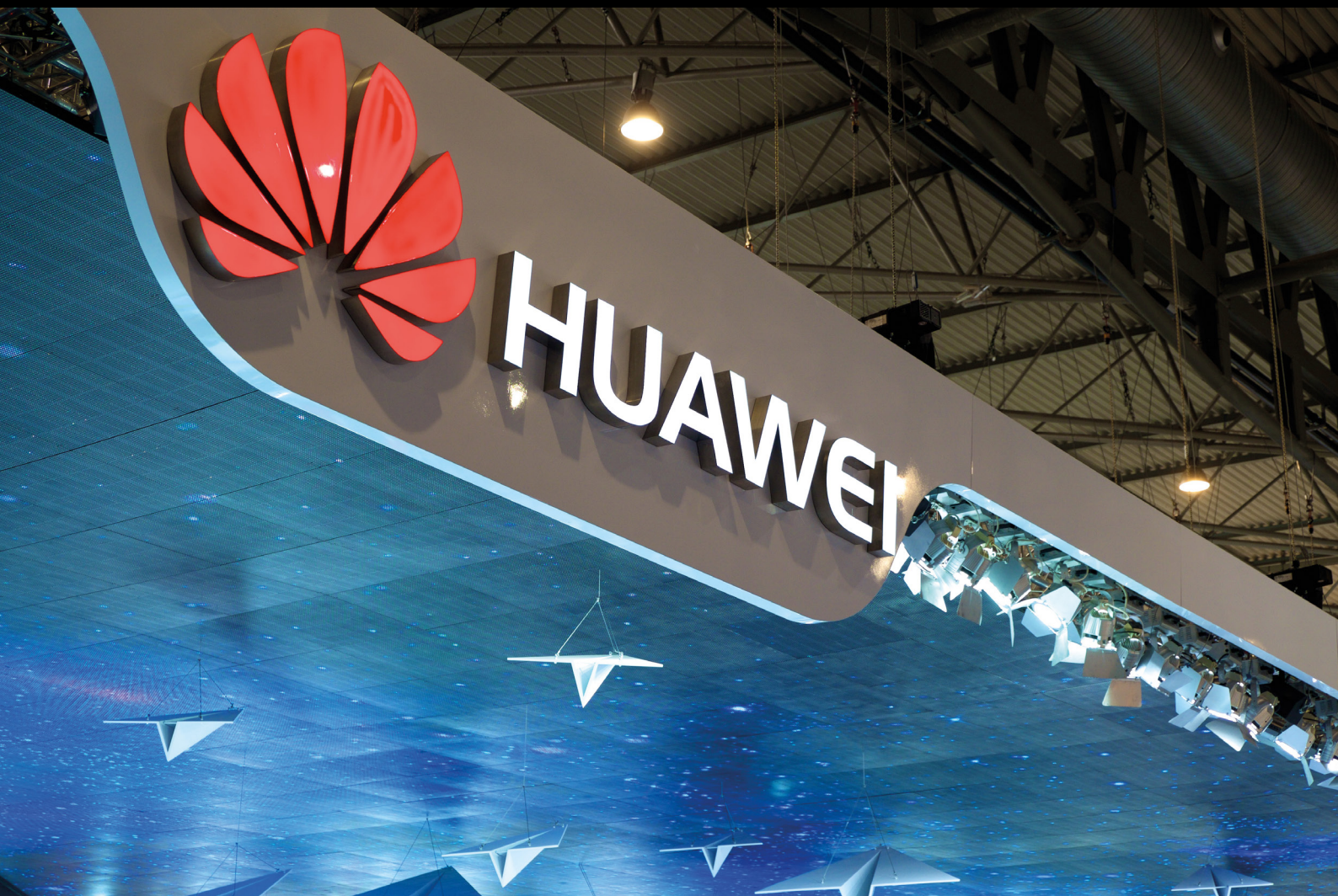


Huawei and Australia's 5G Network

Views from ASPI



What is ASPI?

The Australian Strategic Policy Institute (ASPI) was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

ASPI International Cyber Policy Centre

The ASPI International Cyber Policy Centre's mission is to shape debate, policy and understanding on cyber issues, informed by original research and close consultation with government, business and civil society.

It seeks to improve debate, policy and understanding on cyber issues by:

1. conducting applied, original empirical research
2. linking government, business and civil society
3. leading debates and influencing policy in Australia and the Asia-Pacific.

We thank all of those who contribute to the ICPC with their time, intellect and passion for the subject matter. The work of the ICPC would be impossible without the financial support of our various sponsors.

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

ASPI

Tel +61 2 6270 5100


Fax + 61 2 6273 9566

Email enquiries@aspi.org.au

www.aspi.org.au

www.aspistrategist.org.au

 facebook.com/ASPI.org

 [@ASPI_ICPC](https://twitter.com/ASPI_ICPC)

www.aspi.org.au/icpc/home

© The Australian Strategic Policy Institute Limited 2018

This publication is subject to copyright. Except as permitted under the *Copyright Act 1968*, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Enquiries should be addressed to the publishers. Notwithstanding the above, educational institutions (including schools, independent colleges, universities and TAFEs) are granted permission to make copies of copyrighted works strictly for educational purposes without explicit permission from ASPI and free of charge.

First published October 2018

Cover image: Huawei exhibition stand at Mobile World Congress, Barcelona 2015, courtesy of flickr user [Karlis Dambrans](#).

Huawei and Australia's 5G Network

Views from ASPI

Report No. 8/2018



Contents

Introduction	03
Danielle Cave	
Much ado about Huawei (part 1)	04
Elsa Kania	
Much ado about Huawei (part 2)	05
Elsa Kania	
The technical reasons why Huawei is too great a 5G risk	07
Tom Uren	
Huawei highlights China's expansion dilemma: espionage or profit?	08
Danielle Cave	
Business as usual? Huawei and the Australian Parliament	10
Fergus Hanson and Jessica Clarence	
Government must protect critical infrastructure from external control	11
Peter Jennings	
The campaign against Huawei	14
Greg Austin	
The African Union headquarters hack and Australia's 5G network	16
Danielle Cave	
Huawei: lessons from the United Kingdom	19
Tom Uren	
5G futures: Why Huawei when open source may be the new black?	21
Michael Shoebridge	
Huawei and 5G: clarity in an uncertain world	23
Michael Shoebridge	
Banning Huawei the right decision for Australia's security	25
Peter Jennings	
Huawei ban part of global move to set limits on Chinese influence	27
Michael Shoebridge	
Why Australia banned Huawei from its 5G telecoms network	29
Tom Uren and Danielle Cave	
Huawei and the ambiguity of China's intelligence and counter-espionage laws	31
Samantha Hoffman and Elsa Kania	

Introduction

Over the course of 2018, ASPI staff and writers for *The Strategist* participated in a dynamic public debate about the participation of Chinese telecommunications equipment manufacturer Huawei in Australia's 5G network.

Australia's 5G network is critical national infrastructure, and this was one of the most important policy decisions the government had to make this year. ASPI felt it was vital to stimulate and lead a frank and robust public discussion, in Australia and throughout the wider region, which analysed and debated the national security, cybersecurity and international implications of Huawei's involvement in this infrastructure.

In this report, you'll read analysis authored by:

- Peter Jennings, Executive Director of ASPI
- Michael Shoebridge, Director of the Defence & Strategy Program, ASPI
- Fergus Hanson, Head of ASPI International Cyber Policy Centre (ICPC)
- Danielle Cave, Senior Analyst, ASPI ICPC and PhD Scholar, Coral Bell School of Asia Pacific Affairs, ANU
- Tom Uren, Visiting Fellow ASPI ICPC, seconded from the Department of Defence
- Elsa Kania, Adjunct Fellow at the Center for a New American Security's Technology & National Security Program, non-resident ASPI ICPC fellow and PhD scholar, Harvard University
- Dr Samantha Hoffman, non-resident ASPI ICPC fellow and visiting Academic Fellow, Mercator Institute for China Studies, Germany
- Dr Greg Austin, Professor in the Australian Centre for Cyber Security at the University of NSW (Canberra)
- Jessica Clarence, former intern, ASPI ICPC.

The issue was complicated and multidimensional. And this wasn't the first time Huawei had found itself subjected to intense scrutiny in Australia. In 2012, a Labor government banned Huawei from supplying systems for the National Broadband Network.

Over the following pages, in chronological order from March to September 2018, you'll read a range of views written up in *The Strategist*, *The Australian* and *The Financial Times*. These articles tackle a variety of issues surrounding the decision, including the cybersecurity dimension, the broader Australia-China relationship, other states' experiences with Huawei, the Chinese Government's approach to cyber espionage and intellectual property theft and, importantly, the Chinese party-state's view of state security and intelligence work.

On 23 August 2018, the Liberal-National Government effectively banned Huawei from participating in the 5G network. Notably, and reflecting this public debate, [the media release stated](#):

The Government considers that the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference.

Most of the following articles were published on *The Strategist*. Many were among the most well-read *Strategist* articles of the year, recording thousands of unique views per post and attracting feedback from politicians, senior public servants, business and civil society in Australia and overseas.

When it comes to important national security, cybersecurity and critical infrastructure decisions, ASPI will continue to stimulate Australian public discourse and fill gaps in global debates. We also encourage the Australian Government to take a more [forward-leaning approach](#) to its participation in public discourse so that the public and key stakeholders are as informed as possible when hard and complicated policy decisions like this need to be made.

Danielle Cave

Much ado about Huawei (part 1)

Elsa Kania, 27 March 2018. Originally published by [The Strategist](#).

Huawei has provoked recurrent concerns and generated nearly incessant controversy in recent news cycles.

In the US, the potential for Huawei to dominate 5G network services was the [implicit justification](#) for the recent [presidential order](#) blocking Broadcomm's attempted takeover of Qualcomm, which was seen as a risk to US national security.

Huawei's [quest for leadership](#) in 5G was also an impetus for the Trump administration's [controversial proposal](#) for a US government 'moon shot' to build secure 5G as a 'single, inherently protected, information transportation superhighway' that could serve as the 'Eisenhower national highway system for the information age'.

In Australia, [concerns about](#) Huawei's potential involvement in building 5G networks have also provoked controversy, along with strong [US resistance](#) to the idea.

To date, Huawei's rapid emergence as a global powerhouse in telecommunications has been striking. Already the world's largest telecom equipment manufacturer, as of 2017 Huawei [surpassed Apple](#) to become the world's second-largest smartphone brand.

Huawei [is believed](#) to be on track to lead the 'race' to develop and deploy 5G worldwide. Not only is it dominant in China, but it's also [pursuing partnerships](#) with telecommunications enterprises across Asia and Europe. Huawei plays an increasing role in [creating technical standards for 5G](#).

Its success has provoked a powerful backlash in the US and concerns in Australia. At times, fears about Huawei go well beyond the obvious or known indicators of risk. For instance, US Senator Chuck Grassley of Iowa [has declared](#), 'I can't pronounce their name, but it starts with an H and ends with a W-E-I. Whenever they're involved, it scares the devil out of me.' (Perhaps the activities of Huawei's rival, ZTE, would receive more attention if its name were similarly 'unpronounceable'.)

