors for their secret research and development work on the satellite camera.[104] More recently, the CIA has funded a venture capital firm, In-Q-Tel, whose mission is clearly stated on the firm's website: 'We identify, adapt, and deliver innovative technology solutions to support the missions of the Central Intelligence Agency and broader US Intelligence Community.'[105] Several of In-Q-Tel's leadership teams have links to Silicon Valley, including its CEO Christopher Darby, and trustee James L Barksdale, a former CEO of Netscape Communications and AT&T Wireless.[106] In-Q-Tel claims to receive 10% of its funding from US government agencies and 90% from private investors, and it has already provided capital to around 97 hi-tech businesses in areas such as cyber and mobile security, data analytics, and video and imaging.[107]

While the CIA is quite open about its involvement in In-Q-Tel, presumably there are other classified projects involving US hi-tech firms that remain under the public radar. The leaks by Edward Snowden in 2013 showed that the US National Security Agency (NSA) had been tapping into the trunk lines of US telecom and internet firms for many years, often with the secret cooperation of those firms; and internationally, the NSA had managed to infiltrate the

---

102 See RAND Report, above n 47, front matter.

103 Pan, above n 8, p 81.

104 J E Lewis, *Spy Capitalism: ITEK and the CIA*, Yale University Press, New Haven, 2002; reviewed on the CIA's website at <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no1/article08.html> (accessed 31 March 2015).

105 See In-Q-Tel's website, at <https://www.iqt.org/> (accessed 31 March 2015).

106 'About In-Q-Tel: Team', at <https://www.iqt.org/about-iqt/> (accessed 31 March 2015)

107 'In-Q-Tel Portfolio', at <https://www.iqt.org/portfolio/> (accessed 31 March 2015) and 'About In-Q-Tel', ibid.

online and mobile communications of numerous foreign governments and corporations.[108] While these revelations were not made public until after the PSC Report on Huawei and ZTE was published, one can assume that the Permanent Select Committee's members were aware in broad terms of US cyber intelligence gathering capabilities, and US government agencies' active collaboration with hi-tech firms. They would naturally assume a similar level of covert collusion between Chinese hi-tech firms and the Chinese government or military.

The Snowden leaks made it very clear that if China is involved in similar kinds of cyber espionage, either through the equipment of private firms like Huawei and ZTE or through specialised military intelligence units, it may simply be adopting standard international practice. After the leaks were published, a US government spokesperson tried to distinguish the NSA's conduct from 'Chinese' practices, claiming: 'The NSA breaks into foreign networks only for legitimate national security purposes.'[109] Other reports suggest, however, that the US government and its allies have not been so circumspect, especially in the context of major commercial negotiations. For example, the German chancellor Andrea Merkel protested strongly when leaks revealed that the United States had tapped her personal cellphone during trade talks; and Canada's security agency allegedly hacked into the communications networks of Brazil's mining and energy ministry for commercial reasons relating to oil exploration contracts .[110] The Australian government also caused a major diplomatic row with Indonesia when it emerged that Australia's intelligence agency had hacked into phone calls made by the Indonesian president and used the Australian embassy in Jakarta to collect both political and economic intelligence.[111] Expert commentators noted that Australia 'is part of the Five Eyes intelligence gathering agreement between Australia, the UK, the US, Canada and New Zealand', and 'there's an

108 See the useful archive of articles on the Snowden leaks published by the Washington Post: K Elliott and T Rupar, 'Six months of revelations on NSA', *Washington Post*, 23 December 2013, at <http://www.washingtonpost.com/wp-srv/special/national/nsa-timeline/> (accessed 31 March 2015)

109 Quoted in D E Sanger and N Perlroth, 'NSA Breached Chinese Servers Seen as Security Threat', *New York Times*, 22 March 2014, at <http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?_r=0> (accessed 31 March 2015)

110 See M Birnbaum, 'Germans launch probe into allegations of US spying', *Washington Post*, 24 October 2013, at <http://www.washingtonpost.com/world/uproar-in-germany-continues-over-accusations-that-us-tapped-merkels-phone/2013/10/24/39e4c618-3c96-11e3-b0e7-716179a2c2c7_story.html> (accessed 31 March 2015); and S Ormiston, 'Canada's spying touches nerve in Brazil', *CBC News*, 15 October 2013, at <http://www.cbc.ca/news/world/canada-s-spying-touches-nerve-in-brazil-susan-ormiston-1.2054334> (accessed 31 March 2015).

