Strategic Comments

Australia, Huawei and 5G

The world is on the cusp of rolling out early fifth-generation (5G) mobile-network technology. Compared with 4G technology, 5G will allow for a vastly increased number of devices to be connected to mobile networks and, through increased capacity and speed, will eventually enable new uses including remote surgery and driverless cars on a large scale, and later smart cities in which traffic, utilities and public services are managed through the use of huge volumes of real-time data. 5G has, however, become an area of contention between China and the United States. The latter has expressed grave concerns about the potential for espionage and sabotage.

In August 2018, Australia became the first state in the Five Eyes intelligence alliance – which also includes Canada, New Zealand, the United Kingdom and the US – to issue security guidance to its telecommunications carriers, obliging them to avoid purchasing 5G equipment or services from the Chinese firm Huawei. Australia's decision led to the immediate collapse of a multi-billion-dollar telecommunications project in Australia belonging to TPG, a US corporation, which had already invested hundreds of millions of dollars based on agreements with Huawei. The US later added all Chinese information and communications technology (ICT) corporations to the Bureau of Industry and Security's Entity List, entailing temporary bans under sanctions legislation and some bans under presidential authority. The GCSB, New Zealand's signals-intelligence (SIGINT) agency, raised concerns in 2018 about Huawei's potential involvement in the country's 5G networks, but Wellington has not yet taken a definitive position on the matter. The United Kingdom and Canada – the remaining Five Eyes allies – are also yet to make a final decision on Huawei's involvement, but have indicated a willingness to permit Chinese telecommunications companies' participation in what they deem to be non-essential parts of their 5G infrastructure. In the UK's case, the division at least partly reflects existing dependencies on Chinese telecoms, and specifically Huawei technology. The UK appears to share Canada's view that it may be desirable to have a global set of standards for 5G security that cannot be achieved if one major country or company is completely excluded.

While Australia's decision was scarcely opposed domestically, it has affected Canberra's relationship with Beijing. Although Australia's policy against Huawei is aligned with the current stance of the US, its major treaty ally, it has put Australia at odds with the UK and Canada and stands in contrast to the posture of most of its regional neighbours other than Japan and New Zealand. Canberra has not provided a detailed technical explanation in support of its decision. The extent to which the decision was the outcome of broader geopolitical concerns, as opposed to specific technical issues, therefore remains unclear. It seems unlikely that including Huawei in Australian 5G networks would substantially alter the risk Canberra currently faces from Chinese espionage, as this risk remains high regardless of the transition to 5G and the equipment's country of origin. The probability of sabotage may be slightly increased by the introduction of 5G, and its consequences potentially significantly increased. While its likelihood could be somewhat reduced through Huawei's exclusion, this approach may downplay China's reciprocal vulnerabilities, the difficulties entailed in conducting sabotage in this way and the economic cost of forgoing Huawei's technology.

Australia's decision to ban Huawei from its 5G networks unsurprisingly produced a hostile response in China. The decision was the first of its kind worldwide. Yet it followed a period of intensifying debate within Australia about China's security intent and actions, including what was widely touted as 'territorial expansionism' and covert interference in Australian domestic politics.