Despite and beyond a degree of hype, the concerns about Huawei that have spurred these controversies are legitimate. Huawei isn't unique in its lack of transparency regarding [likely linkages](#) to the Chinese Communist Party (CCP) and People's Liberation Army (PLA). Furthermore, Huawei merits further scrutiny insofar as it's poised to pioneer the construction of networks that promise transformative connectivity—and that could be leveraged to advance Beijing's reach and influence globally in the process.

Huawei's founder, Ren Zhengfei (任正非), [is known](#) to [have served](#) as a former director of the PLA General Staff Department's Information Engineering Academy. In this capacity, he was associated with the [former 3PLA](#), which was responsible for signals intelligence and cyber espionage.

According to Huawei officials, Ren [was a member](#) of the Chinese military's engineering corps who, after leaving the PLA, worked for a state-owned enterprise and then founded Huawei in 1987. Throughout his tenure, Ren Zhengfei himself has remained [quite secretive](#).

In addition, there also have been rumours and [reports](#) that Huawei's former chairwoman, [Sun Yafang](#), once worked with the Ministry of State Security, and later leveraged those connections to enable the company to endure financial difficulties. The lack of candour about the biographies and backgrounds of such prominent leaders within Huawei has deepened suspicions.

In addition, a [2012 investigation](#) by the US House of Representatives Permanent Select Committee on Intelligence obtained internal Huawei documentation from a former employee that reportedly demonstrated that Huawei ‘provides special network services to an entity the employee believes to be an elite cyber-warfare unit within the PLA’.

Huawei is probably still engaged in defence-related research and development. The company has [received support](#) and [participated](#) in projects to advance 5G through the 863 Program, which is linked to dual-use technological developments that often support military modernisation. Huawei also remains engaged with partners from the Chinese defence industry in initiatives that may advance China’s national strategy of military–civil fusion. For instance, in April 2017, Huawei [signed](#) a strategic cooperation agreement involving military–civil fusion communications infrastructure in Yunnan.

At the same time, Huawei has clearly emerged as a ‘national champion’. In recent years, it has received robust support from the Chinese government, which has supported and [celebrated](#) its emergence as a national flagship venture and global powerhouse. Huawei will be a [key player](#) in such iconic initiatives as the ‘[Digital Silk Road](#)’, advancing connectivity that could boost China’s competitiveness.

It can thus be difficult to differentiate Huawei’s quest for commercial advantage from China’s pursuit of strategic objectives. In the future, Huawei’s decisive market share and potential dominance globally could be exploited to advance both corporate and national government interests, at a time when the CCP is seeking to harness and leverage the dynamism of China’s tech sector.

Much ado about Huawei (part 2)

Elsa Kania, 28 March 2018. Originally published by [The Strategist](#).

While Huawei [itself](#), as well as its activities in Australia and worldwide, merit detailed scrutiny, the system and conditions within which it operates constitute a deeper source of concern. At present, the Chinese Communist Party (CCP) is openly seeking deeper ‘fusion’ between the party–state apparatus and business enterprises in ways that raise questions about the extent to which Huawei (regardless of a [reported reshuffling](#) of its board)—or indeed for any Chinese company—can operate with true independence.

Beyond the fact that Beijing’s commitment to true rule of law remains questionable, there are, in fact, new legal frameworks that could mandate that Huawei and other enterprises support Chinese intelligence activities. Consequently, the current concerns about Huawei should be only the start of closer consideration of the implications of these trends.

At a time when Huawei is actively pursuing commercial opportunities and collaborations worldwide, any deliberate introduction of vulnerabilities into its products or networks would clearly contradict its own corporate interests. However, it’s clear that Huawei’s global expansion, in and of itself, can serve as [a vector for Beijing’s influence](#).

Concurrently, the CCP’s potential ability to exploit Huawei’s reach—with or without the company’s complicity or foreknowledge—must be recognised as a risk inherent in the nature of the Chinese party–state, which has become ever more apparent under Xi Jinping.

It’s evident that the CCP is appreciably deepening its influence over China’s rising private sector. In recent years, just about every major Chinese tech company—including Baidu, Alibaba, Tencent, iFlytek, Xiaomi and Sina, [among many others](#)—has [established](#) a party branch or committee.

Huawei is not unique in this regard, and those party committees (党委) can operate without transparency regarding the extent to which the CCP may exercise influence over the company's direction and decision-making.

Huawei's own party committee has tried to keep a low profile. Notionally, its role is limited to issues of ethics and personnel. Reportedly, as of 2007, Huawei's party committee [managed](#) 56 general branches (总支), controlled 300 party branches (党支部) and had over 12,000 members.

Huawei's current Party Secretary is Zhou Daiqi (周代琪), who has [served](#) simultaneously as Chief Ethics & Compliance Officer and Director of the Corporate Committee of Ethics and Compliance. However, Zhou Daiqi often seems to represent Huawei in his official capacity as Party Secretary (党委书记) and senior vice president for [high-level talks](#) and occasions, such as the [signing](#) of a strategic cooperation agreement with a municipal government on the creation of a cloud computing data centre.

As it attempts to exercise greater control and influence over China's dynamic tech sector, the party has sought to co-opt and integrate leaders from this field. At the 'two sessions' of the National People's Congress and the Chinese People's Political Consultative Conference, delegates [included](#) Tencent's Pony Ma, Xiaomi's Lei Jun, Baidu's Robin Li, JD's Richard Liu, Qihoo's Zhou Hongyi and many more.

At the time, Sogou CEO Wang Xiaochuan declared ([translation](#) via Twitter):

We're entering an era in which we'll be fused together. It might be that there will be a request to establish a (Communist) Party committee within your company, or that you should let state investors take a stake...as a form of mixed ownership. If you think clearly about this, you can really resonate together with the state. You can receive massive support. But if it's your nature to go your own way, to think that your interests differ from what the state is advocating, then you'll probably find that things are painful, more painful than in the past.

Under these conditions—and in Xi Jinping's China—it's worth raising the question of whether any Chinese company has adequate freedom to 'go its own way,' particularly on issues that are sensitive or strategic. In the absence of true rule of law, even those companies that may wish to resist impositions by the state on their commercial interests have fewer avenues through which to do so.

Meanwhile, there's also a new legal basis that the Chinese government could use to mandate Huawei's compliance with state security interests that may be contrary to corporate imperatives. Notably, in China's National Intelligence Law (国家情报法), released in June 2017, Article 7 [declares](#):

All organizations and citizens shall, in accordance with the law, support, cooperate with, and collaborate in national intelligence work, and guard the secrecy of national intelligence work they are aware of. The state will protect individuals and organizations that support, cooperate with, and collaborate in national intelligence work.

Similarly, Article 12 highlights that national intelligence agencies may 'establish cooperative relationships with relevant individuals and organizations, and entrust them to undertake relevant work'. At the same time, the law itself is ambiguous as to the scope and bounds of what 'intelligence work' [may entail](#). Pursuant to this framework, there appears to be a direct obligation on the part of Huawei—or any other Chinese company or citizen for that matter—to assist the activities of Chinese state intelligence services.

Ultimately, the 'much ado' about Huawei is arguably justified, not so much because Huawei is Huawei but rather because of nature of the CCP and the framework for Chinese intelligence operations. In this regard, the anxieties and uncertainties about Huawei are similarly applicable to any Chinese company operating with this system, absent rule of law and without full transparency.

Going forward, the trend towards fuller fusion between the party-state apparatus and commercial enterprises—and the ways in which that fusion might be leveraged to support intelligence work—should be taken into account in [business](#) and governmental assessments of risk. These dynamics rightly provoke concern in the case of Huawei but must also be taken into account in assessing the activities of other Chinese companies operating worldwide.

The technical reasons why Huawei is too great a 5G risk

Tom Uren, 14 June 2018. Originally published by the *Australian Financial Review*.

The Chinese government has conducted aggressive and wide-ranging cyber-espionage operations for decades and their intelligence laws oblige companies to assist these efforts.

The 5G network and the NBN will together form the spinal cord of the Australian economy – high-speed low-latency networks that will enable our information and digital economy to grow. As the Australian economy increasingly relies on high-speed internet connectivity to function, these networks will become increasingly important. That means we need to have the highest levels of trust in the reliability and security of these networks.

One of the defining features of the internet and modern telecommunications systems is that they are highly complex and were not necessarily built with security in mind. This combination of complexity and lack of security means that there is a never-ending cascade of security vulnerabilities being discovered – the US National Vulnerability Database lists over 1100 for June so far – and it is impossible to be 100 per cent confident that any product is secure.

When building critical telecommunications infrastructure in this environment, security and reliability must be top of mind. Although no company makes perfectly secure products – Western telecommunications manufacturers have had their share of security vulnerabilities – Huawei presents unique additional risk beyond the “normal” risk of buying complex equipment.

Data breaches

China is thought to be behind data breaches in United States, United Kingdom and Australian government departments, including into the Bureau of Meteorology, CSIRO, and the Australian Parliament email system. But beyond what we’d call “legitimate” government espionage targets, China has engaged in the cyber-enabled theft of intellectual property, trade secrets, and commercial-in-confidence material from Western companies such as BHP, Rio Tinto, Fortescue Metals, Yahoo, Google and many more.

The US Trade Representative’s Section 301 report from March this year details the very close cooperation between the Third Department of China’s People’s Liberation Army (3PLA is a military hacking unit, also known as Unit 61398) and Chinese enterprises. The 3PLA was not only stealing commercial information on behalf of Chinese companies, it was also building secret databases to hold their corporate intelligence.

Coupled with the intent to conduct cyber-espionage, China’s intelligence law provides the capability to compel Huawei to assist with the state’s efforts. Article 7 of China’s Intelligence Law obliges organisations and citizens to support, assist and cooperate with intelligence work.

It is not hard to see how this law could be used to Australia’s detriment. The equipment that will comprise the 5G network is not just a passive piece of infrastructure. It has total visibility and control of all the connections within

the network – it sees who calls who, when, from where, and controls what route data is sent down. There are a multitude of ways this equipment could be subverted.

At one extreme, Huawei could be asked to incorporate “backdoors” into their equipment that would allow Chinese government access for either espionage or sabotage. Phone calls or messages could be intercepted and passed on in a way that blends in with normal network traffic to be difficult to detect. A mechanism to sabotage a network might not be found until it was triggered, by which time it would be too late of course.

Vulnerabilities may already exist.

This may not be the most likely possibility – it seems too overt – but given the close collaboration between 3PLA and other Chinese companies it is certainly a possibility.

A more moderate approach might simply be for Chinese intelligence to ask Huawei to provide engineering assistance and training to examine their software and hardware. It is very likely that vulnerabilities already exist in Huawei’s kit without being deliberately placed there – such weaknesses are present in all sorts of other hardware and software – and this inside information could allow Chinese intelligence to develop the capability to subvert Huawei’s equipment.

This has the great advantage that it provides Huawei with plausible deniability and they could truthfully say: “We don’t write deliberate backdoors.”

Huawei also uses deployed engineers to install and configure their equipment when building and installing a network. So at the “mild” end of the spectrum, even if corporate Huawei isn’t compelled to assist, there are still many opportunities for Chinese intelligence agencies to ask or compel their citizens to assist in undermining our 5G network’s security. This might include, for example, access codes or perhaps network configuration information, both of which could enable espionage or sabotage at a later time.

