Australia-China Relations Institute
澳中关系研究院

Analysis

Huawei: Critically assessing the 5G ban and commonly cited risks

Colin Hawes

August 18 2022

Key takeaways

- Reports that Huawei is controlled by the government of the People's Republic of China (PRC) are inaccurate. Huawei is a private, employee-owned corporation controlled by its senior management with input from an employee representative committee.
- The Communist Party of China (CPC) branch committees in private PRC corporations, including Huawei, have largely been co-opted by corporations to serve their own commercial interests.
- Contrary to many reports, the number of private PRC firms with CPC committees actually declined between 2017 and 2019 by some 400,000 (or 21 percent).
- There is no convincing evidence that Huawei is a military-backed corporation or has any deep ties with the PRC military, and claims that Huawei has been involved in espionage activities are vague and poorly substantiated.
- Banning Huawei's equipment from 5G networks may be prudent, but it distracts from the real issue.
- Governments of the Five Eyes intelligence sharing network – Australia, Canada, New Zealand, the UK and the US – have intentionally prevented full encryption of network data, claiming that it would impede law enforcement and their own intelligence collection efforts, but this opens up networks to exploitation by hostile governments and criminal elements.

Introduction

In the recent political stoush in Australia over which party was 'tougher' on the People's Republic of China (PRC), the name of information and communications technology company Huawei inevitably came up. The decision in 2018 to exclude Huawei from the 5G rollout was 'one of the best decisions our government has made,' opined Liberal Senator James Paterson in an interview in February.[1] Former foreign minister Marise Payne would doubtless agree, having previously defended the Huawei ban as 'aimed at solely protecting

1 Katherine Murphy, 'Former Asio boss accuses Liberal senator of 'grubby' attack over Huawei comments', *The Guardian*, February 18 2022 <https://www.theguardian.com/australia-news/2022/feb/18/former-asio-boss-accuses-liberal-senator-of-grubby-attack-over-huawei-comments>.

Australia's national interests, and the protection of Australia's national security.'[2] Mike Burgess, the Director-General of the Australian Signals Directorate (ASD), further clarified the reasons: 'The distinction between core and edge collapses in 5G networks. ... A potential threat anywhere in the network will be a threat to the whole network. ... My advice was to exclude high-risk vendors from the entirety of evolving 5G networks.'[3] It is unlikely that the current Labor Government will alter this approach to 5G, as the previous ban on Huawei's involvement in the National Broadband Network was introduced by a Labor government in 2012, and the ALP's communications spokesperson confirmed that 'on matters of infrastructure security, Labor will always take the advice of our security agencies.'[4]

Why is Huawei considered a 'high-risk vendor'?

Huawei is one of the PRC's best-known corporations on the international stage. Yet despite its enormous success – as the world's number one telecom networks equipment maker and number two smartphone seller, with reported revenues of over US$100 billion and operations in over 170 countries[5] – it has become a poster child for the 'China threat' in the United States and many other countries. Australia's 2018 ban of Huawei from supplying 5G networks was just one of many volleys against the firm in a lengthy campaign spearheaded by the US government.[6]

As early as 2012, after a lengthy investigation, the Permanent Select Committee on Intelligence of the US Congress (the 'PSC') expressed 'deep concerns' that 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.'[7] This led to a chain reaction of increasingly severe sanctions against Huawei, including bans on both US government entities and telecom firms from using Huawei's products and network equipment; a ban on US suppliers exporting components to Huawei such as advanced semiconductor chips, which threatens to cripple the firm's business; and a complex, still unresolved, criminal lawsuit against the firm.[8]

Citing potential national security risks, several governments besides Australia, including India, Canada, and Japan, have fully or partially restricted Huawei from bidding on their broadband infrastructure or building

2 Christopher Knaus, 'Marise Payne defends 5G ban on Chinese telcos Huawei and ZTE', *The Guardian*, August 27 2018 <https://www.theguardian.com/australia-news/2018/aug/27/marise-payne-defends-5g-ban-on-chinese-telcos-huawei-and-zte>.

3 Gareth Hutchens, 'Huawei poses security threat to Australia's infrastructure, spy chief says', *The Guardian*, October 30 2018 <https://www.theguardian.com/australia-news/2018/oct/30/huawei-poses-security-threat-to-australias-infrastructure-spy-chief-says>.

4 Tony Walker, 'As the Coalition plays up China fears ahead of an election, how might Albanese position himself?', *The Conversation*, February 10 2022 <https://theconversation.com/as-the-coalition-plays-up-china-fears-ahead-of-an-election-how-might-albanese-position-himself-176683>; and Chris Griffith, 'ALP seeks Huawei briefing', *The Australian*, August 28 2018 <https://www.theaustralian.com.au/business/technology/alp-seeks-huawei-security-briefing/news-story/a31c05868b4b078c9e276d77a94ad624>.

