The US-led campaign against the use of technology from the Chinese telecom giant Huawei — the world’s largest provider of telecom technology — in the rollout of 5G mobile networks around the world is shaping up to be a major battle between Washington and Beijing over the future of emerging technologies. Asian countries are struggling not to be sucked into that geopolitical rivalry as they decide who will build their networks.

ESSAYS BY
Henry Farrell & Abraham Newman 8
Andrew Grotto 13
A view from Huawei 16
Danielle Cave 18
Sun-sook Park 24
J. Berkshire Miller 30
Ananth Krishnan 36
Huong Le Thu 40
Huawei’s ‘Trust Deficit’ Kept It Out of Australia’s 5G Network

By Danielle Cave

WHILE THE MEDIA narrative has been that the United States government has pressured its allies to “ban Huawei” from their 5G networks, that wasn’t Australia’s experience. In fact, Australia’s former Prime Minister Malcolm Turnbull, who made the decision, has gone to great lengths in the past year to explain his reasoning.

Turnbull, who was ousted by his own Liberal Party in August 2018, is also on record explaining that he encouraged US President Donald Trump to take action on Huawei.

Huawei’s exclusion from Australia’s 5G network came down to one insurmountable hurdle. At the end of the day, there wasn’t an Australian official in Canberra able to craft a ministerial brief to Australian parliamentarians that would have credibly outlined a way for Huawei to participate in this critical national infrastructure. A way forward would have had to be found to allow the Australian government to manage the full suite of risks — technical, economic, geopolitical and strategic — that come with working with the Chinese telecommunications giant.

Given Australia’s place in the world, the strategic risks were of particular importance.

NOTHING NEW IN AUSTRALIA

A debate about Huawei’s involvement in Australia’s telecommunications industry has been taking place for a decade and this is not the first time Huawei has been locked out of critical infrastructure projects in Australia.

Back in 2012, Huawei was excluded from participating in Australia’s national broadband network (NBN) following advice from Australia’s domestic intelligence agency — the Australian Security Intelligence Organisation. At the time, the office of Australia’s Attorney-General Nicola Roxon put out a statement saying that the NBN “…will become the backbone of Australia’s information infrastructure” and that the government has “a responsibility to do our utmost to protect its integrity and that of the information carried on it.”

Despite rhetoric from the then-opposition Liberal Party — the same party that oversaw Australia’s 2018 5G decision on Huawei — the 2012 ban on Huawei’s participation in the NBN remained intact once the Liberals were elected to office in 2013. New Attorney-General George Brandis, now Australia’s High Commissioner to the UK, cited advice from national security agencies and declined to alter the policy. “The decision of the previous government not to permit Huawei to tender for the NBN was made on advice from the national security agencies. That decision was supported by the then opposition after we received our own briefings from those agencies,” he said at the time.

Fast forward five years and the Australian government was forced to turn its mind to the next major telecommunications infrastructure investment. In 2018, a dynamic and in-depth public debate played out that rapidly zeroed in on Huawei’s participation in Australia’s 5G network. A “whole-of-government” effort went into advising then Prime Minister Turnbull and his cabinet on the potential policy options. The impending decision was complicated by protracted and increasingly typical tensions in the Australia-China relationship, which now characterize most relationships China has with Western states.

In August 2018, the Australian government banned “high-risk vendors,” including Huawei, from involvement in the country’s 5G networks. The government’s move was an example of policy contestability and involved input from multiple departments and agencies. It was also made by Turnbull who, having previously held financial stakes and positions in Internet companies, had a personal passion for telecommunications, cybersecurity and emerging technologies.

But beyond the NBN and now 5G, Huawei continues to do plenty of business in Australia. What is clear, however, is that the Australian government does not want to work with the company in critical national infrastructure. This position is unlikely to change.

So why has the Australian government repeatedly locked the company out of Australia’s largest and most important public investments in telecommunications and connected infrastructure? Because the risks are simply too great. Because there isn’t enough transparency surrounding Huawei’s operations. And because this combination of risk and low transparency has created a trust deficit.

AN ARM OF THE STATE?

First, let’s start with an analysis of the risks associated with a company like Huawei.

When making various decisions related to 5G — and other critical technologies — the potential for “backdoors” is only one of the risks that must be weighed. Governments also need to make assessments about the integrity and availability of the data on the network.

There are a range of risks already on the record regarding working with Huawei, from allegations of systematic intellectual property and sensitive data theft to dubious ethics that occurred on the company’s watch.

Increasingly, governments also need to ensure that they analyze, and fully understand, the laws and the political environment that govern a company’s home environment. Concerns here include the Chinese Communist Party’s tightening grip on its technology companies and the vul-
nerability of telecom systems to subversion for espionage purposes.

Crucially, a key input in Australia's decision-making process is the Chinese government's ability to exert extra-judicial direction on organizations, companies and individuals through its state security apparatus. This extra-judicial capability is clearly explained throughout a suite of Chinese laws, including Article 7 of China's National Intelligence Law (国家情报法) that states:

Any organization and citizen shall, in accordance with the law, support, provide assistance, and co-operate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of. The state shall protect individuals and organizations that support, co-operate with, and collaborate in national intelligence work.

Another law worth close analysis is China's Counter-Espionage Law (反间谍法), which states that during the course of a counter-espionage investigation, “relevant organizations and individuals” must “truthfully provide” information and “must not refuse.”