China has a proven and demonstrated intent, and their laws provide them with the capability to compel Huawei. This credible threat cannot be placed within the centre of our critical 5G network.

Huawei highlights China’s expansion dilemma: espionage or profit?

Danielle Cave, 15 June 2018. Originally published by *The Strategist*.

The Australian government [will soon](#) announce its decision on whether to allow Huawei to participate in Australia’s 5G network. It’s one of the most important policy decisions the prime minister will make this year. And it’s [complicated](#). 5G is the next generation of cellular technology. It will be faster and more responsive, and will provide us with better coverage. It will [underpin](#) our future economy and will supposedly be [up to 1,000 times faster](#) than current 4G networks.

So, it’s critical national infrastructure. Of course, a number of Australian and international companies want a piece of it—including state-owned and [state-supported](#) companies from China that loom large in the global telecommunications field. Huawei—now the largest telecommunications equipment manufacturer in the world—is the most dominant of these.

If all things were created equal, Huawei would be a competitive participant in Australia’s 5G network. But all things aren’t equal, particularly when it comes to critical infrastructure. From the Australian point of view, there are geopolitical and security issues to consider. Much of the public debate has zeroed in on cybersecurity, the potential for backdoors and the need to check Huawei’s [equipment and software](#). Those are serious concerns, but there’s an issue far bigger than Huawei itself.

Ironically, China's own laws make Huawei unsuitable to participate in Australia's 5G network. As [first detailed in *The Strategist*](#) by ICPC fellow Elsa Kania, Article 7 of China's 2017 National Intelligence Law (国家情报法) declares:

All organizations and citizens shall, in accordance with the law, support, cooperate with, and collaborate in national intelligence work, and guard the secrecy of national intelligence work they are aware of. The state will protect individuals and organizations that support, cooperate with, and collaborate in national intelligence work.

A company might have the best of intentions—work hard, foster a good reputation, make a profit—but this law undercuts those intentions by making it clear that Chinese organisations are expected to support, cooperate with and collaborate in national intelligence work. They must also keep the intelligence work they're aware of a secret. In return, the Chinese state will protect them.

How can Australia policymakers working on 5G sidestep this declaration? The law obviously could be used [to Australia's detriment](#).

The law makes things surprisingly easy for the Australian government. It provides the prime minister with uncompromising evidence that Huawei—and any other Chinese company for that matter—isn't a suitable participant in the 5G network and [other public infrastructure](#).

Of course, the timing of the announcement will be tricky. The bilateral relationship isn't in a great place, and the government's announcement will be another [major pothole](#). It will, of course, kick off a new series of *Global Times* [articles](#) and [tweets](#) criticising and threatening the government and [Australian businesses](#) (thankfully, though, there are [creative options](#) to help break this Australia–China media [feedback loop](#)).

There may be moves to double-down on the Chinese Communist Party's famed '[boycott diplomacy](#)' that seeks to coerce policy change in foreign governments by punishing private industry. Or we could see a consumer-led netizen boycott spread online—the [examples of which are endless](#)—targeting Australian products or companies. Governments and global industry should be prepared to be on the receiving end of such boycotts. They're common, and just another input that needs to be considered as part of any company's risk matrix for operating in China. We've seen versions of such boycotts targeting products in Australia ([wine](#)), Norway ([salmon](#)), Japan ([cars](#), [electronics](#), [retail](#)), the United States ([fast food chains](#)), France ([supermarkets](#)), South Korea ([supermarkets](#), [cars](#), [entertainment](#), [tourism](#)) and Taiwan ([tourism](#), [students](#)).

But the decision—particularly if the announcement references this law—will be hard to credibly refute by the Chinese government and its state-owned media. After all, the government has only itself to blame. By introducing expansive and aggressively ambitious intelligence laws, it has locked in a potentially powerful intelligence-collection system. More organisations and individuals collecting material on behalf of the state means a more diverse collection and more intelligence feeds flowing into government. That's great news for the state, particularly China's intelligence analysts and national security policymakers.

But it's a double-edged sword for China. Requiring individuals and organisations to support, cooperate with and collaborate in intelligence activities, of course, comes at a cost. And that cost will be the international expansion plans of Chinese companies—state-owned and private—which have been well and truly boxed into a corner with this law. The CCP has made it virtually impossible for Chinese companies to expand without attracting understandable and legitimate suspicion. The suspicion will be deeper in countries that invest in countering foreign interference and intelligence activities. Most developed countries, including Australia, fall into that category.

This fascinating tension—between commerce and intelligence collection—will only intensify and will eventually force some tough decisions. What’s more important to the CCP? Using Chinese companies operating overseas to collect intelligence or supporting the international success of those companies?

A little from column A and a lot from column B is probably the ideal mix for any government. But betting big and hoping for roaring global success on both fronts is a crucial mistake. The two just don’t go hand in hand. There will be a loser. And this year, at least in Australia, it will be Huawei.

Business as usual? Huawei and the Australian Parliament

Fergus Hanson and Jessica Clarence, 26 June 2018. Originally published by [The Strategist](#).

Q: How many of our politicians have you taken over [to Huawei’s Shenzhen headquarters]?

Huawei Australia chairman John Lord: I personally have taken about a dozen over the last seven years.

Q: And it’s all expenses paid?

John Lord: No, mostly with these groups, even with non-politicians [they] will get themselves to China. And it’s only with the actual Huawei bits that we cover. Obviously if you come on to our campus, which is huge, we give you lunch.

— [ABC RN interview with Huawei chairman John Lord, 4 June 2018 \(at 15:27\)](#)

[New research](#) from ASPI’s International Cyber Policy Centre shows that no company in the world has funded more trips for Australia’s federal parliamentarians than Huawei in the last eight years. Liberal politicians received most trips to China funded by Huawei, although Australian Labor Party politicians received most non–Australian government trips to China.

As the Australian government weighs a critical decision on whether to allow Huawei to participate in the 5G network, the research found that Huawei sponsored 12 trips at the federal parliamentary level over a period spanning almost eight years. While that’s not a huge number, to put it in context the next biggest corporate sponsor of trips was Fortescue Metals Group, with five trips (four to China and one to Papua New Guinea).

The other technology company sponsoring parliamentarians’ travel overseas was Microsoft, with two trips to the US. The ASPI report defined ‘corporate’ to mean companies run for profit, excluding non-government organisations, think tanks, universities, political parties, foundations, societies, and dialogues/forums.

The research looked at sponsored international travel for federal MPs. It found that the top three destinations for funded travel (flights and accommodation as well as just accommodation) were Israel, China and the United States. The top funders for each destination were, respectively, the Australia/Israel & Jewish Affairs Council (a public affairs organisation), Huawei, and the Australian American Leadership Dialogue (a private diplomatic initiative). A full breakdown of the figures can be found in the report.

That Huawei has sponsored trips is not new (see [here](#), [here](#) and [here](#)), given that the last trip declared on the registers of members’ and senators’ interests was in August 2015. But this report puts Huawei’s efforts in a broader context and shows how exceptional they have been. Globally, Huawei alone sponsored a quarter of all corporate trips over the period reviewed. And Microsoft (with two trips) was the only other company sponsoring trips to its home country.

The parliamentary registers appear to show that of the 12 flights and accommodation trips, seven were funded solely by Huawei, three were funded by Huawei and Asialink, and two were funded by Huawei and the Australia China Business Council. When contacted, Asialink stated that it paid for its staff member only and has no further information about the logistics of this trip. ACBC has not yet responded to requests for clarification.

The Huawei-sponsored trips identified in the report are [not the only Huawei-sponsored trips for parliamentarians](#) across Australia. But a lack of state and territory data for the same time period made similar analysis at this level impossible without physically accessing records held by state and territory parliaments. As the report notes, while the federal parliamentary registers of interests could be significantly and easily improved, most registers for the state and territory parliaments also need reform.

While Huawei's sponsorship of politicians' travel to China doesn't breach any rules, the number of trips it has funded raises questions about whether MPs should be able to accept any funded travel from corporations. At a minimum, it raises questions about the appropriateness of allowing politicians to accept travel paid for by companies like Huawei that are lobbying to participate in Australia's 5G network—a critical piece of national infrastructure. As Danielle Cave and Elsa Kania have noted, Huawei's participating in this network matters because it would be [obligated under Chinese law](#) to assist the work of Chinese intelligence services.

Government must protect critical infrastructure from external control

Peter Jennings, 30 June 2018. Originally published by *The Weekend Australian*.

Let's start with a simple test: who thinks it would be a good idea to hand over our next mobile communications network to a company with intimate connections to the Chinese Communist Party and the People's Liberation Army, and which is obliged under Chinese law to support Beijing's intelligence gathering activities?

Second question, who thinks it would be a smart idea to allow a Hong Kong company to dominate electricity and gas distribution in Victoria and South Australia, gas transmission and distribution in Queensland and the Northern Territory and critical gas transmission assets in Western Australia and NSW?

It says nothing positive about Canberra's approach to national security that either of these developments are regarded in some circles as serious possibilities to take over critical infrastructure essential to how we function.

On Mondays, Wednesdays and Fridays our political leaders talk a big national security game. As Malcolm Turnbull said last December, the Australian people will 'stand up' against foreign interference from China. On the other days of the week we have ministers like Steve Ciobo in Shanghai last May praising China for its 'commitment to openness' and echoing a Xi Jinping speech: 'we should bring our boats together and help each other to find a way to the other shore.'

The boats Mr Ciobo refers to are not likely to be the 12 future submarines or nine anti-submarine warfare frigates that Australia will build, primarily in response to a massive expansion of Chinese maritime power and Beijing's illegal annexation of the South China Sea, an area almost as big as the Mediterranean and vital to international trade.

Australia has a massive strategic problem on its hands. Through our own policy choices over many years we consciously built an economic dependence on China, comforting ourselves with the hope that, as China became more wealthy, it would become more open, pluralist and part of a peaceful international system following the 'rules' based order.

This hasn't happened. China under Xi has become more assertive and more aggressively nationalistic. Xi makes no secret of his ambition to supplant the United States as the dominant power in the Asia-Pacific. Domestically, Xi is cementing his personal authority by abandoning the two term limit on the presidency and vigorously 'recentralising' Communist Party influence and control over all elements of Chinese life, including so-called private businesses.

As ASPI has reported in three new studies last week, modern telecommunications technology is enabling Beijing to roll out a nation-wide population surveillance capability that makes the state in George Orwell's *1984* look like a hippy commune. Beijing's increasingly elaborate 'social credit' system will measure people's loyalty to the party like a credit rating, where low scores will cut off access to travel, jobs and promotions, stifling any unauthorised dissent.

Externally, China is squeezing Taiwan to strangle the independence instincts of a liberal democratic state of 25 million people. Beijing's coercion of international airlines, including Qantas, to erase any reference to the 'Republic of Taiwan' is one example of the Chinese Communist Party's desire for an Asia-Pacific that is expected to quietly toe the line while the Party's reach is extended to Southeast Asia, the South Pacific, African and Indian Ocean countries, backed by an increasingly powerful People's Liberation Army.