Chinese and foreign investment in Australia's critical infrastructure

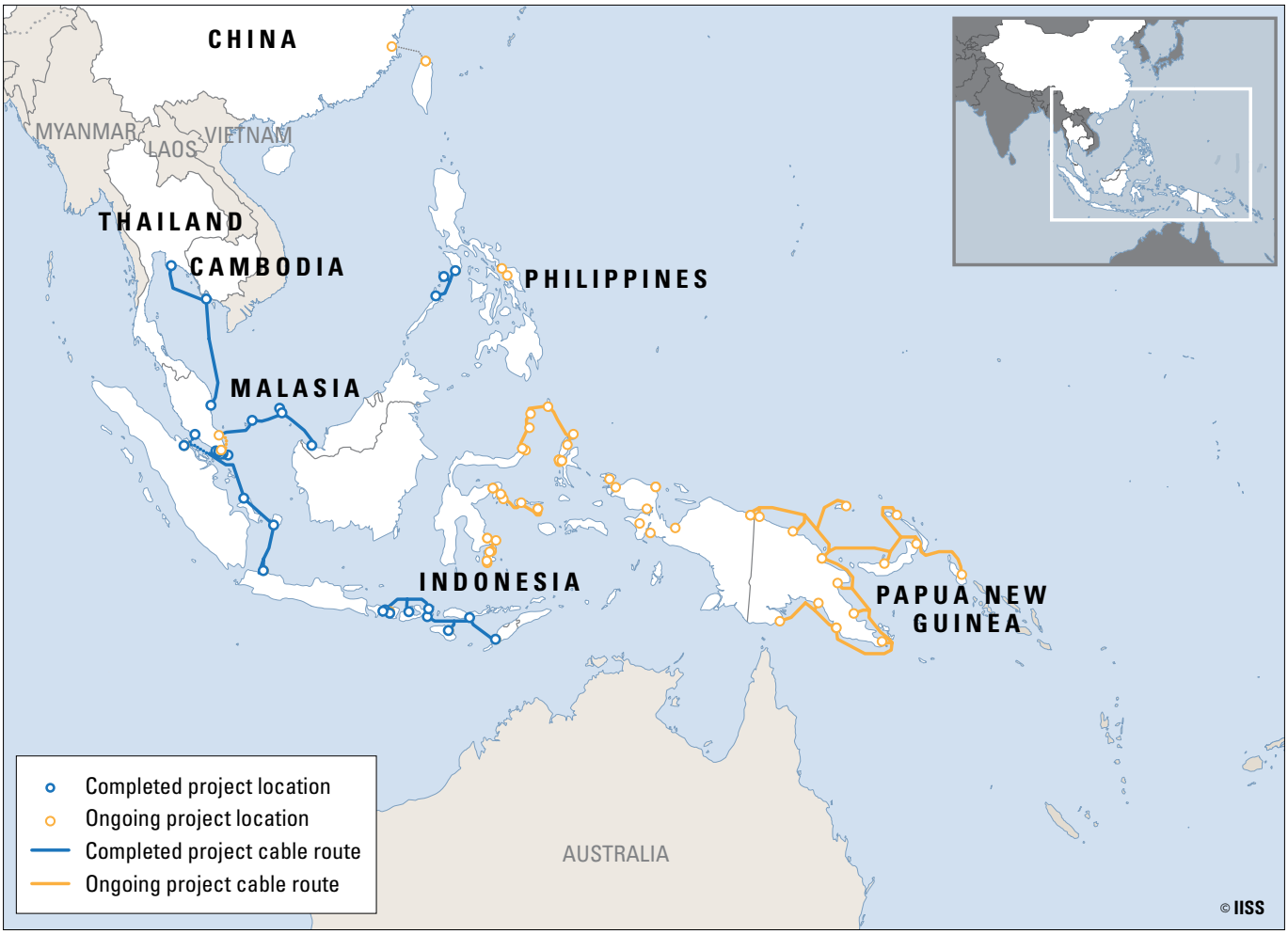
By the time that Australia made its 2018 decision about Huawei's involvement in its 5G networks, the domestic discourse about Chinese investment in Australia's critical infrastructure had already assumed an unfavourable tone. In 2012, Australia decided, on security grounds, to exclude Huawei (by name) as a bidder from formerly open tenders to supply equipment for the National Broadband Network (NBN). The Labor Party government communicated its decision directly to the company. A spokesperson for then attorney-general Nicola Roxon subsequently issued a statement saying that the decision was 'consistent with the government's practice for ensuring the security and resilience of Australia's critical infrastructure more broadly'. This was an allusion to the fear of possible sabotage in times of crisis or war.

NBN, and Australia more generally, appear to have paid a significant penalty for excluding Huawei's potentially cheaper products and services and instead, due to cost constraints, being limited to less advanced technology. By 2018, NBN had resigned itself to delivering sub-standard outcomes, with download speeds of 50 megabits per second (Mbps) from fixed lines and 25 Mbps to mobiles delivered through fibre. These speeds were at least 50% lower than the very modest goals set in 2009. In Singapore by comparison, by 2019 all broadband subscribers could access a 2 gigabits per second option, with average download speeds in January 2019 at 197.04 Mbps.

In 2016, four years after banning Huawei from NBN, the fear of Chinese involvement and the risk of sabotage in the country's critical infrastructure remained visible. In August of that year, Australia prevented a proposed takeover of Ausgrid by either State Grid Corporation of China or Hong Kong's Cheung Kong Infrastructure, which were bidding for a 50.4% share of Ausgrid's electricity network. The deliberations over this proposed deal led to a major change in the composition of the country's Foreign Investment Review Board, so as to include David Irvine, a former director-general of the Australian Security Intelligence Organisation (ASIO), and former ambassador to China, to ensure that in future, national security interests would be considered earlier.

