The Future Project
A King & Wood Mallesons Series

KING&WOOD MALLESONS
金杜律师事务所

5G Snapshot Series

Chinese Equipment Providers

29.05.20

Click to get started

KING&WOOD MALLESONS
金杜律师事务所

5G: Our connected future

THE PRIME MINISTER SCOTT MORRISON HAS HERALDED 5G AS "the next evolution of mobile technology. It promises the ability to improve the daily lives of Australians, strengthen our connectivity and accelerate our networks. 5G will change the way people use, and rely on, mobile services, driving improvements in a range of ways for businesses and communities. It will enable a new wave of innovation across our community and be used to connect other critical infrastructure, including electricity and water. 5G will underpin the development of smart cities and Internet of Things, and connect industrial control and safety of life systems, like remote surgery, and autonomous vehicles." Scott Morrison and Mitch Fifield, Joint Media Release 23 August 2018.

In our 5G "snapshot" series, we take a key component of 5G deployment and consider the state of play domestically and abroad. In the first "snapshot" of the series, we're looking at the approach to Chinese-manufactured 5G equipment.

Chinese Equipment Providers

The future – and security – of 5G networks will depend on the equipment used to build them. American security concerns about Huawei, ZTE and other Chinese tech firms are widely shared. Equally, companies and countries around the world recognise the critical importance of encouraging investment in game-changing technology. Explore how different countries are approaching the issue in this first part of an interactive 5G snapshot series from KWM.

Click to explore more

INTRO
MAP
AMER ICAS
EUROPE
UK
APAC
AUST RALIA

The regions

Back

KING&WOOD MALLESONS 金杜律师事务所

Americas

In the US, a combination of security concerns and intensifying US-China trade pressures have seen President Trump make a series of announcements directed at Chinese equipment manufacturers, and Huawei in particular.

The US Federal Government is now restricting purchases of equipment from companies such as Huawei on the basis that they pose a national security threat.

A reimbursement program has been implemented to remove and replace equipment that was manufactured by entities posing unacceptable national security risk.

US companies remain subject to a ban on using telecommunications equipment made by firms posing a national security risk, including Huawei and ZTE. The ban was extended on 14 May 2020 for a further 12 months.

In Canada, a final decision on Chinese manufacturers' involvement in 5G networks is yet to be announced, making it the only Five Eyes nation yet to take a position on the issue.

Read the details >

Europe

The EU Commission has recommended to its member states that they limit the involvement of "high-risk" 5G network equipment providers, including Huawei, but stopped short of recommending a full ban.

The EU Commission endorsed a "5G toolbox" agreed by EU member states for addressing security risks related to the rollout of 5G networks. 5G network security was described as an issue of strategic importance and critical to the EU's technological sovereignty.

Despite EU coordination efforts, national responses vary between member states.

Huawei's response to the 5G toolbox was to announce new manufacturing hubs in Europe to address security concerns, and ZTE also plans to conduct more 5G network rollouts.

Read the details >

UK

The UK Government announced in January 2020 that Chinese equipment providers may build non-essential parts of its 5G network, but in May 2020 the National Cyber Security Centre commenced a review into Huawei's equipment following additional sanctions being imposed on Huawei in the US.

Although a proposal to phase out the use of Huawei technology was defeated in the UK Parliament, the government said that it "heard loud and clear the points made on all sides of the house".

BT announced in April 2020 that it is "logistically unnecessary" to fulfil its objective to remove Huawei equipment this year and that it is likely to retain the equipment until closer to 2023.

Read the details >

APAC

In the Asia region, approaches are mixed, from proactive support for Huawei and ZTE in Malaysia, to neutrality in Singapore, and no official ban but practical exclusions in Japan.

New foreign direct investment rules in India mean that clearance will be required for all investments by Chinese companies, such as Huawei and ZTE, and such investments are likely to be restricted.

A 15% tax break was announced by the Japanese Government for mobile phone carriers and other businesses investing in 5G infrastructure to help domestic firms compete with China.

Read the details >

Australia

The Telecommunications Sector Security Reforms were implemented in 2018 to provide a framework for Australia's security agencies and industry to share sensitive information on threats to telecommunications networks.