5 Jason Tan, 'Huawei now world's largest telecom equipment-maker', *Caixin Global*, March 19 2018 <https://www.caixinglobal.com/2018-03-19/huawei-now-worlds-largest-telecom-equipment-maker-101223256.html>; Huawei Technologies, 'About Huawei – Corporation information – Milestones' <https://www.huawei.com/en/about-huawei/corporate-information/milestone>; Elizabeth Schulze, 'Huawei smartphone sales surge 50% as Apple and Samsung struggle', *CNBC*, May 1 2019 <https://www.cnbc.com/2019/05/01/huawei-ahead-of-apple-in-q1-2019-smartphone-shipments.html>.

6 For early blows in this campaign, see the US Air Force-funded report: Evan S. Medeiros, Roger Cliff, Keith Crane, James C. Mulvenon, 'A new direction for China's defense industry' (Arlington, VA.: RAND Corporation, 2005), hereafter 'RAND Report', chapter 5; and Steven R. Weisman, 'Sale of 3Com to Huawei is derailed by U.S. security concerns', *New York Times*, February 21 2008 <https://www.nytimes.com/2008/02/21/business/worldbusiness/21iht-3com.1.10258216.html>. Australia's NBN ban in 2012 is another example: See Maggie Lu-YueYang, 'Australia blocks China's Huawei from broadband tender', *Reuters*, March 26 2012 <https://www.reuters.com/article/us-australia-huawei-nbn-idUSBRE82P0GA20120326>. For more recent sources, see nn. 7-8 below.

7 Mike Rogers and Dutch Ruppersberger, *Investigative report on the U.S. national security issues posed by Chinese telecommunications companies Huawei and ZTE*, US House of Representatives, 112th Congress, October 8 2012, pp. vi-vii <https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96> (hereafter, 'PSC Report').

8 Jacob Kastrenakes, 'Trump signs bill banning government use of Huawei and ZTE tech', *The Verge*, August 13 2018 <https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump>; and for the ban on US telecom firms using Huawei's equipment, see *Huawei Technologies USA, Incorporated; Huawei Technologies Company, Limited v Federal Communications Commission; United States of America*, No. 19-60896 (5th Cir. 2021) <https://www.ca5.uscourts.gov/opinions/pub/19/19-60896-CV0.pdf>. For various 'entity lists' and sanctions policies aimed at preventing exports to 'high-risk' Chinese firms including Huawei, see United States Department of Commerce, 'Entity List' <https://www.commerce.gov/tags/entity-list>; and United States International Trade Administration, 'China: US Export Controls' <https://www.trade.gov/country-commercial-guides/china-us-export-controls>. For the criminal lawsuit, see United States District Court, New York East District, *USA vs. Huawei Technologies Co. Ltd. et al*, Superseding Indictment, filed January 24 2019 <https://www.justice.gov/opa/press-release/file/1125021/download>.

their 5G networks.[9] The US government has also exerted extraterritorial pressure on other countries to try to prevent Huawei from doing business in their territories.[10]

Yet when the evidence cited to justify these sanctions is carefully examined, it turns out to be surprisingly thin. The US Congress' PSC Report provides the most detailed attempt to lay out the key 'national security risks' posed by Huawei and their evidential basis, which can be divided into four main points:

1. Ownership;
2. Communist Party branch;
3. Alleged military links; and
4. Espionage allegations.

Assessing the risks

1. Huawei's ownership

The PSC claimed that Huawei had not provided enough clarity on its ownership to prove that it was free from PRC government control.[11] Yet the documents provided by Huawei to the PSC and other widely available independent sources clearly demonstrate that almost 99 percent of Huawei's shares are owned by its employees through the firm's employee union share fund, and the other one percent are owned by Huawei's CEO Ren Zhengfei.[12]

Huawei has a detailed set of Articles that govern the rights of employee shareholders, and an elected employee shareholder 'Representatives' Commission' (the 'Rep Com'). The Articles also set out the criteria for employees to buy or redeem shares, and how they will be priced based on Huawei's net asset value. The shares cannot be transferred or sold, but the company will redeem them when the employee leaves.[13]

Huawei's Rep Com initially consisted of 51 elected employee representatives, but since January 2019, this number has been increased to 115 representatives. They are elected for five-year terms by Huawei's 86,000-plus active employee shareholders, with a voting system based on one vote per employee share.[14] Once the Rep Com is elected, its 115 members then attend the company's shareholder meetings and make decisions

9 For India, see Mehal Srivastava and Mark Lee, 'India said to block orders for ZTE, Huawei Technologies Telecom Equipment', *Bloomberg*, April 30 2010 <http://www.bloomberg.com/news/2010-04-30/india-said-to-block-china-s-huawei-zte-from-selling-phone-network-gear.html>; for Japan, see Reuters staff, 'Japan to ban Huawei, ZTE from govt contracts – Yomiuri,' *Reuters*, December 7 2018 <https://www.reuters.com/article/japan-china-huawei-idUSL4N1YB6JJ>; and for Canada, see Steven Chase, 'Ottawa set to ban Chinese firm from telecommunications bid,' *The Globe and Mail*, October 10 2012 <http://www.theglobeandmail.com/news/politics/ottawa-set-to-ban-chinese-firm-from-telecommunications-bid/article4600199/>. However, Huawei stated that in 2020 it continued to support over 1500 carrier networks across some 170 countries and regions: Huawei Technologies, 'Corporate Information', <https://www.huawei.com/en/corporate-information>.