Australia's foreign policy and defence statements for years have meticulously 'welcomed China's continued economic growth', but Beijing's return to a Leninist autocracy empowered with high-end information technology and growing artificial intelligence capabilities is a complicating factor we can't afford to ignore.

This is the essential broader context for thinking about Chinese foreign direct investment into Australia, particularly of large Chinese companies – State Owned Enterprises or 'private' – into critical infrastructure.

Huawei has been a massive Chinese success story which, with the preferment and backing of Beijing, has grown to operate in 170 countries, and according to Huawei's Chairman in Australia, John Lord, providing a third of the world's population 'with their telecommunications needs.' John Lord admits that there is what he calls a 'Communist Party Branch in Huawei', but claims 'it has no say in our operations, it meets in non-working hours and looks after staff social issues [and] is run by a retired employee of the company.'

Research done for ASPI by American China expert, Elsa Kania, presents a different picture. Kania has found that Huawei's Party committee controls 300 party branches in the company with 12,000 members. Nor is it just a social club: Huawei's current Communist Party Secretary, Zhou Daiqi often represents the company at high level talks.

None of this should be surprising; it reflects how business is done in a country where the Party and the State operate as a single entity. But in communications and information technology, which is so central to the Party's apparatus for controlling the country, the Party and business are getting closer. In the words of one Chinese IT business leader, Wang Xiaochuan, 'we'll be fused together ... [if] you think that your interests differ from what the state is advocating, then you'll probably find that things are painful, more painful than in the past.'

One marker of the Communist Party's intent in controlling business is the National Intelligence Law released in June 2017 which bluntly says, 'all organisations and citizens shall, in accordance with the law, support, cooperate with and collaborate in national intelligence work.'

Would that apply to Huawei's activities in Australia? It's interesting to note a change of emphasis in John Lord's language on this issue. Giving evidence before the Parliamentary Joint Committee on Intelligence and Security in September 2012, Lord said 'We comply with Chinese laws, as we comply with Australian laws, wherever we are operating.' Speaking last week to the National Press Club last Wednesday [27 June] Lord said that the Chinese national intelligence law 'has no legitimacy outside China. We obey the laws of every country in which we operate in. In Australia we follow Australian laws.'

Read that carefully. It may be that Huawei in Australia isn't looking for Chinese intelligence services, but you can be absolutely assured that, in China, the intelligence services are looking at Huawei. As John Lord told Parliament in 2012, 'we obviously do not make the product; that comes from head office.' And what does Huawei's management do in Australia? Lord again: 'market the company ... part of that is football teams, meeting people, offering people the opportunity to go to our headquarters.'

Although Mr Lord said to Parliament 'I am a bit unsure' about who paid the costs, ASPI's research into MP's declarations of interest have found that no corporate entity has sent more Australian federal politicians on free business class trips overseas than Huawei. The aim 'is getting Huawei known.' It's very unlikely though that this will improve the companies' prospects to be allowed into bidding for the 5G mobile network. In 2011 and 2013 Australia's intelligence agencies put cases to Government to keep Huawei out of bidding into the NBN scheme on national security grounds. Both times Government accepted that advice.

In May this year the Turnbull government committed over \$130 million to provide a high-speed undersea telecommunication cable between Australia and Solomon Islands, which will also support internet connectivity to Papua New Guinea. That made it possible for Honiara to avoid a communications deal with Huawei, following 'some concerns raised with us by Australia' according to Solomon Islands Prime Minister Rick Houenipwela.

It is clear that Government and intelligence community concern about the national security risks of giving Huawei access to Australia's telecommunication's backbone have grown substantially over the last decade. On all the information that's publicly available how could it be otherwise. Hopefully we can count on a quick and carefully explained government decision excluding Huawei from 5G consideration.

Hong Kong-based infrastructure firm CKI is now developing a \$13 billion takeover bid for gas pipeline group APA, whose assets are critical to the flow of gas along Australia's east coast from Queensland down to Victoria and between Moomba and Ballera in South Australia.

CKI, along with the Chinese SOE State Grid, were blocked on national security grounds from acquisition of the Ausgrid electricity distribution and transmission network in NSW in August 2016. The government never sought to explain the reason for the decision although it has since been reported that it was connected to a critical operational aspect of the Australia-US Joint Facilities located at Pine Gap near Alice Springs.

An equally surprising decision was to approve the sale of DUET gas facilities in Western Australia to CKI, news of which tricked out of a near-empty Canberra late on a Friday in April 2017 between Easter and an ANZAC day long weekend. Apart from supplying Perth, the Dampier Bunbury Natural Gas Pipeline feeds three critical operational Defence bases in the signals intelligence facility at Geraldton, the Special Air Services Regiment Headquarters at Swanborne, and Navy Fleet Base West at Stirling.

Again the Federal Government didn't see fit to explain the basis this time for an approval of a sale to a foreign company of assets that rather convincingly look like critical national infrastructure. I understand that CKI management found the combination of these decisions to be wholly incomprehensible, as did industry observers.

What then are the prospects for CKI to receive Government approval for the take-over of the much larger stock of gas and electricity assets held by APA? I see at least two problems from a national security perspective and, although this is not my field, a competition problem.

The first problem is China. Hong Kong is trying desperately to hang on to some believable shreds of autonomy as a 'Special Administrative Region of the People's Republic of China', but it is clear that Beijing has no intention of allowing that autonomy to compromise its control of the territory and of the people and businesses that reside there.

While Hong Kong currently maintains a separate legal system to the People's Republic, and therefore the 2017 National Intelligence Law would not (formally) apply to CKI, there is no escaping the reality that President Xi intends for his will to prevail in Hong Kong. Businesses there will have to be as solicitor to the interests of the Communist Party as those on the mainland.

The national security calculation for Australia is hardly less stark for the gas and electricity sector as it is for telecommunications. Can we afford to let the bulk of that critical infrastructure be owned and run by a company that is ultimately subject to an authoritarian one party state with a massive intelligence apparatus and an equally large cyber force within the PLA looking for national vulnerabilities that might offer exploitable advantage?

Since the Ausgrid decision not to sell NSW's 'poles and wires' to State Grid or CKI, a Critical Infrastructure Centre was created by the Federal Government and a new Security of Critical Infrastructure Act passed by Parliament in 2018 showing that more attention is being paid to how Australia can protect critical infrastructure, particularly from malicious cyber interference.

It's true that one does not need to own an asset to be able to damage it through cyber manipulation, but hands-on access to the hardware and software of the industrial systems running our critical infrastructure is a clear vulnerability. The non-negotiable interaction of Chinese intelligence services with their business community remains a persistent challenge.

The non-national security problem for CKI remains what Treasurer Scott Morrison has called the 'aggregation effect' of an ever larger part of Australia's energy infrastructure being owned by a small number of mainly Chinese and Hong Kong businesses.

The Government has warned on a number of occasions that 'Australia's national critical infrastructure is more exposed than ever to sabotage, espionage and coercion.' The statement is not lightly made and we should take it seriously. As difficult as these decisions are, Canberra should move quickly to block Huawei's access to 5G and CKI's access to APA's gas and electricity business. This is the necessary price of maintaining national security interests in the face of an increasingly predatory China looking to maximise its own strategic interests at the expense of all others.

The campaign against Huawei

Greg Austin, 6 July 2018. Originally published by [The Strategist](#).

The case against Huawei's participation in bidding for the 5G network in Australia appears to be based on incomplete information, at least as far as the public record allows us to judge.

For a full picture, there are several fields of knowledge we need to understand and reconcile: espionage, computer science, information and communications technology, cyber security, business studies, foreign policy, China studies, political science, international political economy, and globalisation. But there are also political perspectives and biases. The latter issue was rather brilliantly captured in a recent [Norwegian study](#).

This study saw the Huawei challenge, the Snowden revelations about NSA, and the Volkswagen emissions-monitoring scandal as part of a common problem: assurance of supply chain components in the information age. The study concluded that 'the problem [of supply chain assurance] should therefore receive considerably more attention from the research community as well as from decision makers than is currently the case'.

The consensus of global scholarly opinion on these issues suggests that those in Australia advocating for a ban on Huawei in the 5G network—mimicking the opinion of US intelligence chiefs [expressed in February 2018](#)—have not reviewed all of the available information and perspectives. Public policy analysts in Australia should be wary of their own government when it so closely mirrors senior officials in the Trump administration on any issue of intelligence policy, for two reasons.

The first, and most worrying, is the poor record of the US intelligence community on big issues of analysis if they're highly politicised. Remember Iraqi WMD as one in a 70-year saga of great US intelligence failures. The second is that internal political disputation within the Trump administration and the US Congress on relations with China is at fever pitch.

So what does the study of espionage tell us about the campaign against Huawei?

There's no doubt that countries like China, the United States, Russia, Israel and France find it easier to implant back doors in commercially available equipment manufactured by companies domiciled in their territories. For this and a variety of other reasons, wise governments, corporations and citizens should assume that all equipment in their supply chains, regardless of the country of origin, can be compromised from a cyber security point of view. The Norwegian study found that such back doors are often very difficult to detect.

We can add to this the overwhelming evidence that vulnerabilities in Microsoft Windows have been responsible for a very large share of security breaches globally, including in Australia. As argued in [a study I co-authored with German scholar Sandro Gaycken](#) for the New York-based EastWest Institute in 2014, 'highly secure computing' (that is, non-vulnerable systems) has to be the approach.

The national security damage caused by vulnerabilities in Microsoft Windows puts into the shade the unsubstantiated claims (unsubstantiated in the public domain at least) that Huawei equipment has directly produced security breaches. Moreover, NSA cyber weapons based on the vulnerabilities in Windows, such as Eternal Blue, have caused more documented security breaches globally, and in Australia, than any Huawei products. Yet Australia's Defence Department uses Microsoft Windows.

We also need to assess the relative intelligence value of back doors in Huawei products if they in fact exist. We can assume they do, either by design or by error. But the share of high-grade intelligence collected by this means would be minuscule. Chinese and American spy agencies already have easy access to most unclassified or unencrypted telecommunications from Australia without relying on back doors in telecoms equipment.

If China wanted to use a domiciled company for implanting back doors, it would not rely on the Chinese Communist Party cell in Huawei to set that up. The Huawei party cell would not be in the chain of command for Chinese intelligence operations of this kind. The cell is not oriented towards espionage, though its members would report on internal security issues to the Ministry of Public Security.

If the US wanted to plant back doors in the equipment of a US-domiciled company, it would not need a law to compel the cooperation. It would simply get consent from people at the top of the company, as it did with NSA's PRISM program, where US telecoms companies, such as AT&T, and information utilities, such as Google, provided a direct feed to NSA headquarters of all communications, according to documents leaked by Snowden.

Beyond intelligence studies, we need industry knowledge. Huawei estimates that 50% of Australians rely on its systems of some kind for their telecommunications. This is probably a radical underestimate—I think it would be closer to 95% if we're talking about all Chinese-made systems. Most of Australia's unclassified communications today probably depend on systems using at least one component manufactured in China.