Australia effectively banned Chinese manufacturers, most prominently Huawei and ZTE, from providing equipment to Australian telecommunications carriers.

Australia has stood by its decision to ban Huawei equipment despite the UK's decision to allow Huawei equipment in "non-core" networks.

The Australian House of Representatives Standing Committee on Communications and the Arts released its "The Next Gen Future" report on 13 May 2020 in relation to the deployment, adoption and application of 5G in Australia. Key recommendations were to increase Australia based manufacturing and reduce Australia's dependency on foreign 5G equipment, and to ensure 5G equipment vendors enforce cyber supply chain risk management processes.

Read the details >

Positions on this issue are evolving; this represents a snapshot as at 29.05.20

Americas

President Trump and the US legislature have been active in the technology and communications space recently by **taking a hard line on Chinese 5G technology**.
On 12 March 2020, President Trump signed the Secure and Trusted Communications Networks Act which prohibits the use of federal funds to purchase equipment from companies that pose a national security threat and creates a reimbursement program to remove and replace equipment that was manufactured by entities posing unacceptable national security risk. Huawei was specifically referenced when the bill was introduced.

The ban follows an executive order signed by President Trump in May 2019 declaring a national emergency and **barring US companies from using telecommunications equipment** made by firms posing a national security risk, including Huawei and ZTE, for 12 months. The order was reported to be aimed at protecting the telecommunications equipment supply chain from "foreign adversaries to the nation's information and communications technology and services supply chain". On 14 May 2020, the ban was extended for a further 12 months. President Trump said that the companies subject to the ban "pose an unusual and extraordinary threat to the national security, foreign policy, and the economy of the United States."

A bill was introduced into the US Congress on 3 April 2020 to **remove preferred investment status** for countries that allow for the installation of Huawei equipment in their 5G networks. Direct foreign investment from countries such as the UK, Australia and Canada is exempt from screening (for example, in relation to real estate and venture capital deals), but the bill proposes to end the exemption for countries that install Chinese 5G technology and it will require the US Government to report on how it coordinates with close trade and investment partners to develop alternatives to Chinese 5G technology providers.

Another bill was introduced to US Congress in January 2020 by a bipartisan group of senators that **calls for more than US $1 billion to fund the development of homegrown 5G solutions** that compete with "heavily subsidised" Chinese vendors. The bill proposes to set aside another US $500m for an international programme to encourage the adoption of trusted and secure telco equipment by foreign allies.

Huawei and 70 of its affiliates were placed on the Department of Commerce's Entity List in May 2019, which prevents US companies from purchasing Huawei equipment without US Government approval. Huawei received a 3-month temporary licence from the Department of Commerce for the sale of a certain goods in the US, solely for the purpose of allowing existing Huawei users and rural broadband networks to transition away from Huawei equipment. The US Department of Commerce has issued several extensions to Huawei's licence, most recently to 13 August 2020. However, in May 2020 the Department of Commerce announced that the "Entity List" restrictions will also be applied to additional Huawei affiliates (including Huawei India) and a new rule change will "narrowly and strategically target Huawei's acquisition" of semiconductors for any equipment using US technology, subject to a limited waiver for items already in production as of 15 May 2020.

The Department of Commerce has issued licences to several US vendors (such as Microsoft) to allow Huawei to access certain information and communications technologies or components from US manufacturers "where there is no threat to US national security". This is despite Huawei being subject to export restrictions.

In June 2019, FedEx sued the US Department of Commerce, alleging in its complaint that the requirement that FedEx must enforce export bans is unfair and has imposed **an "impossible burden" of liability** because FedEx is strictly liable for shipments that may violate the Export Administration Regulations. FedEx claims that this violates their Fifth Amendment Constitutional rights by imposing strict liability without requiring evidence of knowledge of any violation. A few days before filing, FedEx came under fire for refusing to ship a Huawei phone because of legal concerns.

Limited competition and access regulation has meant telco infrastructure investment in rural or poorer areas typically lags due to lower return on investment and smaller rural broadband providers across a limited geographic area. There are concerns that these providers will not be able to afford to replace existing equipment or build out new networks. A group of rural broadband companies have been fighting the ban since as early as 2018. Huawei launched a legal challenge against the ban claiming it to be unconstitutional, which was ultimately rejected.