10 See, for example, Eliza Gkritsi, 'More European countries are turning their backs on Huawei,' *Technode*, November 16 2020 <https://technode.com/2020/11/16/insights-more-european-countries-are-turning-their-backs-on-huawei/>; and for Eastern Europe, see Andreea Brinza, 'How Russia helped the United States fight Huawei in Central And Eastern Europe', *War on the Rocks*, March 12 2020 <https://warontherocks.com/2020/03/how-russia-helped-the-united-states-fight-huawei-in-central-and-eastern-europe/>.

11 PSC Report, pp. 13-14.

12 Colin Hawes, 'Why is Huawei's ownership so strange? A case study of the Chinese corporate and socio-political ecosystem,' *Journal of Corporate Law Studies* 21(1) (2021): 1-38; and for other sources, see Cheng Dongsheng and Liu Lili *Huawei zhenxiang* (The Truth about Huawei) (Beijing: Dangdai zhongguo chubanshe, 2003); revised and updated in 2016, *Huawei sanshi nian* (Huawei at Thirty) (Guiyang: Guizhou renmin chubanshe, 2016). The documents about Huawei's ownership summarised in the PSC Report (pp. 14-20) also support this conclusion.

13 PSC Report, pp. 16-20. Cf. Huawei Technologies, *2018 annual report*, p. 131. Retiring employees can keep their shares and continue to receive dividends, but cannot purchase new shares: see PSC Report, p. 17, p. 20; and Huawei Technologies, ;Who runs Huawei?' <https://www.huawei.com/minisite/who-runs-huawei/en/> [accessed November 3 2019], which states that currently 10.02 percent of the employee shareholders are 'retired and restructured employees'.

14 See Huawei Technologies, 'Who runs Huawei?'. Huawei's total current workforce is around 194,000 employees, but very junior and low-performing Chinese employees cannot participate in the Employee Stock Ownership Plan, and retired or restructured employees have no voting powers: PSC Report, pp. 16-17. Likewise, non-Chinese employees of Huawei in other countries do not directly participate in the Chinese ESOP, but they are given units in employee investment funds managed by Huawei's regional divisions overseas and tied to the company's performance: author's conversation with a senior executive at Huawei's Australian subsidiary, Sydney 2015.

on behalf of the employee shareholders and elect the Board of Directors and the Supervisory Board. Members of these two boards serve for five-year renewable terms.[15]

In practice, as with most large public companies elsewhere in the world, new candidates for Huawei's Board of Directors are nominated by the existing Board and then approved by the Rep Com.[16] All Huawei's Board members are long-serving employees, having joined Huawei during the 1980s or 1990s.[17] There has never been any credible evidence of involvement by external parties, whether government or otherwise, in the selection of Huawei's senior management or Board members.

While Huawei has only two formally registered shareholders, namely the Huawei Investment and Holding Corporation Trade Union Committee ('Huawei TUC', with approximately 99 percent of the equity) and Ren Zhengfei (with around one percent), the Trade Union Committee is merely a nominee shareholder holding those shares on behalf of Huawei's employee shareholders, who exercise their powers through the Rep Com. Indeed, the Trade Union Committee has no members and no concrete existence except as a legal fiction conduit – in Chinese, a 'community legal person' (*shetuan faren*) – whose sole purpose is to hold shares on behalf of others.[18]

It is true that employees who have reached the level of senior management, and especially Ren Zhengfei, exert the most influence over the company's managerial appointments and decision-making, but this is normal in the vast majority of business corporations elsewhere in the world. Allegations of some other external locus of control over Huawei's ownership, such as the PRC government, lack any convincing evidential basis.[19]

2. Huawei's Communist Party branch

The PSC also claimed that because the Communist Party of China (CPC) has a branch committee within Huawei, this is further evidence of PRC government control, because 'experts in Chinese political economy agree that it is through these Committees that the Party exerts influence, pressure, and monitoring of corporate activities.'[20]

However, this characterisation of the CPC's role in Huawei (and in most other private Chinese firms) is inaccurate. Several rigorous empirical studies have demonstrated that, in the words of George Washington University Professor of Political Science Bruce Dickson, 'Party building in the private sector has been more successful at promoting the firms' interests than exerting Party leadership.'[21] Likewise, Hong Kong academics Xiaojun Yan and Jie Huang found that 'most Party branches within private enterprises just do what the business owners want, never what the owners don't want,' and the Party's 'organisational presence in private

15 Huawei Technologies, *2018 Annual Report,* p. 131; PSC Report, pp. 18-19. The Supervisory Board theoretically monitors the Board of Directors and has powers to bring lawsuits for breach of directors' duties, but up to now the role of Supervisory Boards in most PRC companies has been a passive one, due to the relatively low status of Supervisors as company employees compared to senior executives. See discussion in Colin Hawes and Grace Li, 'Transparency and opaqueness in the Chinese ICT cector: A critique of Chinese and international corporate governance norms', *Asian Journal of Comparative Law*, vol. 12(1) (May 2017): 41-80; and Donald C. Clarke, 'The independent director in Chinese corporate governance," *Delaware Journal of Corporate Law*, 31 (2006): 125-228, at pp. 173-5.