In 2016, Huawei and the government of the Solomon Islands agreed on a joint project for Huawei to lay a submarine cable to Australia, thereby giving the Solomon Islands more reliable communications. Throughout 2017 and 2018, this project was the subject of an escalating public debate within Australia, fuelled by various government statements and leaks, over unwanted Chinese influence in the South Pacific and various high-intensity covert activities in Australia, including cyber espionage. By June 2018, Australia had persuaded the Solomon Islands to drop Huawei in favour of an Australian-funded project (with a US corporation). Australia scored a small victory in this case, but Huawei submarine cables are nonetheless taking their place in the infrastructure of Southeast Asia, including Papua New Guinea (see Figure 1).

Figure 1: **Huawei submarine cables in Southeast Asia**



Source: Huawei Marine

Canberra's claims

Australia's main official statement on Huawei's exclusion from 5G networks was a joint press release by the then-communications minister Mitch Fifield and Scott Morrison, then-acting minister for home affairs and treasurer, on 11 August 2018. Australia's primary consideration, they said, was 'the safety and security of Australians'. While they did not mention Huawei by name, they warned that 'vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law' could threaten the protection of a 5G network 'from unauthorised access or interference'. The guidance excluding Huawei relied for its legal authority on the Telecommunications and Other Legislation Amendment Act 2017, which entrenched an obligation on Australian carriers to 'do their best to protect telecommunications networks and facilities from unauthorised interference or unauthorised access'. The Act described this obligation further in two ways. The first addressed espionage concerns: protecting the 'confidentiality of communications carried on, and of information contained on, telecommunications networks or facilities'. The second addressed concerns about possible sabotage in a time of war or major political crisis: an obligation to ensure the 'availability and integrity of telecommunications networks and facilities'. The August 2018 joint statement highlighted national security considerations, including the long-term risk to 'the security of critical infrastructure' (presumably from sabotage).

The joint statement puts on an equal footing the questions of access (for espionage) or interference (for sabotage or subversion). It declared that Australia's national security agencies had been unable to find '[any] combination of technical security controls that sufficiently mitigate the risks'.

The mixed effectiveness of national equipment bans

In justifying Australia's decision, the ministers specifically dismissed technical arguments that have been raised in some quarters to justify giving Huawei some access to 5G bidding: namely, that Huawei equipment could be safely deployed to the 'periphery' (or 'edge') network and excluded from the more sensitive 'core'. They argued that, unlike with previous networks, '5G is designed so that sensitive functions currently performed in the physically and logically separated core will gradually move closer to the [periphery] of the network'. In other words, as 5G networks matured, traditional technical mitigation strategies would become obsolete.

In public, Canberra has provided no detailed technical case, based on intelligence or strategic policy considerations, that banning Huawei would reduce national security risks or the burdens of managing them. It can be credibly argued that the risks and the burdens associated with containing Chinese espionage remain essentially the same regardless of whether Huawei equipment is banned in Australia and a handful of other countries.

Arguments made against Huawei in Australia's public debate have been based largely on the risks posed by possible backdoors in hardware or possible programming of software to allow access to Chinese spies or saboteurs. This argument appears less convincing after acknowledging that Chinese spies and saboteurs, like their US and Russian counterparts, already have myriad other ways of attempting to access Australian communications content and infrastructure if they so desire. Their access does not depend on the country of origin of the equipment or the nationality of registration of the vendor corporation. The Stuxnet attack on Iran's nuclear programme was delivered through

German equipment. Chinese attacks on Australia have often been delivered through vulnerabilities in ubiquitously used commercial software (including Microsoft), as were the worldwide ransomware attacks in 2017 attributed to Russia and North Korea.

Moreover, 5G can never be just be an internal network for Australians within Australia. Many internet-based services that Australians use, including Facebook, Google and Netflix, are provided through servers in other countries. Apart from the country's telecommunications links with the US and Japan, the country's new 5G systems will be communicating with and relying upon Huawei-equipped networks in Indonesia, Singapore, China and South Korea. These connections are multiple and unavoidable. For example, China is working with the International Civil Aviation Organisation, and all of its members, to integrate 5G technologies into aircraft (using Huawei equipment) that will be connected to Australia's air-traffic-control systems once these aircraft enter Australian airspace.

Simply put, China can access most Australian communications regardless of whether its companies have the primary contract for any particular portion of the country's network equipment. Cyber espionage is best managed through good cyber-security practice, such as encryption; the risk of sabotage, however, is much harder to mitigate. The biggest technical concern for Australia was, it seems likely, the fear of Chinese control of the basic infrastructure.