While Huawei executives have repeatedly claimed that the company would not hand over data if requested, the company really doesn't have a choice in the matter. Not only that, the company is obliged by law to “guard the secrecy of any national intelligence work that they are aware of.”

By introducing expansive and aggressively ambitious intelligence laws over the past few years, the Chinese government has built a potentially powerful and wide-ranging intelligence-collection system. But requiring individuals and organizations to support, co-operate with and collaborate in intelligence activities comes at a cost and these laws are a double-edged sword for China, and in particular for Chinese companies seeking a sustained global presence. These laws have made it virtually impossible for many 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, as do most developed countries, including Australia.

Western states, including Australia, also need to worry about public relations and perception. While this hasn't received international media attention so far, working with a company that is complicit in enabling human rights abuses in Xinjiang through its work with the region's public security apparatus opens up governments and businesses who choose to partner with Huawei to understandable criticism.

One option that Canberra considered was to follow the UK government's approach — to start a cyber security evaluation center that would be responsible for providing Australian policy-makers with an ongoing technical assessment of Huawei's products. This option was seen as a sort of middle road compromise. Given the ongoing tensions in the Australia-China relationship, this would have also been seen as acceptable in Beijing.

But while it might have been a better outcome for Australia's embassy in Beijing, the UK's approach has not been able to solve the rapidly growing basket of problems associated with working with Huawei in critical national infrastructure. After seven years of operation, the UK's National Cyber Security Centre (NCSC) has only been able to provide “limited assurance” that risks to UK national security have been sufficiently mitigated.

In 2018, the UK's security center said 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.” More damning were comments made earlier this year to Reuters by Ian Levy, the technical director of the NCSC, who said: “The chance of a vulnerabili

Incredibly, Huawei has continuously struggled to explain who exactly owns the company and how its governance structure works. This is no small matter for Western governments who have an obligation to be transparent with the publics that vote them in.

In a 2018 media release discussing the decision to bar “high-risk” vendors from the Australian 5G network, the Australian government indirectly indicated why it did not follow the UK's 5G path. “[The Australian] government has found no combination of technical security controls that sufficiently mitigate the risks,” the release said.

**OPAQUE OWNERSHIP**

Second, let's take a look at Huawei's transparency, or lack thereof — a problem that governments don't have to worry about when working with other 5G vendors such as Sweden's Ericsson and Finland's Nokia.

Incredibly, Huawei has continuously struggled to explain who exactly owns the company and how its governance structure works. This is no small matter for Western governments who have an obligation to be transparent with the publics that vote them in.

Huawei has also been unable to prove full independence from the state. One key way of assessing this independence is to investigate the Communist Party's direct links with Huawei. In June 2018, Huawei Australia's chairman, John Lord, told the National Press Club in Canberra that the idea that Huawei is ruled by the Communist Party is a “myth” and that the company has just one Party branch in China, like most other companies. “But that branch has no say in our operations,” Lord said, “It meets in non-working hours and looks after staff social issues and activities. It has nothing to do with the management of the company and is run by a retired employee of the company.”

This explanation is not correct. In 2017, it was reported in Chinese-language media that by
2007 Huawei had established more than 300 Chinese Communist Party (CCP) branches and counted 12,000 CCP members among its employees. The expectations for these party branches are quite clear. Article 32 of the CCP’s constitution outlines their responsibilities, which include encouraging everyone in the company to “consciously resist unacceptable practices and resolutely fight against all violations of party discipline or state law.”

The company has also failed to explain a data breach at the gleaming China-built and China-financed headquarters of the African Union in Addis Ababa between 2012 and 2017. Both Le Monde and the Financial Times reported in 2018 that data containing sensitive information was whisked every night to servers in Shanghai. Huawei was the key ICT provider on the headquarters project and was responsible for protecting data from security threats. Huawei CEO Ren Zhengfei has not denied that the hack took place, but told a media gathering it had nothing to do with his company. “For the breach of equipment used by the African Union, it had nothing to do with Huawei,” Ren said, according to an account on the Huawei website.

That may well be true, but wouldn’t a private company conduct an independent review to figure out how it all went so wrong for so many years?

Huawei’s work in Xinjiang is also increasingly under the spotlight, and for good reason. In June, John Suffolk, Huawei’s vice-president and global cyber security and privacy officer, was grilled in the House of Commons as British lawmakers inquired into the company’s role in providing surveillance equipment used against Uighurs. Suffolk responded that the company follows the laws under which it operates in any country. Suffolk argued that the company is merely providing equipment in Xinjiang through a “third party.” This is not true. In fact, many of Huawei’s business dealings in Xinjiang are done directly with local authorities, police and security agencies.

The announcement of one Huawei public security project in Xinjiang in 2018 even quoted Huawei director Tao Jingwen saying, “Together with the Public Security Bureau, Huawei will unlock a new era of smart policing and help build a safer, smarter society.”

Because 5G is critical national infrastructure, most governments must make sure they can trust the companies they partner with. The result of the suite of risks outlined above, combined with a troubling lack of transparency, has resulted in a crippling trust deficit for Huawei. Given the evidence available, it would have been negligent of the Australian government to allow high-risk vendors such as Huawei into Australia’s 5G network.

Excluding Huawei from its 5G network was the only reasonable option for Australian policymakers and parliamentarians.

Danielle Cave is Deputy Head of the International Cyber Policy Centre at the Australian Strategic Policy Institute.