111 See M Brissenden, 'Australia spied on Indonesian president Susilo Bambang Yudhoyono, leaked Edward Snowden documents reveal', *ABC News Online*, 5 December 2014, at <http://www.abc.net.au/news/2013-11-18/australia-spied-on-indonesian-president-leaked-documents-reveal/5098860> (accessed 31 March 2015); and A Henderson and G Roberts, 'Indonesia says embassy spy claims "just not cricket" as Australian ambassador Greg Moriarty questioned by Foreign Ministry', *ABC News*, 2 November 2013, at <http://www.abc.net.au/news/2013-11-01/australian-ambassador-emerges-from-jakarta-spy-claims-meeting/5064224> (accessed 31 March 2015).

expectation that most embassies in foreign countries probably indulge in some form of intelligence gathering'.[112]

In stark contrast with the Permanent Select Committee's keen focus on intelligence gathering programs was its rudimentary knowledge of Chinese economic reforms over the past three decades. In particular, the committee seemed to assume that all Chinese businesses must be state-controlled, either directly or indirectly; and that a Communist government would not allow a private business to become nationally successful. This attitude is apparent throughout the PSC Report.[113] But it overlooks the massive privatisation of the Chinese economy that has been ongoing since the 1980s, involving millions of business enterprises, to the extent that around 70% of Chinese industrial output is now produced by non-state controlled business firms, and over 80% of the industrial workforce in China is now employed in the private sector.[114] The committee was also blissfully unaware of the exponential growth of mobile phone and internet use in China since the 1990s. In fact, the number of mobile phone users in China grew from around 47,000 in 1991 to over 1.2 billion by late 2013; and the number of internet users grew from effectively zero in the early 1990s to around 632 million by 2014,[115] which provides a perfectly rational explanation for the expansion of firms that service this market with their equipment like Huawei. Instead, however, the committee assumed that Huawei and ZTE's growth must have been subsidised by the Chinese government for its own covert purposes.[116] And the committee wrongly stated: 'Huawei operates in . . . one of seven "strategic sectors" [ie, the telecom industry] . . . considered as core to the national and security interests of the state'.[117] This statement ignores the longstanding distinction between Chinese telecom services, which is indeed a 'strategic sector' strictly controlled by the state, and telecom equipment manufacturing, which has been opened up to private enterprises since the 1980s. The fact that US competitors

112 See L Yaxley, 'Foreign embassies expected to be used for spying: expert', *ABC News: The World Today*, 1 November 2013, citing ANU Professor Michael Wesley, at <http://www.abc.net.au/news/2013-11-01/foreign-embassies-expected-to-be-used-for-spying/5064418> (accessed 31 March 2015).

113 For example, PSC Report, above n 1, pp 22, 24, 26.

114 For historical surveys of privatization in China, see S Yusuf, K Nabeshima and D H Perkins, *Under New Ownership: Privatizing China's State-Owned Enterprises*, Stanford University Press, Palo Alto, CA, 2006; and Zeng, above n 63. For more recent statistics on the size of the private sector, see V Koen, R Herd and S Hill, 'China's March to Prosperity: Reforms to Avoid the Middle-income Trap', *OECD Economics Department Working Papers*, No 1093, 2013, pp 16–18 (OECD Publishing), at <http://dx.doi.org/10.1787/5k3wd3c4219w-en> (accessed 31 March 2015)

115 Statistics for internet users come from China Internet Network Information Center, '34th Statistical Survey on Internet Development in China', July 2014, at <http://www1.cnnic.cn/IDR/> (accessed 15 January 2015); and for recent mobile phone figures, see Xinhua, 'China's Mobile Phone Users Hit 1.22 Billion' *Xinhua Online*, 21 November 2013, at <http://news.xinhuanet.com/english/china/2013-11/21/c_132907784.htm> (accessed 31 March 2015). For earlier statistics on mobile phone users, see Ministry of Industry and Information Technology, '2000 nian qian yidong tongxin fazhan qingkuang' (The development of mobile communications prior to 2000), at <http://www.miit.gov.cn/n11293472/n11293832/n11294132/n12858447/12864552.html> (accessed 31 March 2015).

116 PSC Report, above n 1, pp 27–8.

117 PSC Report, above n 1, p 21.

of Huawei such as Cisco Systems have been able to sell large amounts of network equipment to Chinese state telecom enterprises and government institutions for over two decades underscores the relative openness of this industry sector to private firms.[118] In other words, there is nothing sinister about Huawei's and ZTE's rapid growth when placed within the broader context of Chinese economic reforms, the massive expansion of the consumer market, and the privatisation of large swathes of the economy.

Whether or not these omissions and distortions resulted from lack of knowledge or consciously biased selection, they certainly contributed to narrowing the frame through which the committee interpreted Huawei's and ZTE's behaviour and responses.