5G does introduce some new risks for states. As the technology reaches maturity, more and more services and activities will depend on mobile internet connections and the provision of real-time data. These would potentially be subject to sabotage in times of war or acute strategic crisis. Nonetheless, carrying out cyber disruption (sabotaging a network, for example) in a 5G environment is not straightforward. Mobile networks in most advanced countries are part of a much larger and highly complex telecommunications infrastructure, with inbuilt redundancy and resilience. Any Chinese attempt to sabotage a complex network using Huawei equipment would risk being of limited effectiveness, or possibly failing.

It would also risk retaliation. If the country of origin of telecommunications equipment is significant from a security perspective, then it is noteworthy that US firms including Apple, Cisco, Google, IBM, Intel, Microsoft, Oracle and Qualcomm remain indispensable to China's telecommunications infrastructure and, despite multiple attempts to replace Microsoft Windows, the People's Liberation Army (PLA) is yet to develop its own operating system.

Some states, such as the UK and Canada, appear inclined to manage these risks, whereas others, such as the US and Australia, seem determined to try to eliminate them entirely. While this latter approach perhaps seems the most straightforward when considering national security factors alone, the calculation is complicated by issues of national prosperity.

The best single explanation for Australia's decision may be Canberra's long-standing concern about foreign involvement in critical infrastructure. It is also possible that Australia's intelligence agencies consider themselves so overwhelmed in trying to deal with Chinese covert activity more broadly that they have come to believe that excluding Huawei will ease that burden.

Alliance considerations

In advance of the August 2018 decision, US intelligence chiefs made several public prompts to Australia about the need to ban Huawei from its 5G networks. Ironically, Washington had not itself announced as strict a policy against Huawei that Australia was to adopt, even if segments of the public rhetoric in both countries were aligned on this matter. In fact, the US pressure was unnecessary, since Australia's conservative government was already disposed to ban Huawei from key infrastructure projects, as its Labor predecessor had done in 2012.

In May 2019, US President Donald Trump issued an executive order freezing new acquisition of Huawei equipment by US firms, but the legal position and durability of these bans was less clear than in Australia. Some US senators were so concerned that Trump might relinquish the Huawei ban as a bargaining chip in trade negotiations with China that in July 2019 they introduced a bill (the Defending America's 5G Future Act) to have the US permanently ban Huawei from 5G, unless Congress agreed otherwise. The bill has been referred to committees in both houses.

Australia's alliance considerations have been complicated by the fact that the UK and Canada appear to be reserving their final judgements on Huawei's participation in their 5G networks. Their ambivalence is due in part to a desire to wait for Washington's policy to solidify, but stems mainly from fundamental differences with the US and Australia about the feasibility and desirability of managing technological risks and about the geopolitical importance of globally inclusive standards for 5G security. It is likely that US public warnings to Five Eyes allies that they risk exclusion from intelligence sharing if Huawei participates in their 5G networks have been repeated in private. While Canada and the UK may doubt the likelihood of such a threat being enacted, given their critical roles in US mechanisms for gathering SIGINT, the potential consequences are sufficiently severe that the concern must remain a real one.

Outlook

With the exclusion of Huawei, Australia finds itself at one end of a spectrum of national policies, at least for the time being. It remains possible that Australia will eventually be considered a trendsetter among the Five Eyes allies: the US posture against Huawei could solidify, with New Zealand and then perhaps the UK and Canada following suit. For now, however, London and Ottawa appear to favour an approach to 5G security that aims to contain as many supply-chain risks as possible regardless of the country of origin of equipment, perhaps believing that the risk can be diluted by diversification.

It is also possible, therefore, that Australia could find itself somewhat exposed. Washington may yet waver in its opposition to Huawei, conceivably as part of a broader deal to resolve the US–China trade war. Moreover, credible US voices, including Microsoft and Google, have argued publicly against the current US policy trend, saying that its harmful consequences will outweigh its benefits. Australia's key trading partners and security allies in the region, including Indonesia, Singapore and South Korea, have no strong aversion to Huawei products. Japan has introduced some limitations on Huawei access to government contracts but has been less direct in its approach than Australia. China will seek to take some punitive action against Australia, while calibrating the severity of its response. It remains very unlikely, however, that Canberra will reverse its decision.

go.iiss.org/stratcom

Editor: Benjamin Rhode

For information on sales and reprints of *Strategic Comments*, as well as subscriptions, contact: T&F Customer Services, Informa UK Ltd, Sheepen Place, Colchester, Essex, CO3 3LP, UK. Tel: +44 (0) 20 7017 5544; Fax: +44 (0) 20 7017 5198; Email: subscriptions@tandf.co.uk