I base this very rough estimate on several considerations. According to a 2018 study on smaller countries like Australia, the bulk of our domestic internet traffic and email is probably routed through foreign servers and internet gateways. A large slice goes to countries like the UK where BT is the provider using Huawei equipment, not to mention other Chinese equipment manufacturers like ZTE. And not to mention the share of our communications traffic to and from China itself. According to a [2018 Chinese study](#), the diversion of internet traffic through other countries is increasing in spite of intensifying claims to internet sovereignty.

The campaign against Huawei imagines that Australia has a cyber border. It does not. It's deeply entangled in a globalised laissez-faire ICT economy and diffuse internet traffic pathways. Our public policy is still learning the nature and scope of this reality.

The African Union headquarters hack and Australia's 5G network

Danielle Cave, 13 July 2018. Originally published by [The Strategist](#).

Last week, [Greg Austin wrote in The Strategist](#) that 'those in Australia advocating for a ban on Huawei in the 5G network—mimicking the opinion of US intelligence chiefs expressed in February 2018—have not reviewed all of the available information and perspectives'. While I don't agree with the article's broader argument, Austin was spot-on in one area—we haven't reviewed all of the available information.

In Addis Ababa, the gleaming 20-storey [headquarters of the African Union](#) (AU) rises above the dusty skyline as a testament to the China–Ethiopia and broader China–Africa relationship. The Chinese government, which announced the project in 2006, built and financed the entire US\$200 million complex, from the attached 2,500-seat [grand conference hall](#) to the [office furniture](#). [According to the World Bank](#), around 12,000 to 15,000 officials and representatives from various entities visit the AU Commission for summits, meetings and other events each year.

In January 2012, the completed building was handed over at a [public ceremony](#). At the opening, Jia Qinglin, then-chairman of the National Committee of the Chinese People's Political Consultative Conference, delivered a speech in which [he said](#):

The international community should provide support and help to the resolution of African issues. China believes that such help should be based on respect for the will of the African people and should be constructive. It should reinforce, rather than undercut, Africa's independent efforts to solve problems. Interference in Africa's internal affairs by outside forces out of selfish motives can only complicate the efforts to resolve issues in Africa.

The AU's grand and sprawling complex was the focus of intrigue and controversy earlier this year—controversy that [sheds light on](#) reported '[national security concerns](#)' in Australia about which companies should be involved in our 5G network and other critical infrastructure projects.

In January 2018, France's *Le Monde* newspaper published an [investigation](#), based on multiple sources, which found that from January 2012 to January 2017 servers based inside the AU's headquarters in Addis Ababa were transferring data between 12 midnight and 2 am—every single night—to unknown servers more than 8,000 kilometres away hosted in Shanghai. Following the discovery of what media referred to as 'data theft', it was also [reported](#) that microphones hidden in desks and walls were detected and removed during a sweep for bugs.

The Chinese government refuted *Le Monde*'s reporting. Chinese state media outlet CGTN (formerly CCTV) [reported that](#) China's foreign ministry spokesperson called the *Le Monde* investigation 'utterly groundless and ridiculous'. China's ambassador to the AU said it was '[ridiculous and preposterous](#)'. The BBC also quoted the ambassador [as saying](#) that the investigation 'is not good for the image of the newspaper itself'.

Other media outlets, [including the Financial Times](#), confirmed the data theft in reports published after the *Le Monde* investigation. It's also been reported on by [think tanks](#) and [private consultancies](#) from around the world.

One AU official [told the Financial Times](#) that there were 'many issues with the building that are still being resolved with the Chinese. It's not just cybersecurity'.

The *Le Monde* report also said that since the discovery of the data theft, 'the AU has acquired its own servers and declined China's offer to configure them'. Other media reports [confirmed](#) that servers and equipment were replaced and that following the incident 'other enhanced security features have also been installed'.

Since the reported theft, the AU Commission has put out a variety of tenders and awarded contracts in relation to the headquarters' [information and communications technology \(ICT\) infrastructure](#), including bidding documents for [a new WiFi system](#) and a US\$85,406 contract for the 'supply, delivery and installation [of firewalls](#) for the AU Commission'.

This week an additional tender was published in relation to the [AU's data centre](#)—the same centre that is referenced in *Le Monde*'s report. The tender invited organisations to bid for the 'supply, installation, configuration, testing and implementation of next generation firewall data center for the African Union Commission' and the bidding document [explained that](#):

African Union's Data Center is a very critical asset for the African Union. The data stored and systems hosted in this data center need to be protected from any form of internal or external threats and unauthorized access.

What seems to have been entirely missed in the media coverage at the time was the name of the company that served as the key ICT provider inside the AU's headquarters.

It was Huawei.

The AU Commission [signed a contract](#) with Huawei on 4 January 2012. By the time the building hosted its first AU Summit on 29 January 2012, Huawei's ICT solution—which included computing, storage sharing, WiFi and unified resource allocation services through cloud data centres—was in play. As [explained](#) on Huawei's website:

As a top organization coordinating pan-African political, economic, and military issues, the African Union Commission (AUC) needed a robust information system to support a large number of conferences and the larger amounts of data that they entail. As most of this information is of a confidential nature, legacy PCs were proving too vulnerable to hackers, phishing, viruses, and other forms of compromise.

Huawei provided a range of services to the AU. It provided [cloud computing](#) to the AU headquarters and signed [a memorandum of understanding](#) with the AU on [ICT infrastructure development and cooperation](#). It also trained [batches](#) and [batches](#) of the AU Commission's technical ICT experts.

The main service that Huawei provided to the AU was a 'desktop cloud solution'. Huawei [described the service provision as follows](#):

The AU needed a robust solution to streamline their conference operations and protect their data from a variety of security threats. They chose Huawei's FusionCloud Desktop Solution, which offers computing, storage sharing, and resource allocation through cloud data centers.

According to Huawei's [website](#), part of [this solution](#) included providing equipment and resources to the AU's data centre:

The [Huawei] solution deployed all computing and storage resources in the AU's central data center where it seamlessly connects to the original IT system. Then, Huawei installed Wi-Fi hotspots and provided the industry's first Thin Clients (TC) customized with Wi-Fi access ... Traditional PC-based architecture exposes data to serious security risks. With Operating Systems (OS) and applications installed on individual machines, data is vulnerable to viruses and plain text transmissions are easier to steal. The FusionCloud solution moves the OS and applications to centralized servers in the AU's data center to minimize information leakage while TC security measures such as authentication and encryption further secure data.

Huawei's [desktop cloud solution](#) was central to the AU's cybersecurity and data-protection efforts. Huawei listed '[better security](#)' as one of its key benefits. Huawei [described](#) the provision of this better security as follows:

Centralized storage in the data center protects data from attack and prevents data leakage from PCs. The system further protects with terminal authentication and encrypted transmission.

But despite the installation and use of Huawei's ICT services, [reputable media outlets reported that the AU's](#) confidential data wasn't protected.

There are several possible explanations for why the AU's confidential data wasn't protected and safeguarded appropriately from security threats. Let's say that Huawei was in no way complicit in the alleged data theft. With this option placed to the side, what else is left on the table? There's the possibility of a (very lengthy) insider threat, for example. There's also cybersecurity incompetence. Or perhaps the company never discovered the alleged five-year data theft?

Could the reported theft of data have occurred from a set of servers that were outside of Huawei's purview? While that's possible, we do know that Huawei 'deployed all computing and storage resources in the AU's central data center'. *Le Monde* [described](#) the data transfer as occurring from the AU's servers—servers which were [then replaced](#).

There was also another company that had some involvement in the AU headquarters' ICT infrastructure: Chinese telecommunications company ZTE. A current bidding document [states](#): 'New Conference Center (China Building) uses ZTE and HUAWEI technologies.' There's little information, in open-source documents at least, about the services ZTE may currently or have previously provided. Nor is there information that suggests it had an overarching role in the provision of ICT services inside the headquarters. Job advertisements for telecommunications engineers inside the AU Commission [do](#) cite managing a 'ZTE integrated business exchange device (IBX)' as one of the role's major responsibilities.

So let's cycle back to the debate on whether Huawei should be allowed to participate in Australia's 5G network. Let's say you're not bothered by the fact that Huawei regularly [funds the overseas travel](#) of our politicians (which is within the law). You're also not convinced by the arguments that Huawei is too great of a [technical and cybersecurity](#) risk to our 5G network.

You've also decided to dismiss—although I don't know how—[China's 2017 National Intelligence Law](#) (and other legislation, such as the [counterespionage law](#)), which states that 'all organizations and citizens shall, in accordance with the law, support, cooperate with, and collaborate in national intelligence work, and guard the secrecy of national intelligence work they are aware of'.

Now we have a startling piece of new information to add into the mix. Despite a very public commitment to cybersecurity and the provision of secure data protection, and despite [promotional material](#) that boasts of Huawei's robust and enhanced information security services to the AU—it turns out the AU's confidential data wasn't secure at all.

This doesn't mean the company was complicit in any theft of data from the AU headquarters. But it does mean it must answer [some tough questions](#) in relation to this incident. Why? Because it's hard to see how—given Huawei's role in providing equipment and key ICT services to the AU building and specifically to the AU's data centre—the company could have remained completely unaware of the apparent theft of large amounts of data, every day, for five years.

But if in fact Huawei never discovered what appears to be one of the longest-running thefts of confidential government data that we know about, and if it remained completely unaware of this alleged theft for approximately 1,825 days in a row—what are we left with?

[A national security concern.](#)

Huawei: lessons from the United Kingdom

Tom Uren, 25 July 2018. Originally published by [The Strategist](#).

The UK government released the Huawei Cyber Security Evaluation Centre oversight board's [2018 annual report](#) on 19 July. HCSEC is a Huawei-owned facility that was created seven years ago to deal with the perceived risks of Huawei's involvement in UK critical infrastructure by evaluating the security of Huawei products used in the UK telecommunications market.

The oversight board was set up in 2014 to assess HCSEC's performance relating to UK product deployments. It comprises senior representatives from government and the UK telecommunications sector and a senior executive from Huawei.

For those worried about Huawei's involvement in Australia's 5G network, the oversight board's report does not make reassuring reading.

The central concern in the debate over Huawei's participation in Australia's 5G network is that Chinese intelligence services could compel or coerce Huawei to leverage its involvement in critical infrastructure to enable espionage.

China has certainly demonstrated an intent to conduct wide-ranging espionage in Australia. There's now a large body of evidence that China has been behind an array of data breaches, including at the [Bureau of Meteorology](#); the [departments of Defence, Prime Minister and Cabinet, and Foreign Affairs and Trade](#); and the [parliamentary email system](#). But beyond what could be described as 'legitimate' espionage targeting government agencies, there have also been thefts of intellectual property, commercial-in-confidence material and trade secrets for commercial advantage from companies such as [BHP](#), [Rio Tinto](#) and [Fortescue Metals](#).

China's intelligence services also have the *ability* to compel Huawei to assist them with their intelligence work.

Article 7 of [China's National Intelligence Law](#) says that '[a]ll organizations and citizens shall support, assist, and cooperate with state intelligence work according to law' and [Article 14](#) states that national intelligence agencies 'may request that concerned organs, organizations, and citizens provide necessary support, assistance, and cooperation'. In addition, Article 10 says that 'national intelligence work institutions are to use the necessary means, tactics, and channels to carry out intelligence efforts, domestically and abroad'.