To be fair, such a one-dimensional view of Chinese industrial development and corporate governance reform is not confined to US politicians. Many popular accounts of the Chinese political system give the impression that all corporations are controlled by the CCP. Richard McGregor, for example, argues that all Chinese business enterprises work to mobilise the population collectively towards CCP-designated goals, a system he calls 'China Inc', and cites research suggesting that the 'pure private sector' in China is 'minuscule'.[119] Rowan Callick states that the CCP has 'ultimate approval over every investment, and branches in all state-owned enterprises and 85% of private enterprises'.[120] He also quotes Cheng Li, an American expert on Chinese politics, as saying: 'All the state's assets are the Party's in reality, if not in theory.'[121] And Martin Jacques declares that the Chinese government is a 'hyperactive and omnipresent state, which enjoys a close relationship with a powerful body of State Owned Enterprises, a web of connections with the major firms in the private sector, and has masterminded China's economic transformation'.[122] The problem with this kind of analysis is that it downplays the very real differences between the structures and management practices of state-controlled and private firms. Certainly, the Chinese government is still conflicted about the extent to which private enterprises should be allowed to develop within a socialist economy — and rather than using the controversial term *siying qiye* (privately-operated enterprises), the government prefers to call them *minying qiye* (enterprises operated by the people), or *fei gongyouzhi qiye* (non-state-owned enterprises).[123] Yet as we noted earlier, there is still a major distinction between state-controlled enterprises, where the CCP plays a leading role in management decisions and hiring of executives, and private firms, where the CCP is separate from the management and not directly involved in the executive hiring process.

Interestingly, McGregor does also cite a comprehensive survey of Chinese

---

118 See Cisco Systems, '*Gongsi jieshao*' (Introducing the Company), at <http://www.cisco.com/web/CN/aboutcisco/company_overview/about_company_overview_overview.html> (accessed 31 March 2015)

119 R McGregor, *The Party: The Secret World of China's Communist Leaders*, Harper Collins, New York, 2010, pp 34, 197–-9.

120 R Callick, *Party Time: Who Runs China and How*, Black Inc, Collingwood, 2013, pp 142–3.

121 Ibid, p 43.

122 M Jacques, *When China Rules the World*, Penguin Books, London, 2012, p 615.

123 McGregor, above n 119, p 200; and see the CCP's web page for 'non-state-owned enterprises' at <http://dangjian.people.com.cn/fg/> (accessed 31 March 2015).

private entrepreneurs by Bruce Dickson, which suggests that the influence may be working in the other direction. Dickson concluded: 'Party building in the private sector has been more successful at promoting the firms' interests than exerting Party leadership.'[124] But when the PSC Report cites McGregor's book, it only uses those parts that fit within the committee's own frame of reference. For example, 'experts in Chinese political economy agree that it is through these [CCP] Committees that the Party exerts influence, pressure, and monitoring of corporate activities. It is therefore suspicious that Huawei refuses to discuss or describe that Party Committee's membership.'[125]

Likewise, the international media has perpetuated negative stereotypes about Chinese hi-tech firms by repeating inaccurate stories long after they were shown to be false. Virtually every article about Huawei in the mainstream English-language media parrots the firm's supposed 'close ties' to the Chinese military and government without providing any new evidence to support the assertions.[126] Perhaps news editors find it more exciting to write about cyber-spying rather than a highly successful private Chinese business selling telephone and internet hardware, but this is negligent reporting and merely reinforces the distorted frame of reference. Interestingly, the few reporters who carefully read the PSC Report expressed strong doubts about the committee's cyber spying allegations against Huawei, and suggested the underlying issue was more likely US trade protectionism.[127]

Conclusion

Privately controlled Chinese hi-tech firms are easy targets for governments who want to show they are doing something about countering the 'Chinese cyber-threat', even if excluding their products will have little impact on stopping the hackers. US Congressmen and Australian/Canadian/Indian politicians alike are clearly playing to their domestic voters. They think they have nothing to lose and everything to gain by attacking Chinese firms selling

124 Ibid, p 219, citing B Dickson, *Wealth into Power: The Communist Party's Embrace of China's Private Sector*, Cambridge University Press, 2008.

125 PSC Report, above n 1, p 23, citing McGregor, above n 119, even though McGregor is a journalist rather than an 'expert in Chinese political economy', and no page number is given for this opinion attributed to him.