Canada has indicated that **Chinese manufacturers' involvement in its 5G networks remains under review**. The Canadian Government is examining the security challenges and potential threats involved in 5G technology but has delayed announcements multiple times. It remains the only Five Eyes member not to have shared its position on whether it will use Chinese equipment.

Despite the uncertainty, Canadian operator Telus has reportedly selected Huawei as the supplier for its 5G network, but said that **it will follow any direction handed down by the government** in relation to a future ban on the technology.

Europe

The EU Commission endorsed a "5G toolbox" agreed by EU member states which sets out a range of measures and actions that – if appropriately combined and effectively implemented – form the basis for a coordinated approach to security risks related to the rollout of 5G networks. 5G network security is considered to be of strategic importance for the EU's technological sovereignty so the 5G toolbox assists member states to strengthen their security requirements, assess suppliers' risk profiles, apply restrictions to "high risk" suppliers and critical or sensitive assets, and have strategies in place to ensure diversification of vendors. The recommendations follow the completion of national risk-assessments by member states and a co-ordinated EU-wide assessment in 2019.

In relation to Chinese equipment, the Commission **recommended that member states limit the involvement of "high-risk" 5G network equipment** providers including Huawei, but stopped short of recommending a ban. Positions and attitudes vary between member states.

Huawei announced in February 2020 that it plans to **move forward with a "made in Europe" marketing image** and that it will set up manufacturing hubs in Europe to respond to the security concerns outlined in the EU's 5G toolbox. ZTE also plans to conduct more 5G network rollouts, stating that the 5G Toolbox has given suppliers the confidence to expand in its largest overseas market.

The French Government announced in November 2019 that **it will not exclude Huawei from networks but will seek to manage any security risks through heightened vetting**. It also has been reported, although not officially confirmed, that the French cybersecurity agency will approve the use of Huawei equipment but only for non-core parts of the network as they pose less significant security risks. This follows Huawei's announcement in February 2020 that it will spend more than €200 million on purchasing land and establishing a new factory in France that will specialise in 4G and 5G equipment.

In Italy, the government indicated that it has **no intention to restrict Chinese vendors**, notwithstanding a parliamentary security committee report released in December 2019 which recommended a ban claiming that alleged security concerns were "largely well-founded".

Use of Chinese 5G equipment in Germany is not yet agreed, particularly as Chancellor Angela Merkel's coalition has yet to decide a policy position in response to a proposal to shut Huawei out of the 5G rollout. However, Deutsche Telekom has said that it needs Huawei's involvement in 5G to quickly solve the problem of 5G signal coverage as other providers' equipment is not compatible with existing Huawei antennas.

The Czech Republic made **a joint declaration with the US in May 2020** which said that 5G technology suppliers should be assessed for undue foreign influence, whether they have transparent ownership, are committed to intellectual property rights or are subject to legal regimes that enforce transparent corporate practices. In 2018, the Czech Government was warned of potential risks from using Huawei and ZTE technologies, although the state has not banned the companies.

On 6 February 2020, **Vodafone announced that it would remove all Huawei equipment** from the core of its European networks following the UK's decision to restrict Huawei's role. Vodafone expects it will take five years and cost around €200 million to implement the change.

US officials have issued **repeated warnings to European allies over the dangers of allowing Huawei's participation in 5G networks**. In May 2019, US Secretary of State, Mike Pompeo, warned European leaders that the use of Chinese-made equipment in national 5G networks may result in the US withholding national security information security reasons.

A 2019 report by telecoms industry group GSMA estimated that **5G roll-out in Europe could be delayed by 18 months** and cost an extra €55 billion as a result of a ban on Chinese equipment providers, highlighting concerns over the significant loss of competition in the European market.