I've previously [written](#) about *how* Huawei could be used to enable espionage, with or without Huawei corporate's complicity. Espionage doesn't necessarily require sophisticated 'backdoors'— even compelling Chinese engineers to assist could enable Chinese intelligence services to get useful access to Australia's 5G network.

This demonstrated intent combined with the power provided by legal obligations imposed by Beijing means that Chinese companies like Huawei carry additional supply-chain risk compared with companies from countries without a long history of cyberespionage and/or countries without laws that specifically compel cooperation with intelligence agencies.

On the face of it, the UK approach to mitigate this supply-chain risk with HCSEC—assessing products to reassure ourselves that they are operating as expected—seems entirely reasonable. Can't we assess products to make sure they won't be used to spy on us?

The four HCSEC oversight board annual reports ([2015](#), [2016](#), [2017](#) and [2018](#)) show that it is very difficult indeed.

On the bright side, the reports have consistently stated that 'HCSEC continues to provide unique, world-class cyber security expertise and technical assurance of sufficient scope and quality as to be appropriate for the current stage in the assurance framework around Huawei in the UK'.

HCSEC is also developing new tools and techniques to better understand security assurance in telecommunications, has found vulnerabilities that Huawei has subsequently remediated, and is actually improving Huawei's basic engineering and security processes and code quality. These efforts have resulted in a more secure Huawei product.

Despite all this, the three most recent board reports have noted that HCSEC cannot confirm that what it has been testing matches what Huawei is using in the UK: the source code HCSEC has been given (that is, the computer instructions for Huawei's equipment) doesn't correspond with what has been deployed in the UK. So, much of the security testing that HCSEC has been doing may be irrelevant to the security of products used in the UK. At this point, the oversight board 'can offer only limited assurance'.

This year's report also indicates that some security-critical third-party software used in Huawei equipment is 'not subject to sufficient control'. This is viewed as possibly a significant risk to UK telecommunications infrastructure mostly because of inconsistent product support lifetimes.

Overall, the report describes HCSEC as a high-functioning, world-class security evaluation centre. However, the board cautions that confidence in HCSEC's ability to provide 'long term technical assurance of sufficient scope and quality around Huawei in the UK' is declining due to the 'repeated discovery of critical shortfalls' in 'Huawei engineering practices and processes that will cause long term increased risk in the UK'.

Worse yet, the trend across the four oversight board reports suggests that as HCSEC has improved in capability, confidence that the security evaluation process will sufficiently mitigate risks has declined—the more HCSEC learned, the less confident they were.

There is a simple lesson for Australia from the HCSEC oversight board reports: using Huawei in our 5G network will introduce risks that we will find very difficult to mitigate.

5G futures: Why Huawei when open source may be the new black?

Michael Shoebridge, 11 August 2018. Originally published by [The Strategist](#).

So, the Australian government has a big decision to make about whether it will allow Huawei to be a provider of Australia's 5G communications network that [will power the internet of things](#) for us. The national security concerns with having the large Chinese firm take on such an important role [have been outlined well by ASPI's cyber policy team](#) and [others](#) in a series of recent *Strategist* posts.

The big question people have asked, though, is, if not Huawei, then what? Ex-head of the UK's GCHQ signals intelligence organisation [Robert Hanigan](#), for example, has said, 'The dilemma for western governments is that Chinese technology is no longer derivative or cheap, it's often world-leading. Do we cut ourselves off from this technology by banning it, or find ways of managing the risk?' It sounds like there's an inevitability to embracing the solutions of China's big tech firms, either now or sometime in the future.

But that may well be just plain wrong. Rather than asking who's the alternative supplier to Huawei, the better question might be, why would Australia go with an outdated approach to hardware and software provision at a time when new approaches might play to industry strengths and be far more durable and effective over the longer term?

Let's remember that Huawei offers an end-to-end proprietary 5G solution combining hardware and software. It uses some third-party hardware and software, but it's all built around a proprietary Huawei model. That's the attraction and that's the risk. In a carefully bureaucratically worded report, the [UK's National Cyber Security Centre](#) has [advised](#) that 'it is less confident that the NCSC and HCSEC can provide long term technical assurance of sufficient scope and quality around Huawei in the UK', adding that there are further medium-term risks associated with shifts in technology like virtualisation and edge computing architectures like 5G. That's as close to alarm bells and flashing lights as such a report can get.

Huawei's end-to-end approach is apparently what makes it so attractive as a solution and helps the company undercut competitors' pricing. But it also means that identifying vulnerabilities, providing updates, doing patches, and designing and distributing upgrades of both hardware and software are in Huawei's hands. It's the Microsoft or even IBM model that gave us personal computers and the Microsoft operating system, combined with Bell Telephone's or AT&T's approach to building telecommunications networks.

But we're now living in a world of virtualisation and software-defined hardware. The old way of acquiring and operating systems that makes customers dependent on big end-to-end proprietary solutions is not the only way. Similarly, the internet of things is a world of myriad manufacturers of sensors and devices—control systems, fridges, toasters, TVs, security cameras, machinery, servers, networks, smartphones and computers—that will connect to 5G and its successors, with no single proprietor having a dominant market share.

This means that with 5G (and the next 6, 7 and 10Gs) Huawei may have tried to corner a market that's about to be disrupted. If that sounds crazy, then it's worth thinking about some parallels that we know work. The biggest is the [Linux](#) operating system—the most famous (and probably the most successful) example of open-source software. It has succeeded in large part because the software is developed by lots of people scattered across the globe. These same people, universities and companies all fix bugs, patch vulnerabilities and improve the Linux operating system's functionality. It is robust not because it's a sealed system, but because it's an open system kept strong by open participation.

Another example from the world of cybersecurity: anti-viral software and vulnerability patching also gains a huge advantage from multiple eyes and actors spotting viruses, malware and vulnerabilities and providing fixes and patches. This type of crowd-sourcing of solutions is not novel in the software industry. And it works. At speed.

In hardware land, though—think electronics, networks and telecommunications systems—open-source design hasn't been popular. Building big end-to-end proprietary systems has required large investments from big firms that produced large profits—a bit like Big Pharma with drug development.

The hardware world and the electronics industry as a whole, though, knows its future looks like the software industry's. The move to virtualisation of hardware and rapid configuration of hardware functions through software has begun and is gathering pace in areas like networking and cloud provision. [Open-source hardware](#) is becoming real, quickly.

As DARPA's [Bill Chappell](#) said recently about open-source hardware, '[T]he parallel is to the software community. The hardware community really hasn't figured out that ethos of sharing. We're trying to pull some of that excitement and methodology into hardware design.' Chappell says that open-source hardware is finally starting to take off because of the increasing abstraction of hardware design. '[I]t gets closer to the software community's mentality.'

DARPA has been placing big bets on an open-source hardware future—its timeframes for real solutions are 2025 and 2030. The goal of its US\$1.5 billion, five-year [electronic resurgence initiative](#) is to 'change how everything is done in electronics, top to bottom'. POSH, DARPA's project on open-source hardware, for example, intends to create a Linux-based platform and ecosystem for designing and verifying open-source hardware internet protocol blocks for next-generation systems on chips.

The world of telecom and networking technology looks far more likely to shift from big single proprietary solutions to more participatory open-source solutions for both hardware and software. That's in part because it will provide the most rapidly reconfigured and most secure solutions in a world of cyber threats, but also because the internet of things is well suited to an open-source approach given the huge number of individual vendors.

This open approach plays to the strength of countries that see open participatory systems as the path to success, not closed, state-sponsored proprietary solutions. It's a model that works well when you want to combine the capabilities and strengths of diverse firms and research organisations across national boundaries. It is a great fit for Western political systems that can work as partners, combined with strong market-based policies and practices.

In this already emerging future world, companies like Qualcomm, Intel, Nvidia, IBM, Nokia, Ericsson—and firms like Australia's Telstra, Atlassian and Quintessence Labs—can combine to build open-source hardware and software solutions. These will provide far more resilient, rapidly upgradeable and configurable communications backbones than can be achieved by the historical big proprietary model. They'll have built-in cybersecurity because vulnerabilities can be identified and patched fast.

This future plays to the strengths of US, EU, UK, Japanese, Indian and Australian technologists, and to the market-driven way our tech sectors operate. Australia can help by working with its partners to provide the policies, regulation and drive to accelerate this emerging future. As DARPA's Bill Chappell has said, where governments stepping in helps is at moments like this when a larger leap is required. Oftentimes, industry isn't looking too far ahead as it has more immediate pressures and concerns.

So, the solution after having banned Huawei from 5G here in Australia is first a short-term one followed by a medium-term one. In the short term, alternatives from an alliance of existing 5G competitors to Huawei—like Qualcomm, Nokia and Ericsson—could meet the more immediate need. That will give time for the more durable open hardware solutions to arrive in the mid-2020s. It turns out there are alternatives to living in a world dominated by big proprietary tech. That's good news.

Huawei and 5G: clarity in an uncertain world

Michael Shoebridge, 24 August 2018. Originally published by [The Strategist](#).

The Turnbull government's latest [announcement](#) on how its new telecommunications sector security reforms will apply to 5G in Australia has effectively excluded Huawei (and ZTE, the other Chinese large telecoms provider) as vendors of 5G systems and services.

Or at least that's what the lengthy media release from acting Home Affairs Minister Scott Morrison and Communications Minister Mitch Fifield seems to mean.

Beijing's *Global Times* newspaper, which often channels the views of the Chinese government in a fairly strident way, had predicted that the decision would be the bilateral relationship's next test. [Reacting](#) to yesterday's decision, it's a different tune—apparently the paper's thoughts are with consumers, and it's extremely disappointed for them.

Those who welcomed Malcolm Turnbull's recent '[resetting](#)' of the [China relationship](#) had cautioned that banning Huawei would put Canberra back in the diplomatic deep-freeze. They didn't add that such frostiness hasn't stopped Chinese customers from buying our high-quality resources and services at globally competitive prices.

Intelligence agencies have clearly provided frank security advice about embedding Huawei deep in Australia's data system.

The government's media release is studious in not naming any vendors, but says:

The Government considers that the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorized access or interference.

That sounds like it applies to Huawei (and ZTE).

Huawei Australia has said there's no security problem, because Huawei in Australia will [obey Australian law](#). Inconveniently, however, [Chinese law](#) requires Huawei to comply with Chinese intelligence organisations' demands—and 5G networks and services provide compelling opportunities for those intelligence agencies. Huawei employees in Australia need not understand what's done.

Assurances in large ads carried in Australian newspapers about Huawei creating 'a better and safer ICT landscape for everyone' were welcome. According to credible international reporting, though, assurances don't seem to have stopped the African Union's data on Huawei systems from being sent without permission to [unknown servers in Shanghai every night for five years](#).

The *Global Times* reports Huawei [is considering](#) mounting a legal challenge to the government's direction on unfair competition grounds.

It might be better for Huawei not to draw more attention to Australia's decision, which appears well supported factually and in line with the government's regulatory powers.

Yesterday's decision has also recognised that 5G isn't just a new version of the 4G network. It's the central nervous system that will connect Australian people, businesses, power, electricity, water and other systems to the internet much more deeply. It will make the internet of things real.