16 PSC Report, p. 16; and for entrenchment of existing management in international firms through board nomination and share proxy practices, see Paul Redmond, *Companies and Securities Law* 5th ed. (Pyrmont, NSW: Thomson Reuters Lawbook Co., 2009), 2.185 and 6.85.

17 Huawei Technologies, *2018 Annual Report*, pp. 135-9.

18 There is a slight complication pointed out by Balding and Clarke that in 2003, Huawei established a 100 percent holding company on top of Huawei Technologies, so the employee shareholding trade union committee referred to in the main text is actually holding around 99 percent of the shares of the holding company Huawei Investment and Holding Corporation, and this Holding Corporation owns 100 percent of the shares of Huawei Technologies Corporation: Christopher Balding and Donald C. Clarke, 'Who owns Huawei', April 17 2019, SSRN, pp. 3-4 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3372669>. So, when we talk about the Rep Com above, it refers to the Holding Corporation, but all decisions of the Holding Corporation are presumably then duplicated by Huawei Technologies: for example, according to their corporate records, the Boards of Directors and Supervisors of Huawei Holding and Huawei Technologies are exactly the same people: see Baidu Enterprise Credit, 华为投资控股有限公司 <https://xin.baidu.com/detail/compinfo?pid=xlTM-TogKuTwp4lstb5Hlq2s4pLs-uuwjwmd> and 华为技术有限公司 <https://xin.baidu.com/detail/compinfo?pid=xlTM-TogKuTwmQldC%2A09kbLmkDAjgAlc1gmd&fl=1&castk=LTE%3D>.

19 For detailed analysis, see Colin Hawes, 'Why is Huawei's ownership so strange? A case study of the Chinese corporate and socio-political ecosystem,' *Journal of Corporate Law Studies* 21(1) (2021): 1-38.

20 PSC Report, p. 23.

21 Bruce Dickson, *Wealth into Power* (Cambridge University Press, 2008), p. 111. See also Xiaojun Yan and Jie Huang, 'Navigating unknown waters: The Chinese Communist Party's new presence in the private sector,' *The China Review,* 17(2) (2017), pp. 37-63; and Fan Xia, 'Woguo siying qiye dang zuzhi gongneng he shixian tujing yanjiu' (A study of the functions and implementation practices of Party organizations in Chinese private enterprises), Ph.D. dissertation, Shandong University 2016.

enterprises may have been expanded, but the benefits of its business-oriented party building tend to accrue to private entrepreneurs rather than to the party-state.'[22]

Private firms' CPC Committee members are appointed by the firm's management, not by the PRC government. To ensure there is not a competing CPC power centre within the business, in many private firms, the CEO/founder simply appoints him or herself as the firm's Party Secretary.[23] One national survey in 2010 found that almost 70 percent of private entrepreneurs with Party membership were also the Party Secretaries for their enterprises,[24] a phenomenon known as the 'familisation' (or co-opting) of CPC branches by the controlling shareholders of private firms.[25]

Not surprisingly, this disjunction between personal/firm incentives and Party building means that short-term profits tend to be prioritised over Party initiatives like anti-corruption, environmental protection, and tedious study of the latest speeches of PRC President Xi Jinping issued by Party Central in Beijing. In most private firms, Party branches only hold meetings once every three to six months, and in 15 percent of firms, there are no regular Party meetings at all, with the Party branch being just an empty shell.[26] Only 0.4 percent of private entrepreneurs in the PRC in one national survey thought that CPC branches were essential to the operation of their businesses.[27]

Contrary to numerous media reports that President Xi has expanded the Party's presence in private PRC firms,[28] the author's own research reinforces the message of these empirical studies that the CPC's role in private firms is anaemic and in decline. The author found that between 2017 and 2019, the number of private PRC firms with CPC committees actually declined by some 400,000 (or 21 percent).[29]

In contrast to many other firms, Huawei's CPC branch is quite active, but its role is not a political one. Huawei's management has effectively co-opted its CPC branch to serve as a motivational training centre, developing employees' ethical values and psychological resilience, to enable them to contribute better to Huawei's performance.[30]

While Huawei's Party branch (and its CEO Ren Zhengfei) borrow revolutionary language from former Chairman Mao's speeches and the CPC's revolutionary history, they have radically reinterpreted this language for the corporate context. For example, the CPC branch has organised regular 'self-criticism' sessions, where the firm's various divisions can meet and publicly reflect on the errors they have made, and how they should improve the effectiveness of the company's products and systems. 'Self-criticism' was a harsh revolutionary technique promoted during political campaigns by Chairman Mao, but Ren Zhengfei claimed that the company's version of self-criticism was much 'gentler'. He likened it to 'hitting employees a hundred times with a soft pillow.' Even if the blows are soft, they will remind employees to keep improving their work.[31]