INTRO
MAP
AMERICAS
EUROPE
UK
APAC
AUSTRALIA

UK

The UK Government issued a press release on 28 January 2020 stating that it would **allow Chinese equipment providers to build only non-essential parts of its 5G network**. The National Cyber Security Centre (NCSC) issued guidance to UK telco operators providing that they should limit the presence of "high risk vendors" to no more than 35% of the peripheral "access network" and exclude them from "core functions" and safety-related and safety-critical networks in all critical national infrastructure, as well as from sensitive geographic locations such as nuclear sites and military bases.

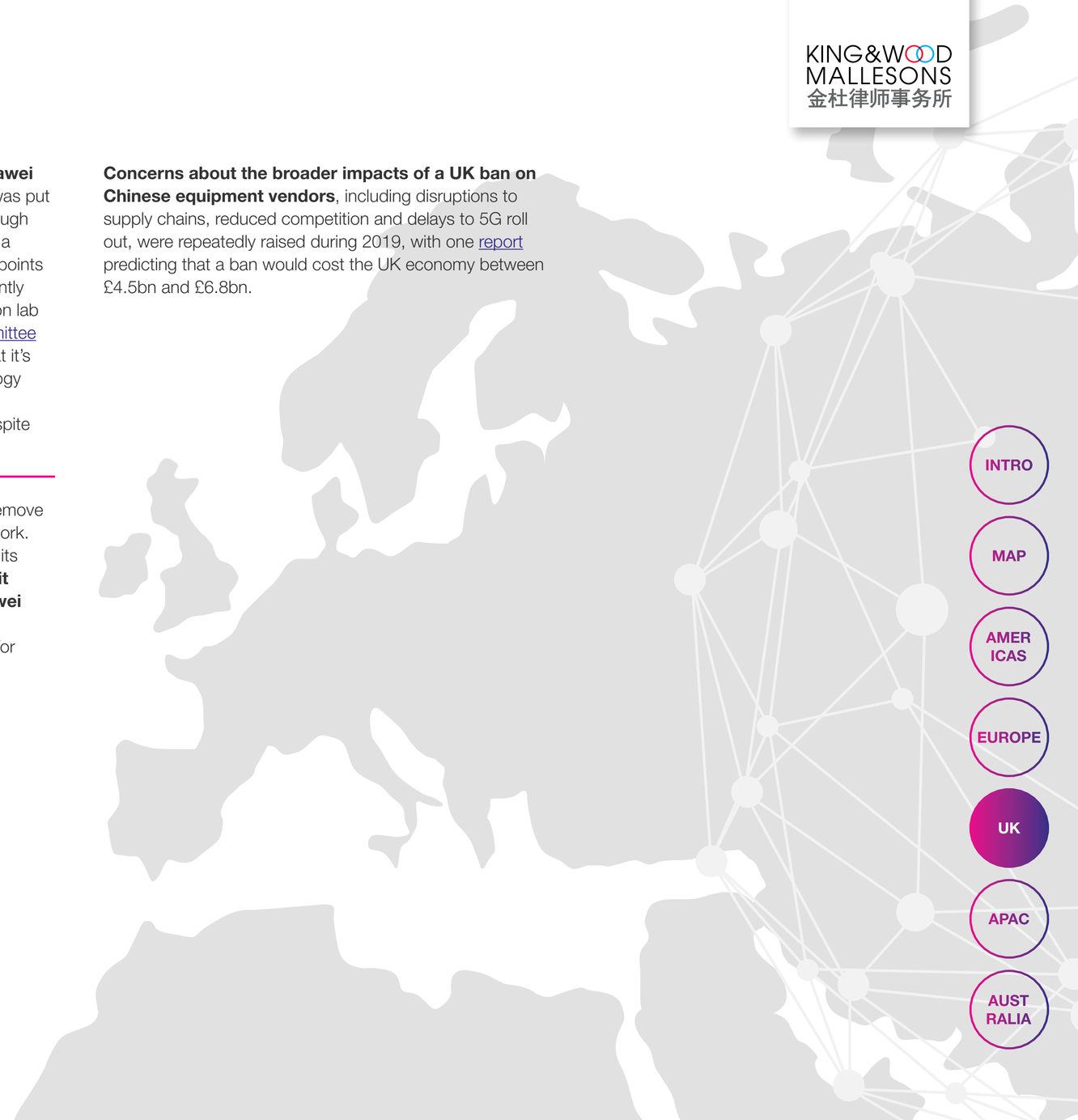
Critical in shaping the final decision was the UK Parliamentary Science and Technology Select Committee's letter which concluded that there were **no technical grounds for excluding Huawei entirely from the network**. Also significant was the Intelligence and Security Committee's statement which warned that a ban on Huawei would reduce the market to two vendors (Nokia and Ericsson), resulting in less resilience and lower security standards.