Its design means that current controls, which depend on a clear distinction between the core (NBN) network and edge systems like WiFi and 4G, don't work in the 5G world—because the distinction between the core and the edge will disappear over time.

Most refreshingly of all, the government seems to have recognised that a combination of saying no to some systems and components but yes to others from Huawei, along with adopting the UK evaluation centre model, just wouldn't work. That was the [rumoured](#) magical compromise solution.

The ministers said the government 'has found no combination of technical security controls that sufficiently mitigate the risks'. That's good news, because the UK solution that tries to put such controls in place is [failing in plain sight](#).

The UK's Huawei Cyber Security Evaluation Centre has cybersecurity and telecommunications specialists examining various Huawei components, software and source code to assess security risks. In a bureaucratically worded [report last month](#), the centre's oversight board (which is chaired by the head of the UK's National Cyber Security Centre) said that 'the NSCS has advised ... that it is less confident that NSCS and HCSEC can provide long term technical assurance of sufficient scope and quality around Huawei in the UK'. It reports 'repeated discovery of critical shortfalls' and 'a further medium-term issue [in] the shift in architecture and technology brought about by ... edge compute architectures such as 5G'.

Australia's politicians may have taken some comfort that the US provides good company for this decision. Last week, Donald Trump signed the [John S. McCain National Defense Authorization Act](#) into law. It prohibits the US government from buying telecommunications equipment or services from China's Huawei and ZTE, and from companies doing business with them. Phase-in periods allow orderly replacement of current Huawei and ZTE systems. Not a bad approach.

So, it appears that the Turnbull government has made a decision that actually confronts the problem—compromise of Australia's 5G network to the Chinese state. And it's done so in a way that will deliver 5G benefits to Australians and Australian businesses.

The decision sets the scene for new directions in how communications systems and services are designed and provided in future years.

Not locking in a big Chinese tech company as a Big Telco end-to-end provider creates room for the emerging [open standard, open source software and hardware future](#) that is emerging across electronics more generally. That's the land of opportunity for Australian carriers, and Australian software houses, in partnership with US and EU firms. And it's the next Great Game in international communications technology.

As the Big Telco model gets disrupted by technological change, the future is likely to show that the path the government has opened up is smart economics and smart strategy at the same time.

It'd be great now to see some bipartisanship on this critical national decision. Having doubt cast on the strategic direction of the national communications sector could risk telecommunications policy becoming the new energy policy—something both sides of politics might avoid to show that our system of government can still work well.

Now for the follow-through on implementation.

Banning Huawei the right decision for Australia's security

Peter Jennings, 25 August 2018. Originally published by *The Weekend Australian*.

Amid the political chaos last week, Malcolm Turnbull's National Security Committee delivered an essential, decision to exclude Chinese telecommunication companies Huawei and ZTE from participation in the 5G network.

The *Global Times*, the English language media organ of the Chinese Communist Party, declared that this was a "stab in the back" and threatened that "those who wilfully hurt Chinese companies with an excuse of national security will meet their nemesis."

It's unlikely, though, that Chinese officials really expected their telcos to be given access to Australia's 5G network. Just as Beijing guards their own communications security, so would they expect other countries to protect the future backbone of Australia's economy and social well being.

The government's decision to exclude Huawei and ZTE from 5G came only after attempts to see if steps could be put in place to mitigate worries about Chinese cyber intrusion. But 5G technology is such that critical components can't be isolated. The 'core' of the 5G system, which will be typically housed in data centres, and 'edge' technology used to connect handsets, laptops and tablets to the core network, will be equally vulnerable to penetration by hostile intelligence services.

For all of Huawei's denials that it 'has never received any request from the Chinese government to gather information' it's clear that all Chinese companies are bound by Beijing's National Security Law of 2017 to assist intelligence agencies when so directed. Chinese companies cannot say no when the Communist Party's Ministry of State Security comes knocking at the door.

That's the meaning of the coded language in Scott Morrison's press release of last Thursday, which said that 'the Government considers that the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference.'

Beijing has not helped itself by brazenly continuing industrial-scale espionage against Australia and any other country which has intellectual property worth copying, and military, political and business secrets worth stealing.

Chinese espionage efforts directed by the signals intelligence arm of the People's Liberation Army has, in the last few years, successfully infiltrated the Federal Parliament's IT network as well as the Bureau of Meteorology. Chinese intelligence so thoroughly penetrated the Australian National University's networks that the University still can't be sure they have effectively excluded Chinese spy's from the system.

This is just the publicly known tip of a much larger Chinese intelligence gathering iceberg. Australian businesses, universities and state and federal government agencies should assume that Chinese intelligence gathers either have or will try to infiltrate their IT networks.

China's interest is not just intellectual property theft. It's also to monitor the 'chat' of their own students, to cultivate useful contacts and to look for further access into more sensitive networks.

The Chinese Communist Party's well-practiced and all-pervading domestic surveillance regime means that Chinese intelligence services have a deep interest in mining big data. You may not think that the details of your gas, electricity and phone bills will be valuable to an intelligence service, but aggregate that information across millions of users and cross reference it to yet other data sources and material of genuine intelligence use emerges.

This is the broader context for the Government's decision to exclude Huawei and ZTE from 5G, and notwithstanding the inevitable whining from China's red brigade of useful idiots in Australia, this was absolutely the right call.

It's hardly a stab in the back to China that Australia will take all steps necessary to protect its information systems from their intrusion. As 5G will be the information spine for everything from automated vehicles to modern agriculture, protecting the network is an essential part of national security.

As Scott Morrison moves into the Prime Ministerial suite one of the biggest policy challenges he faces will be to make Australia's China policy more consistent and focussed on doing what's necessary to protect Australia's national interest.

Malcolm Turnbull struggled with China. He began his time as Prime Minister with a businessman's intuition that China was simply a market and a way to make money. Three years of access to defence and security briefing made it clear to Turnbull that Beijing was a tough intelligence rival and an increasingly malign influence in Asia Pacific security.

Morrison's job must be to recognise that Australia has built an unhealthy economic dependency on China. Our national way forward must be to diversify economic ties and to limit the extent to which Chinese business is becoming so central in Australian critical infrastructure.

The rise of an assertive and increasingly authoritarian China will force Australia to make some difficult policy decisions. In the next few weeks Morrison will have to decide whether to allow a Hong Kong company, CKI, take over Australian gas and electricity giant APA.

While Treasury's Foreign Investment Review Board deludes itself with the fantasy that Chinese business is no different from any others, having the bulk of our gas and electricity assets owned by Beijing's state owned entity, State Grid, and Hong Kong's CKI exposes Australia to yet more Chinese intelligence gathering and, potentially, sabotage.

Russia used cyber means in December 2015 to damage part of Ukraine's electricity grid. China is developing similar cyber weapons. China doesn't have to own the grid to damage it by cyber means, but ownership makes it easier to access the hardware and software of the industrial control systems that run critical infrastructure.

As Beijing erodes Hong Kong's autonomy, CKI is no better placed to avoid the predations of Chinese intelligence services any more than Huawei. Morrison will need to step in to prevent the take over of APA to prevent any further Chinese control of Australia's gas and electricity infrastructure.

Huawei ban part of global move to set limits on Chinese influence

Michael Shoebridge 29 August 2018. Originally published by [The Strategist](#).

Scott Morrison took a step last week that will define him as prime minister, but it wasn't about getting party room numbers. It was his [announcement](#) as acting minister for home affairs that effectively banned two big Chinese telcos—Huawei and ZTE—from selling 5G in Australia.

This was big news for three reasons: the centrality of fast, secure 5G technology to Australians and Australian businesses; the policy message it sends to Beijing; and the direction it sets for Australia's future economic and communications partnerships. 5G communications systems are not just about curing blackspots and increasing bandwidth for Netflix and Stan. 5G will be Australia's data central nervous system, connecting businesses and families to the internet in much deeper ways than the current 4G/NBN networks. The security issue comes from the nature of 5G technology and that of the Chinese state.

Huawei is a provider of systems, components and services to Optus's, Vodafone's and TPG's 4G mobile networks, which support millions of Australians and thousands of Australian businesses. Under this model, network equipment used by telecommunications operators has been categorised by the network providers as either the 'core' or 'edge' network. Having a clear boundary between the core and the edge has allowed operators to have effective technical controls to protect the security data and functions in the core. The operators' networks then connect into the NBN. In 2012, Labor [banned Huawei](#) from supplying systems for the NBN.

Sensitive data, including confidential information of individuals and businesses, and functions such as authentication and access control, are in the physically and logically separated core network.

The design of 5G removes the distinction between the core and edge. As Morrison said last week, the new network 'would render these current protections ineffective in 5G'. He said the 'government has found no combination of technical security controls that sufficiently mitigate the risks'. He's on solid ground here. In Britain, where Huawei is a core supplier, the latest [oversight report](#) from that government's cyber watchdog said 'it is less confident that NSCS and HCSEC can provide long-term technical assurance of sufficient scope and quality around Huawei in the UK'. It identified 'a further medium-term issue [in] the shift in architecture and technology brought about by ... edge compute architectures such as 5G'. That's as close to alarm bells and flashing lights as a top-secret government agency gets in a public report.

No doubt faced with similar advice, Donald Trump just [signed a law](#) prohibiting his government from buying telecommunications equipment or services from China's Huawei and ZTE and from companies doing business with them.

So why are Huawei and ZTE different from other suppliers? As our new prime minister put it, 'The government considers that the involvement of vendors who are likely to be subject to extrajudicial direction from a foreign government that conflict with Australian law may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference.'

This looks very much like a reference to China's [National Intelligence Law](#), which requires all Chinese companies to comply with Chinese intelligence agencies' demands—and 5G networks and services provide compelling opportunities for those agencies.

Banning two big telcos tells Beijing that its drive to gain strategic and economic advantage through the next wave of internet technologies can't happen in a way that undercuts Australians' national security.

Australia's decision has been received in odd and expected ways in Beijing. The first, odd, reaction was in the Communist Party's strident mouthpiece, the *Global Times*, expressing disappointment that Australians won't get cheap Huawei services. That swiftly moved to more predictable if concerning statements, also in the *Global Times*, such as '[Canberra stabs Huawei in the back](#)' and 'those who willfully hurt Chinese companies with an excuse of national security will meet their nemesis'.

The *Global Times* claimed Huawei is 'a company that embodies China's reform and opening up'. China's leaders know this is disingenuous. Beijing's track record on 'opening up' to non-Chinese providers is of partnerships subject to deep control by Chinese authorities and technology transfer to the Chinese entities.

More interestingly, the article asked, 'Will the move cause a domino effect in Western countries?' This gets to a real concern for China's leaders about the precedent effect of the US and Australian decisions.

These fit with rising global concern about how the Chinese state is using its power. Chinese assertiveness under President Xi Jinping's One Belt, One Road China-centred infrastructure initiative has provoked unease in countries from Sri Lanka to Malaysia, and even Tonga.

Add to this the glimpses we are gaining into China's use of digital technologies through '[social credit](#)' to control its citizens and its electronically enabled surveillance and repression of millions of [Uyghurs](#).

So, Xi is right to worry if the reality of the Communist Party in action looks very different from the 'win-win' words of his 'China Dream'. This goes well beyond the Australia-China relationship.