126 For earlier accounts that mention the RAND Report or quote it without acknowledgement, see J Dean, 'Outside of US, Few Fear Huawei', *Wall Street Journal* (Asian ed), 22 February 2008, at <http://online.wsj.com/news/articles/SB120359554277582713> (accessed 31 March 2015); and Tech Law Journal, '3Com Huawei transaction to be reviewed by CFIUS', *Tech Law Journal*, 9 October 2007, at <http://www.techlawjournal.com/topstories/2007/20071009b.asp> (accessed 31 March 2015). For a more recent article citing the PSC Report, see J Robertson, 'The Chart That Helps Explain Cisco's 6,000 Job Cuts', *Bloomberg*, 15 August 2014, at <http://www.bloomberg.com/news/2014-08-14/the-chart-that-helps-explain-cisco-s-6-000-job-cuts.html> (accessed 31 March 2015)

127 For example, P Dwyer, 'Congressional Report on Huawei Smacks of Protectionism', *Bloomberg News*, 9 October 2012, at <http://www.bloomberg.com/news/articles/2012-10-08/congressional-report-on-huawei-smacks-of-protectionism> (accessed 31 March 2015); and Anon, 'Huawei and ZTE Put on hold: Two big Chinese telecoms firms come under fire in America', *The Economist*, 13 October 2012, at <http://www.economist.com/node/21564585?fsrc=scn/fb/wl/pe/putonhold> (accessed 31 March 2015)

mysterious internet technology and competing with US and other Western corporations, especially if they can somehow link the issue to China's human rights record.[128] Yet taxpayers certainly lose out when projects like the National Broadband Network become significantly more expensive, as the most cost-effective bidders are excluded from the competition.[129] And just as seriously, it appears that the Chinese government has started to retaliate against Apple, Microsoft and other international hi-tech firms, restricting purchase of their products by Chinese government officials due to 'security concerns' about foreign infiltration of Chinese networks.[130] Though not a direct response to the PSC Report, these measures occurred soon after the revelations by Edward Snowden that US hi-tech firms had cooperated with the NSA in its cyber espionage programs, and that targets had included Chinese servers and networks.[131] There were even NSA documents revealing a plan to 'exploit Huawei's technology so that when the company sold equipment to other countries — including both allies and nations that avoid buying American products — the NSA could roam through their computer and telephone networks to conduct surveillance and, if ordered by the president, offensive cyber-operations'.[132] It is not clear whether this nefarious plan succeeded, but it reveals how ludicrous the situation has become, when the Chinese firm being accused of (potential) cyber espionage by one arm of the US government is the target of cyber espionage by another arm of the US government.

Huawei has gone to great lengths to assure foreign governments that its products are secure, and some countries like the United Kingdom have welcomed the firm's business after special monitoring safeguards were put in place.[133] But one can predict that whatever Chinese hi-tech firms like Huawei do will be inadequate to convince the United States to welcome them with open arms. Of course it is impossible to have a completely objective view of the 'other', particularly when dealing with very different cultures and political

128 See, eg, C Frates, 'Wolf Continues to Push Lobbying Firm to Drop Chinese Client', *National Journal*, 30 April 2012, at <http://www.nationaljournal.com/blogs/influencealley/2012/04/wolf-continues-to-push-lobbying-firm-to-drop-chinese-client-30> (accessed 31 March 2015), which links to an open letter from Congressman Frank Wolf making a dubious connection between Huawei and Chinese human rights abuses.

129 See S Bevan and J Sturmer, 'NBN review reveals cost blow out' *ABC The World Today*, 12 December 2013, at <http://www.abc.net.au/worldtoday/content/2013/s3910183.htm> (accessed 31 March 2015)

130 US firms that have recently been excluded from bidding on government contracts for 'security reasons' include Apple (iPad and Macbook Air), Symantec Corporation, Kaspersky Lab, and Microsoft (for its Windows 8 system). See K Rushton, 'China bans officials from buying Apple products', *The Telegraph*, 6 August 2014, at <http://www.telegraph.co.uk/technology/apple/11017019/China-bans-officials-from-buying-Apple-products.html> (accessed 31 March 2015).

131 See Sanger and Perlroth, above n 109.

132 Ibid.

133 Huawei has cooperated with the UK government in setting up a cyber security evaluation centre where independent technical analysts can test the company's products for vulnerabilities: see HM Government, 'Huawei Cyber Security Evaluation Centre: Review by the National Security Adviser', at <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266487/HCSEC_Review_Executive_Summary_FINAL.PDF> (accessed 31 March 2015).

systems.[134] But it should be possible to reduce the distortion in the frames through more careful and open-minded investigation. At the root of the problem is the deeply embedded psychological framework of mutual suspicion between opinion leaders and policymakers in the United States and China, and their consequent unwillingness to make the effort to reframe their perspectives and gain a more nuanced and sophisticated understanding of each other's behaviour.

134 Pan, above 8, pp 10–12.