Of course, Huawei's Party branch certainly promotes broader CPC policies within the firm, such as President Xi's eco-civilisation campaign, and organises regular entertainment/propaganda shows to commemorate Party anniversaries, such as National Day. And like all other PRC organisations, Huawei needs to ensure that its employees do not rock the political boat by actively challenging the CPC's rule, something that Ren Zhengfei

22 Xiaojun Yan and Jie Huang, 'Navigating unknown waters: The Chinese Communist Party's new presence in the private sector,' *The China Review,* 17(2) (2017): 37-63 at p. 55.
23 Wei Zhang, 'Minqi waiqi weihe dou yao jian dangwei?' (Why are private and foreign enterprises all setting up Party committees?), *Beijing Youth Daily*, July 6 2015 <http://epaper.ynet.com/html/2015-07/06/content_141902.htm?div=-1>.
24 Xiaojun Yan and Jie Huang, 'Navigating unknown waters: The Chinese Communist Party's new presence in the private sector,' *The China Review,* 17(2) (2017): 37-63 at p. 52.
25 Ibid., pp. 54-5.
26 Fan Xia, 'Woguo siying qiye dang zuzhi gongneng he shixian tujing yanjiu' (A study of the functions and implementation practices of Party organizations in Chinese private enterprises), Ph.D. dissertation, Shandong University 2016, pp. 72-3, 78.
27 Cited in Xiaojun Yan and Jie Huang, 'Navigating unknown waters: The Chinese Communist Party's new presence in the private sector,' *The China Review,* 17(2) (2017): 37-63 at p. 55.
28 See, for example, Richard McGregor, 'How the state runs business in China,' *The Guardian*, July 25 2019 <https://www.theguardian.com/world/2019/jul/25/china-business-xi-jinping-communist-party-state-private-enterprise-huawei>; and Jude Blanchette, 'Against atrophy: Party organizations in private firms,' *Made in China Journal*, April 18 2019 <https://madeinchinajournal.com/2019/04/18/against-atrophy-party-organizations-in-private-firms/>.
29 Colin Hawes, The Chinese Corporate Ecosystem (Cambridge University Press, 2022), chapter 4 <https://www.cambridge.org/au/academic/subjects/law/corporate-law/chinese-corporate-ecosystem>.
30 For more details, see Colin Hawes, *The Chinese Transformation of Corporate Culture* (Routledge, 2012), chapter 2.
31 Ibid., pp. 38-9.

has emphasised in his speeches to employees.[32] Yet within this generally assumed political framework, there is a great deal of flexibility in how private firms like Huawei utilise their CPC branches.

3. Alleged military links

The PSC also expressed its deep suspicion that Huawei may have hidden links with the PRC military, due to Ren Zhengfei's previous career in the People's Liberation Army. They claimed that the military continues to influence Huawei's business both as an important customer and a financial backer of the firm.[33] However, the evidential foundations for these alleged military links are shaky.

It is true that Ren Zhengfei was once a relatively low-ranking officer in the PRC military construction corps. However, he left the army during a major military downsizing in 1983, and a few years later in 1987 set up a small private business selling simple telephone exchange switches imported from Hong Kong, which later grew into Huawei.[34]

In making its claims about Huawei's continuing military influence, the PSC mainly relied on a 2005 report by the RAND Corporation, an American defence-focused think tank. This report claimed that Huawei was part of a new 'digital triangle' between the PRC 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.'[35] However, a careful reading of this RAND report reveals that its only named source for these assertions is a brief and rather speculative magazine article by reporter Bruce Gilley from 2000, which is then massaged and misquoted to spin 'deep ties,' 'military patronage' and 'R&D partnerships'.[36] If this is the best evidence that a well-funded US congressional intelligence committee can dig out for Huawei's military ties, the substance of the allegations is highly dubious.

Huawei has never denied that it sells telecom and network equipment to the PRC military, making up less than 0.1 percent of the company's overall sales.[37] But this is a far cry from the military being an 'important customer' and 'financial backer' of the firm.

4. Espionage allegations

Even if Huawei has no military links or direct PRC government control, the US government has alleged that Huawei's network equipment could still be used to transmit sensitive information back to Beijing, and that Huawei would not be able to refuse demands by the PRC security and intelligence services to cooperate with such espionage activities, which potentially threatens US national security.[38] This 'potential threat' argument is also the stated basis for Australia's 5G ban on Huawei.[39]

Without access to classified information, it may not be possible to definitively answer the question whether Huawei's network equipment poses a 'potential' national security threat. Yet none of the various public investigations of Huawei have uncovered any evidence of the company assisting the PRC government to engage in espionage or seeking to undermine the security of foreign governments.[40] The UK government has conducted the most intense scrutiny of Huawei's telecom and network equipment, with continuous testing by independent technical experts since 2003 through the Huawei Cyber Security Evaluation Centre (HCSEC). The Centre's annual reports have certainly criticised technical vulnerabilities in Huawei's products, and have