Morrison has set a course in managing the relationship that will welcome our valuable two-way trade in resources and services, based on us selling world-class items that China needs at globally competitive prices. But he's also laid out clear markers that where our national interests differ—as they do in questions of deep access to, and potential control of, our critical infrastructure—he will put national interests first.

Refreshingly, he won't pretend that repetition of slogans such as 'win-win' and 'mutual benefit' will make everything okay, even if it's the 'correct line' that Beijing wants to hear.

The future directions for broader economic and technology policy seem clear. They align with the government's big strategic direction to work with partners to advance a 'free and open Indo-Pacific'.

This is a vision of broad economic and security partnerships, not deep dependency on single markets and partners. That drive towards economic diversification is one we'll probably hear a lot more of as the new Morrison government gets underway.

Why Australia banned Huawei from its 5G telecoms network

Tom Uren and Danielle Cave, 30 August 2018. Originally published by *The Financial Times*.

As Canberra, Australia's sleepy bush capital, was gripped by yet another political leadership crisis this month that later overthrew former Prime Minister Malcolm Turnbull, an unexpected media release was dropped on the capital's distracted media.

Amid the chaos, the government had finally taken a much-anticipated decision on the involvement of Chinese telecommunications giant Huawei in the build of Australia's next piece of critical national infrastructure, its 5G network. Informed by a national security review that had been undertaken, then acting home affairs minister — and now prime minister — Scott Morrison had banned Huawei.

The text of the announcement worked hard to avoid stating this directly. Instead, you had to carefully read between the lines. But China's state-run media agencies were quick to confirm the ban and get to work.

The nationalist tabloid Global Times published exclusive statements from Huawei that threatened legal action. Their first English-language editorial on the topic, titled "Canberra stabs Huawei in the back", stated "those who wilfully hurt Chinese companies with an excuse of national security will meet their nemesis".

The Chinese government also vocalised its frustrations in press briefings. China's Foreign Ministry urged the Australian government "to abandon ideological prejudices and provide a fair competitive environment for Chinese companies."

The Commerce Ministry responded to the ban with a statement. "Australia should look at the big picture of bilateral economic and trade co-operation, rather than easily interfere with and restrict normal business activities in the name of national security," it said.

The Australian government's closed-door review focused on the security of the telecommunications industry and the vendors supplying equipment to that industry. A key sentence in its announcement pointed to concerns over unauthorised access or interference by "vendors who are likely to be subject to extrajudicial directions from a foreign government that conflicts with Australian law".

A debate about Huawei's involvement in Australia's telecommunications industry has been simmering for a decade. Last week's ban is not the company's first in Australia. In 2012 it was excluded from Australia's National Broadband Network. Since then, [Huawei](#) has engaged in a charm offensive in the hope of swaying public and political opinion.

They've used the same template in Australia as they have elsewhere round the world, placing former politicians on their local board of directors, hiring advisers straight out of relevant political offices, sponsoring popular sports teams (including the Australian capital's rugby league team) and, most controversially, funding the travel of federal and state politicians to visit their headquarters in China.

However, it was not concerns over such moves that spelt the end for Huawei's 5G ambitions in Australia. Rather, a series of security issues weighed heavy.

These included the Communist party's tightening grip on its technology companies and the vulnerability of telecoms systems to subversion for espionage purposes.

[African Union officials this year accused](#) China of hacking its computers at the Beijing-funded \$200m headquarters building in Addis Ababa. There were no allegations made about Huawei and China's foreign ministry denied the AU hacking allegations as "baseless" and "complete nonsense".

More generally, there were concerns in Australia over allegations of Chinese government's intellectual property theft and cyber espionage. The latter was highlighted again in Australia last month after [allegations](#) that Chinese cyber actors had not just hacked into one of Australia's premier universities — the Australian National University in Canberra — but had held an ongoing presence in the university's IT systems for at least seven months.

One option under consideration by Canberra was the UK government's approach, to start a cyber security evaluation centre that would be responsible for providing Australian policymakers with an ongoing assessment of Huawei products. This option was seen as a sort of middle road compromise. Given the less-than-happy state of the Australia-China relationship, this option was seen as one that would at least avoid a backlash from Beijing.

But, there was a hitch. While it might have been a better outcome for Australian diplomacy, the UK's approach has not worked. After seven years of operation, this world class research centre has only been able to provide "limited assurance" that risks to UK national security have been sufficiently mitigated.

The UK's National Cyber Security Centre [said last month](#) that it "is less confident" it can provide "long-term technical assurance of sufficient scope and quality around Huawei in the UK" because of the "repeated discovery of critical shortfalls".

In bureaucratese, the language used by the UK government in this report was damning. Clearly informed by the experience of its five-eyes partner, the announcement read: "[The Australian] government has found no combination of technical security controls that sufficiently mitigate the risks."

However, a key impetus behind the Australian decision was a close analysis of China's 2017 national intelligence law which states: "Organisations and citizens shall, in accordance with the law, support, co-operate with, and collaborate in national intelligence work and guard the secrecy of national intelligence work they are aware of."

This law is a double-edged sword for China. Requiring individuals and organisations to engage in intelligence activities bolsters intelligence collection but with a clear cost to companies, their reputation and ongoing access to international markets.

As Australia prepares for more threatening statements from the Chinese Government and intimidating op-eds from its state controlled media, which will no doubt include accusations of "anti-China" bias and threats to retaliate against Australian industry through boycott diplomacy", it's important to note two things.

First, this decision was not taken lightly, nor was the decision political. There were several compelling and overlapping cyber and national security concerns that forced the Australian government's hand. As new Foreign Minister Marise Payne has noted, the decision was about solely protecting Australia's interests.

Second, China's 2017 National Intelligence Law is bad news for the international expansion ambitions of China's companies. When weighing up the involvement of foreign companies in critical infrastructure projects, how can policymakers put forward credible arguments in support of companies whose international behaviour is bound by their domestic security laws?

Long-term, the Chinese Communist party is going to have to make a tough call about how it sees its citizens and organisations. Which is more important — that they participate in espionage or participate in and benefit from the global economy?

As Huawei's demise in Australia has shown, you can't have your cake and eat it too.

Huawei and the ambiguity of China's intelligence and counter-espionage laws

Samantha Hoffman and Elsa Kania, 13 September 2018. Originally published by [The Strategist](#).

Since late August, Chinese telecom firm Huawei, along with another Chinese telecom, ZTE, [has been banned](#) from providing 5G equipment to Australia. The Australian government didn't directly name the companies, but [said](#) that 'the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference'.

Huawei later issued a statement, [saying that](#):

Chinese law does not grant government the authority to compel telecommunications firms to install backdoors or listening devices, or engage in any behaviour that might compromise the telecommunications equipment of other nations. A mistaken and narrow understanding of Chinese law should not serve as the basis for concerns about Huawei's business. Huawei has never been asked to engage in intelligence work on behalf of any government.

The problem is, Huawei's claim doesn't respond adequately to the evidence-based scepticism on which the Australian government based its decision. For Chinese citizens and companies alike, participation in 'intelligence work' is a legal responsibility and obligation, regardless of geographic boundaries.

This requirement is consistent across several laws on the protection of China's state security. For instance, Article 7 of the [National Intelligence Law](#) (国家情报法) declares:

Any organisation and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of [emphasis added]. The state shall protect individuals and organisations that support, cooperate with, and collaborate in national intelligence work.

Similarly, Article 22 of the 2014 [Counter-Espionage Law](#) (反间谍法) states that during the course of a counter-espionage investigation, 'relevant organisations and individuals' must 'truthfully provide' information and 'must not refuse'. The [implementing regulations](#), released in November 2017, clarified the law's provisions:

When State Security organs carry out the tasks of counter-espionage work in accordance with the law, and citizens and organisations that are obliged to provide facilities or other assistance according to the law refuse to do so, this constitutes an intention to obstruct the state security organs from carrying out the tasks of counter-espionage work according to law.

The scope and parameters of what Chinese authorities might deem to be 'intelligence work' and 'counter-espionage work' are not clearly defined in these laws—which are, at best, ambiguous and open to varying interpretations.

So, even if Huawei may be technically correct in saying that Chinese law doesn't explicitly 'compel' the installation of backdoors, there are still reasons for concern. China's intelligence and counter-espionage activities tend to be so expansive that these provisions could be used to justify activities extending well beyond China's borders.

Moreover, these recent laws only codify and formalise existing practices, and the Chinese Communist Party has often advanced a ‘rule by law’ (法治) rather than a true ‘rule of law’ (法制) approach that places its own power and interests clearly above the law. Indeed, as the Australian government pointed out, the nature of the ambiguous but tightening relationship between the Chinese party-state and the tech companies that it claims as ‘national champions’, including through its party secretaries and committees, means there’s real potential for ‘extrajudicial directions’ beyond such formal frameworks of laws in this context.

The Chinese party-state’s view of intelligence is tied to the CCP’s expansive conception of national security or, more accurately, ‘state security’ (国家安全), which [differs markedly](#) from the US and Australian approaches to their own national security challenges.

The idea that ‘[everyone is responsible](#)’ for ensuring state security is a central feature of this concept. According to China’s 2015 [State Security Law](#), ‘Citizens of the People’s Republic of China, every state organ and the armed forces, each political party, the militia, enterprises, public institutions and social organisations, all have the responsibility and obligation to maintain state security.’

The ‘responsibility’ requirement doesn’t stop where China’s geographic borders end. There is [ample evidence that the state applies its laws and policies with extraterritoriality](#), in ways that can infringe upon the sovereignty of other nations and the civil liberties of individuals entitled to those nations’ freedoms.

As Huawei’s reach and access expand around the world, the opportunities for Chinese intelligence to leverage its products and infrastructure for espionage will only increase. Given the opacity of these issues and inherent uncertainties, the ‘[case](#)’ [against Huawei](#) may not meet the strictest of evidentiary standards in a legal sense, but there are enough red flags to raise serious questions about the potential for risks that cannot be mitigated satisfactorily without greater transparency.

Beyond the core features of the CCP’s approach to intelligence, Huawei itself has been linked to data theft, allegedly for intelligence purposes. As ASPI’s Danielle Cave [has revealed](#), Huawei was the primary provider of ICT infrastructure to the African Union headquarters, which an [investigation by Le Monde](#) showed had been the victim of data theft over a five-year period.

If Huawei is given the full benefit of the doubt, its apparent involvement in this case demonstrates negligence at best. However, in light of the scope and scale of the alleged data theft, it’s difficult to imagine that the company wasn’t aware of, or perhaps even complicit in, these activities.

Is this an isolated incident, or might there be other cases in which Huawei’s networks and products have been linked to data theft and cyber espionage undertaken by Chinese intelligence agencies? That question may not have easy answers, given the opacity of these activities, but it’s worth asking—and investigating further—nonetheless.

Ultimately, what matters isn’t whether Huawei can be ‘proven’ to be ‘guilty’ or ‘innocent’, but whether it’s prudent to let a company that is constrained and influenced both by CCP priorities and by Chinese laws and extralegal mechanisms to build or operate the next generation of Australian critical infrastructure.

Some previous ICPC publications