However, on 25 May 2020 the NCSC announced a new review into Huawei 5G equipment following additional sanctions being imposed on Huawei by the US Government and UK mobile operators have been instructed to phase out Huawei equipment by 2023.

This follows a proposal to **phase out the use of Huawei technology by 2022 on security grounds**, which was put to the UK Parliament voted on 10 March 2020. Although the proposal was defeated, the government released a statement indicating that it "heard loud and clear the points made on all sides of the house". However more recently in April 2020, a leader of a UK based cyber information lab spoke at the opening of the UK's Defence Sub Committee about the security of the UK's 5G network, saying that it's time to "face up" to China becoming a world technology superpower and that it would be better for the UK's economy and industries to continue with Huawei, despite the security risks it presents.

Back in 2018, BT gave itself a two-year deadline to remove Huawei's access to the core of the UK's biggest network. Despite selecting Ericsson as the operator to replace its core equipment, **BT announced in April 2020 that it is "logistically unnecessary" to remove the Huawei equipment in 2020** and that BT is likely to retain the equipment until closer to UK Government's deadline for removal of such equipment in 2023.

Concerns about the broader impacts of a UK ban on Chinese equipment vendors, including disruptions to supply chains, reduced competition and delays to 5G roll out, were repeatedly raised during 2019, with one report predicting that a ban would cost the UK economy between £4.5bn and £6.8bn.



KING&WOOD MALLESONS
金杜律师事务所

APAC

India: Huawei and other Chinese 5G vendors will be allowed to participate in India's 5G trials, suggesting that India is unpersuaded by US warnings and undeterred by historical tensions with China. However, new foreign direct investment rules introduced in response to the coronavirus pandemic mean that clearance will be required for all investments by countries that share land borders with India. The rules are likely to have an impact on Huawei and ZTE.

Malaysia: The Malaysian Communications and Multimedia Commission (MCMC) has indicated that it will continue to support Huawei and ZTE because they are affordable. In May 2019, Malaysian Prime Minister Mahathir Mohamad visited Huawei's Beijing office and said that Malaysia would use Huawei's technology 'as much as possible', as it is more advanced than American technology.

Singapore: The Singapore Infocomm Media Development Authority (IMDA) stated that "Singapore encourages vendor diversity in our telecommunication systems to mitigate risks from dependency on any one vendor" in response to questions about whether Huawei will be blocked form submitting proposals to build Singapore's 5G network.

Singapore: More recently, Singapore PM Lee Hsien Loong reiterated his government's focus on assessing operational requirements, noting that any differences in opinion on Huawei do not necessarily signal a loss of US influence in the region. Further, the Minister for Communications and Information commented in April 2020 that TPG's failed bid for a nationwide 5G spectrum licence was not related to TPG's use of Huawei equipment, stating that "our focus has not been about particular vendors, [but] on overall network resilience and security, and ensuring vendor diversity".

South Korea: Huawei has been working to promote its 5G technology, including by launching a next generation 5G wireless network lab in May 2019.

Japan: Japan was one of the first nations to exclude Huawei and ZTE from its 5G rollout, announcing in late 2018 that the Chinese vendors would be prohibited from bidding for government contracts due to security concerns. The country's largest carriers, NTT Docomo and KDDI Corp, followed by announcing that they have selected Nokia and Ericsson as 5G vendors. In December 2019, a 15% tax break was announced for mobile phone carriers and other businesses investing in 5G infrastructure to help domestic firms compete with China.

Thailand and the Philippines: These traditional US allies have ignored calls to ban Chinese equipment as alternative vendors are providing equipment which is 20% to 30% more expensive.