32 Ibid., chapter 2.
33 PSC Report, pp. 13-14, 21-2, 24-5.
34 See Guanjing Zhang, *Huawei si zhang lian* (The four faces of Huawei) (Guangdong: Jingji chubanshe, 2007), pp. 23-4, 135, 223-4.
35 Evan S. Medeiros, Roger Cliff, Keith Crane, James C. Mulvenon, 'A new direction for China's defense industry' (Arlington, VA.: RAND Corporation, 2005), hereafter 'RAND Report', p. 218-21.
36 Bruce Gilley, 'Huawei's fixed line to Beijing,' *Far Eastern Economic Review* (28 Dec. 2000), pp. 94-8 at 94.
37 See testimony provided by Huawei to the PSC investigators: PSC Report, p. 34.
38 PSC Report, p. 3.
39 Gareth Hutchens, 'Huawei poses security threat to Australia's infrastructure, spy chief says', *The Guardian*, October 30 2018 <https://www.theguardian.com/australia-news/2018/oct/30/huawei-poses-security-threat-to-australias-infrastructure-spy-chief-says>.
40 Of the two US criminal cases currently under way against Huawei, neither involves charges of espionage or PRC government interference. One involves alleged breach of US trade sanctions, especially in Iran, and related bank fraud; the other case rehashes a previous civil lawsuit in which Huawei was found liable for stealing trade secrets related to a mobile phone screen robotic testing device from a US firm T-Mobile.

required the company to remediate defects in its software engineering and cyber security processes to prevent potential breaches.[41] Yet its 2019 report concluded: 'NCSC does not believe that the defects identified are a result of Chinese state interference.'[42] In other words, the UK government's National Cyber Security Centre, which has a duty to protect UK citizens from cyber risks, has not detected any PRC government/military 'interference' in any of Huawei's hardware or software that is used in the UK.

Likewise, in a detailed April 2019 investigation of Huawei by the *Los Angeles Times*, the reporters concluded: 'None of the US intelligence officials interviewed over several months for this story have made information public that supports the most damning assertions about China's control over Huawei and about Ren's early ties to Chinese military intelligence. They have yet to provide hard evidence and, privately, these officials *admit they don't have any*' (author's emphasis).[43]

Of course, there have been occasional media reports alleging Huawei's involvement in espionage activities, but most are based on unverifiable tips by anonymous sources or speculation.[44] A typical example is a December 2021 *Bloomberg* article alleging that 'Chinese spies ... infiltrated the ranks of Huawei technicians' back in 2012, and installed a software update containing 'malicious code' on the network of a 'major Australian telecommunications company,' which sent information from the network back to the PRC for a few days before self-destructing.[45] The report claims that this incident was a 'core part of the case built against' Huawei by several governments, who suspect that the firm has been a 'conduit for espionage,' but the evidence presented in the report is unconvincing for several reasons. First, it states that investigators of the alleged breach 'arrived too late,' and only 'fragments of the malicious code' still remained, so they had to 'reconstruct the attack' using 'human informants and secretly intercepted conversations.' The risks of relying on human informants in intelligence gathering are widely known.[46] Second, Australia's three major telecommunications firms all denied that any such incident took place: Telstra has never installed Huawei equipment in its networks, and both Optus and TPG Telecom rejected the claim that their systems had been compromised. This is problematic, because the report also cites a statement from the Australian Signals Directorate that 'whenever ASD discovers a cyber incident affecting an entity, it engages the relevant entity to provide advice and assistance.'[47] Third, the reporters 'didn't find evidence that Huawei's senior leadership was involved with or aware of the attack,' and could not specify what information was taken, or 'what, if anything, the attackers did' with the information.[48]

41 HCSEC Oversight Board, *Annual Report 2019: A report to the National Security Adviser of the United Kingdom*, March 2019, p. 4 <https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019>.
42 Ibid., p. 21.
43 My emphasis. Norman Pearlstine et al, 'The man behind Huawei,' *Los Angeles Times*, April 10 2019 <https://perma.cc/EQL3-W2RB>.
44 See, for example, Salem Solomon, 'After allegations of spying, African Union renews Huawei alliance,' *Voice of America News,* June 7 2019 <https://www.voanews.com/africa/after-allegations-spying-african-union-renews-huawei-alliance>; Huawei Technologies, 'Court orders Lithuanian news outlet to retract false statements on Huawei', October 11 2019 <https://www.huawei.com/en/facts/voices-of-huawei/court-orders-lithuanian-news-outlet-to-retract-false-statements-on-huawei>.; and Reuters staff, 'Dutch telecoms firm KPN: no sign Huawei has improperly monitored users', *Reuters,* April 19 2021 <https://www.reuters.com/article/kpn-huawei-tech-report-idUSL1N2MC0CZ>.
45 Jordan Robertson and Jamie Tarabay, 'Chinese spies accused of using Huawei in secret Australia telecom hack,' *Bloomberg News*, December 17 2021 <https://www.bloomberg.com/news/articles/2021-12-16/chinese-spies-accused-of-using-huawei-in-secret-australian-telecom-hack>.
46 See, for example, Martin Chulov and Helen Pidd, 'Defector admits to WMD lies that triggered Iraq war,' *The Guardian*, February 15 2011 <https://www.theguardian.com/world/2011/feb/15/defector-admits-wmd-lies-iraq-war>.
47 Ibid.
48 Ibid. No espionage cases against Huawei have led to prosecutions, except for the 2019 arrest of Huawei's Polish sales manager Wang Weijing for allegedly acting as a PRC 'intelligence agent' and attempting to obtain information about the Polish government's networks to assist Huawei's sales bids. However, over two years later, this case has stalled: Wang was briefly released by the judge in June 2021; prosecutors then appealed this decision and re-arrested Wang in July 2021, but no further updates are available. Romanian academic Andreea Brinza has suggested that Poland and other East European countries are keen to retain US political and military support by publicly making a show of coming down hard on Huawei with sanctions, but when US attention is diverted elsewhere, they quietly shelve their initiatives. The much-delayed prosecution of Wang may be another example of this political gamesmanship. See Joanna Plucinska, Koh Gui Qing, Alicja Ptak and Steve Stecklow, 'How Poland became a front in the cold war between the U.S. and China,' *Reuters*, July 2 2019 <https://www.reuters.com/investigates/special-report/huawei-poland-spying/>; Monika Scislowska, 'Huawei ex-director on trial in Poland on China spying charge,' *APNews*, June 2 2021 <https://apnews.com/article/asia-pacific-europe-poland-china-business-2c7d6f2e3c42f7883f54b3d70e7fae6c>; and for Wang's initial release and re-arrest, see Sylwia Czubkowska, 'Staszek Wang ponownie zatrzymany przez służby. Kulisy ciągnącej się od 2,5 roku sprawy' (Staszek Wang again detained by the services. Behind the scenes of the case that has been dragging on for 2.5 years), *Spider's Web*, July 31 2021 <https://spidersweb.pl/2021/07/staszek-wang-abw-zatrzymanie.html>; Andreea Brinza, 'How Russia helped the United States fight Huawei in Central And Eastern Europe', *War on the Rocks*, March 12 2020 <https://warontherocks.com/2020/03/how-russia-helped-the-united-states-fight-huawei-in-central-and-eastern-europe/>.

Even if such an incident is taken at face value – as a foreign intelligence agency taking advantage of a flaw in Huawei's software without the company's knowledge – it is not clear why it differs from numerous similar incidents by state-backed hackers, criminals and fraudsters that have compromised US or multinational technology firms using phishing and other methods, such as Microsoft, Apple, Google, Cisco Systems, and many others.[49]

More broadly, the commonly cited argument that the CPC and its intelligence services could simply compel large PRC corporations to risk their whole businesses by handing over their source code for government exploitation[50] ignores the fact that both private and state-owned PRC corporations do regularly resist CPC policies and orders when their commercial interests would be threatened.[51] Part of the reason is that both the Central CPC and its security services are themselves riven by corruption and factional infighting, as is clear from thousands of recently prosecuted anti-corruption cases, including a minister and two deputy ministers of state security, and numerous senior public security officials.[52] And much of this corruption involves the 'capture' of government officials by private corporations.[53]

Problems with the 'potential threat' test

Without convincing evidence of Huawei's involvement in espionage or PRC government/military control of Huawei, the sanctions and bans of the firm by Australia, the US, and other countries must be justified based on the 'potential' rather than actual threat of harm.[54]

The problem is that the potential national security threat will not be overcome by restricting Huawei from critical infrastructure, even if this is a prudent approach. The networks and software operating systems of numerous technology and other firms are regularly exploited by criminal cyberhackers and state-backed actors. Serious disruption of public institutions, banks, and critical infrastructure has occurred in both the US and Australia, causing economic losses to businesses and consumers.[55] The perpetrators are able to exploit those systems and cause major damage without using any Huawei network equipment. Banning PRC firms like Huawei only gives a false sense of security to Australian network users.

Technology experts have identified one key reason for this cyber vulnerability: governments of the Five Eyes intelligence sharing network, led by the US, have intentionally prevented full encryption of network data due to their own law enforcement and intelligence collection concerns. They have promoted legislation requiring tech companies to leave 'back doors' to allow law enforcement and security service access. A 2019 Five Country ministerial communique declared: 'Tech companies should include mechanisms in the design of their encrypted products and services whereby governments, acting with appropriate legal authority, can obtain

49 For just a few recent examples, see Kif Leswing, 'Apple iPhones can be hacked with spyware even if you don't click on a link, Amnesty International says', *CNBC,* July 19 2021 <https://www.cnbc.com/2021/07/19/apple-iphones-can-be-hacked-even-if-the-user-never-clicks-a-link-amnesty-international-says.html>; Lily Hay Newman, "This Is really, really bad": Lapsus$ Gang claims Okta hack', *Wired*, March 22 2022 <https://www.wired.com/story/okta-hack-microsoft-bing-code-leak-lapsus/>; Joseph Menn, 'Microsoft says new breach discovered in probe of suspected SolarWinds hackers,' *Reuters*, June 28 2021 <https://www.reuters.com/technology/microsoft-says-new-breach-discovered-probe-suspected-solarwinds-hackers-2021-06-25/>; Catalin Cimpanu, 'Hackers have started attacks on Cisco RV110, RV130, and RV215 routers,' *ZDNet*, March 3 2019 <https://www.zdnet.com/article/hackers-have-started-attacks-on-cisco-rv110-rv130-and-rv215-routers/>; Dan Milmo, 'Google warns of surge in activity by state-backed hackers,' *The Guardian*, October 15 2021 <https://www.theguardian.com/technology/2021/oct/15/google-warns-surge-activity-state-backed-hackers>.