Vietnam: Vietnam is the only major nation in the region to counter the trend, where mobile carriers have developed native equipment to fulfil their 5G plans.

China: In a display of technological prowess, Huawei has set up three 5G stations at Mount Everest's base and transition camps (at 5,300m and 5,800m) and another two at the 6,500m advance camp. Further, Huawei announced in May 2020 that it stepped up development of 5G-connected vehicles by forming a **"5G automotive ecosystem"** alliance with 18 other companies. Huawei is pursuing "C-V2X" (cellular vehicle-to-everything) technology, which includes connected road side units, traffic lights, cameras and speed limit signs, so 5G-linked roads can support its autonomous vehicles. The Chinese government's widespread rollout of 5G and ongoing 5G innovation has reportedly contributed to making the technology a source of national pride and geopolitical might.

China: Unicom and ZTE jointly announced a cooperation agreement on 17 May 2020 in relation to research and collaboration for 6G technology, particularly in relation to technical trends and standards. The focus of the agreement includes development of 6G technologies and integration with satellite networks, IoT infrastructure, connected vehicles and other infrastructure, with a peak data rate of up to 1Tb/s.

New Zealand: The Government Communications and Security Bureau issued a decision in early 2019 to block telco provider Spark from using Huawei equipment in its 5G roll out citing concerns about national security. On 12 August 2019, Huawei reportedly threatened to pull out of the NZ market if it could not participate in Spark's 5G roll-out. Earlier in the year, the NZ Commerce Commission warned that excluding Huawei, or any supplier, could impact competition and the cost of 5G deployment.

INTRO
MAP
AMER ICAS
EUROPE
UK
APAC
AUST RALIA

Australia

SUMMARY

In September 2018, the Telecommunications Sector Security Reforms (TSSR) commenced. The TSSR provides a framework for Australia's security agencies and industry to share sensitive information on threats to telecommunications networks. The four key measures are:

1. **A security obligation** on carriers and carriage service providers to protect networks and facilities against threats to national security from unauthorised access or interference;
2. **A notification requirement** on carriers and nominated carriage service providers to tell the Australian Government of any proposed changes to their telecommunications systems or services that are likely to have a material adverse effect on their capacity to comply with their security obligation;
3. **The ability for the Australian Government to obtain** more detailed information from carriers and carriage service providers in certain circumstances to support the work of the Critical Infrastructure Centre; and
4. **The ability to intervene and issue directions** in cases where there are significant national security concerns that cannot be addressed through other means.

The TSSR followed a joint statement on 23 August 2018 from the Departments of Home Affairs and Communications explaining that 5G equipment vendors that are **"subject to extrajudicial directions from a foreign government that conflict with Australian law"** may risk failure to adequately protect a 5G network from unauthorised access. The announcement effectively banned Huawei and ZTE from providing 5G equipment to Australian telecommunications carriers.

Despite the ban, **Huawei has continued to lobby for its involvement in the 5G rollout**. However, Huawei Australia dissolved its board in March 2020 and axed 500 jobs as the ban impacted its business in Australia as well as prospects of growth. Huawei Australia reported a 78% decline in 2019 profit after tax compared to the 2018 year, a figure it attributes to the Australian Government's effective ban on use of Huawei and ZTE's 5G equipment.

The Australian House of Representatives Standing Committee on Communications and the Arts released its report "The Next Gen Future" on 13 May 2020 following an inquiry into the deployment, adoption and application of 5G in Australia. **Key recommendations** included:

- investigate ways to encourage manufacturing of 5G infrastructure within Australia and as part of manufacturing partnerships with other "Five Eyes" nations (Canada, New Zealand, the UK and the US);
- establish a 5G "R&D Innovation Fund" to fast track the development and scale-up of alternative manufacturing approaches to reduce dependency on foreign 5G equipment; and
- conduct a review of current legislative arrangements enforcing network and data security for the supply of 5G equipment so that it is incumbent on vendors to enforce cyber supply chain risk management throughout procurement, roll out and maintenance of the Australian 5G network.