50 See, for example, Simeon Gilding, 'Editors' picks for 2020: 5G choices: a pivotal moment in world affairs,' *The Strategist*, Australian Strategic Policy Institute, reprint of article from January 20 2020 <https://www.aspistrategist.org.au/editors-picks-for-2020-5g-choices-a-pivotal-moment-in-world-affairs/>.

51 Numerous examples are provided in Colin Hawes, The Chinese Corporate Ecosystem (Cambridge University Press, 2022), chapters 2-4 <https://www.cambridge.org/au/academic/subjects/law/corporate-law/chinese-corporate-ecosystem>.

52 Ibid., chapter 4.

53 Ibid., chapter 5.

54 Gareth Hutchens, 'Huawei poses security threat to Australia's infrastructure, spy chief says', *The Guardian*, October 30 2018 <https://www.theguardian.com/australia-news/2018/oct/30/huawei-poses-security-threat-to-australias-infrastructure-spy-chief-says>.

55 For a useful list of Australian examples, see Webber Insurance Services, 'The complete list of data breaches in Australia for 2018-2022', <https://www.webberinsurance.com.au/data-breaches-list>; for a recent US example, see Stephanie Kelly and Jessica Resnick-ault, 'One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators,' *Reuters,* June 9 2021 <https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/>.

access to data in a readable and usable format.'[56] Australia has already introduced such a legal mechanism in its *Telecommunications and Other Legislation Amendment (Assistance and Access) Act* (Cth 2018), 'on a very short timetable, with little public consultation or parliamentary debate.'[57]

While law enforcement and national security concerns are important, unfortunately 'there is no way to make a door that only the 'good guys' can open and the 'bad guys' cannot. Creating a back door weakens the security of the whole system and puts all its users at risk,' making us 'vulnerable to the crimes we collectively are trying to prevent.'[58]

Conclusion: A complex issue with no simple solution

To sum up, the evidence against Huawei is surprisingly weak, and banning the company from Australia's networks will not protect the country from continued cyber-intrusions from 'hostile powers' and organised criminals. Difficult decisions are required to balance individual privacy with domestic law enforcement and national security access. This does not mean Australia should open its networks to Huawei's 5G equipment, but it does mean that real protection will only come from the hard grind of continuous, long-term multilateral efforts to reduce tensions with the PRC and other authoritarian states, and to incentivise them to introduce further political reforms.

Author

Colin Hawes is Associate Professor in the Law Faculty at University of Technology Sydney (UTS), and a Research Associate at the Australia-China Relations Institute.

Dr Hawes joined the UTS Law Faculty in 2005 after obtaining his PhD at the University of British Columbia and practising law in Vancouver, Canada. He has published three books and numerous articles on Chinese law and society and Chinese corporate governance in international journals such as *Law and Society Review*, *Journal of Corporate Law Studies*, and the *American Journal of Comparative Law*.

Colin is interested in the intersection between corporations, law, and the natural/human environment. His research focuses on the complex dynamic networks of Chinese corporations, the growth of legal precedents and creative interpretation of corporate law by Chinese judges, and the impact of technology on the operation of the Chinese legal system.

His most recent book, *The Chinese Corporate Ecosystem* (Cambridge University Press, 2022), shows how Chinese corporations have co-evolved by interacting creatively with their sociopolitical environment, leading to rapid growth yet massive ecological degradation. The book proposes channelling the 'vital energies' (qi) of government officials and corporate leaders through realigned incentive mechanisms to reverse the damage.

Colin has also acted as an expert witness in Australian and Canadian courts, and advised Chinese and international corporations on cross-cultural legal issues and minimizing the risks of cross-border legal disputes.

56 Christopher Parsons, 'Canada's new and irresponsible encryption policy: How the government of Canada's new policy threatens Charter rights, cybersecurity, economic growth, and foreign policy', *Citizen Lab*, August 21 2019 <https://citizenlab.ca/2019/08/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cybersecurity-economic-growth-and-foreign-policy/>.

57 Keiran Hardy, 'Australia's encryption laws: practical need or political strategy?' *Internet Policy Review*, vol. 9(3) (August 26 2020) <https://doi.org/10.14763/2020.3.1493>; and for a survey of other countries, see M.J. Masoodi and Alexander Rand, 'Why Canada must defend encryption,' *Cybersecure Policy Exchange,* September 2021 <https://www.cybersecurepolicy.ca/why-canada-must-defend-encryption>.

58 Internet Society, 'Breaking encryption myths: What the European Commission's leaked report got wrong about online security,' November 19 2020, pp. 1, 4 <https://www.internetsociety.org/resources/doc/2020/breaking-the-myths-on-encryption/>.