In April 2019, China raised the issue of restrictions on Chinese equipment providers as an agenda item before the WTO Council for Trade in Goods, claiming the ban constituted a **"discriminatory market access prohibition on 5G equipment"**. Vodafone Australia's recent decision to replace 4G radio infrastructure supplied by Huawei wherever it was co-located with 5G infrastructure has further contributed to China's support for claims that that Australia's 5G "ban" on ZTE and Huawei has extended by stealth to cover 4G, meaning that a formal dispute at the WTO may be on the horizon.

The effective ban on Huawei from participating in 5G networks is not Australia's first ban on the company – it was barred from the National Broadband Network from as early as 2012.

Huawei is the third-largest supplier of mobile phones in Australia, behind Samsung and Apple.

Major equipment providers for 5G technology include Cisco, Ericsson, Nokia, Samsung and Chinese companies Huawei and ZTE.

Click to see more insights

INTRO
MAP
AMER ICAS
EUROPE
UK
APAC
AUST RALIA

Australia

INSIGHTS

The Australian Government has said the decision to restrict the use of Chinese equipment in national 5G networks involves **a careful balancing of constantly evolving technical, political, economic and social considerations**. In the Australian context, the Government's approach appears to give greater weight to concerns of national security and the need to maintain strategic political and security ties against the backdrop of growing geopolitical tension. Australia has adopted this position notwithstanding claims of cost and delay impacts for 5G deployment.

Example: TPG, as part of its successful appeal against the ACCC's decision to oppose the merger between Vodafone and TPG, indicated it will not be able to viably roll out a 5G network without Vodafone's input and Huawei's equipment – Huawei being the only vendor which had indicated it could meet TPG's rollout timeframe.

If the cost impact of a Chinese equipment ban is **a reluctance to roll out future mobile networks** in rural and regional areas, this could undermine the efforts the Australian Government has been making to close the "digital divide".

Australia has not banned Huawei handsets but the US ban could discourage investment in new applications and software for Huawei handsets. These impacts may be felt even if the ban is lifted, as Huawei may still suffer reputational damage. This could affect competition and development in the Australian handset market, particularly for 5G enabled handsets.

Uncertainty about use of Chinese manufactured equipment may **represent an opportunity for manufacturers in other jurisdictions.** However, the growing uncertainty in the face of an increasingly hostile international trade environment, and the supply chain impacts of the coronavirus, may see those suppliers seek to source inputs domestically and limit exposure to foreign markets to minimise the risk of supply chain disruption. The increasing nationalisation of supply chains for the production of telecommunications equipment, devices and information-based technologies may result in increased costs, and extended lead times, the effects of which may be passed on to Australian businesses and consumers, although increased domestic manufacturing may bring other economic benefits to the country.

We may experience an increasing drive towards support for non-Chinese supply chains for the production of telecommunications equipment, devices and technology, to limit exposure to security risks.

COVID-19 **pressure on supply chains** may heighten the drive to nationalise strategic manufacturing to reduce Australia's reliance on foreign markets and future supply chain disruption.

An increasingly domestic supply chain may result in increased costs and extended lead times, the effects of which would likely be felt by Australian businesses and consumers.

Back

KING&WOOD MALLESONS 金杜律师事务所

INTRO
MAP
AMERICAS
EUROPE
UK
APAC
AUSTRALIA

Click for contact details

KING&WOOD MALLESONS
金杜律师事务所

Who to contact if you're interested to learn more:

Kate Creighton-Selvay
Partner, Melbourne
T +61 3 9643 4071
M +61 405 993 122
kate.creighton-selvay@au.kwm.com

Rachael Lewis
Partner, Canberra
T +61 2 6217 6074
M +61 448 056 645
rachael.lewis@au.kwm.com

Cheng Lim
Partner, Melbourne
T +61 3 9643 4193
M +61 419 357 172
cheng.lim@au.kwm.com

Renae Lattey
Partner, Melbourne
T +61 3 9643 4065
M +61 417 214 795
renae.lattey@au.kwm.com

Michael Swinson
Partner, Melbourne
T +61 3 9643 4266
M +61 488 040 000

michael.swinson@au.kwm.com

Contributors:

- **James McGrath**
- **Tom Dysart**
- **Capucine Hague**