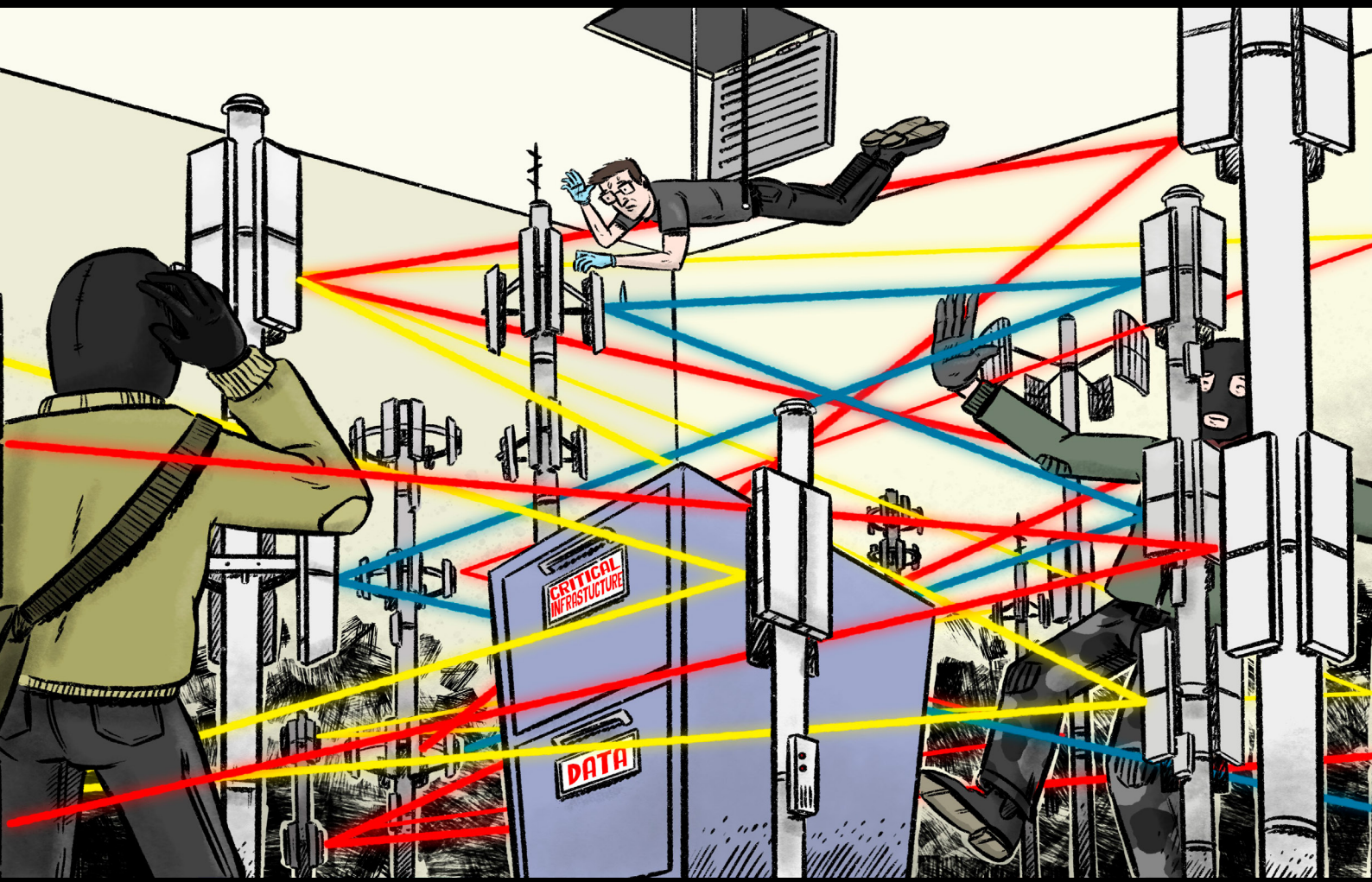
Ensuring a trusted 5G ecosystem of vendors and technology

Rajiv Shah



ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE

Policy Brief
Report No. 30/2020

About the author

Rajiv Shah is a Fellow at ASPI's International Cyber Policy Centre. He has worked in the cyber, intelligence and security business for more than 20 years, over which time he has seen the internet evolve from an academic curiosity to today's hyperconnected world. He has held a broad range of senior leadership roles with major multinational companies and now also leads his own consulting business, MDR Security, providing expert advisory services to government and businesses to grow capacity and capability through building effective and mutually beneficial partnerships. He is also a regular speaker at industry conferences and contributor to industry publications.

Rajiv's experience has spanned a broad range of business and technical domains, with roles that have included business analysis, technical architecture, program delivery, operational management, strategy, business transformation, client relationship management and more. He has spent time working in the UK and the US, and since 2011 has been based in Canberra, Australia.

Before joining the commercial world, Rajiv completed a PhD in quantum physics and retains a keen interest in mathematics and science.

Acknowledgements

The author thanks those government and industry stakeholders who made themselves available for discussions and openly shared their thoughts and perspectives, and ASPI colleagues who provided constructive comments on this report. The author also thanks all anonymous peer reviewers for their feedback. No specific sponsorship was received to fund production of this report. The work of ICPC would not be possible without the financial support of our partners and sponsors across governments, industry and civil society.

What is ASPI?

The Australian Strategic Policy Institute 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's sources of funding are identified in our Annual Report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements.

ASPI International Cyber Policy Centre

ASPI's International Cyber Policy Centre (ICPC) is a leading voice in global debates on cyber, emerging and critical technologies, issues related to information and foreign interference and focuses on the impact these issues have on broader strategic policy. The centre has a growing mixture of expertise and skills with teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building, satellite analysis, surveillance and China-related issues.

The ICPC informs public debate in the Indo-Pacific region and supports public policy development by producing original, empirical, data-driven research. The ICPC enriches regional debates by collaborating with research institutes from around the world and by bringing leading global experts to Australia, including through fellowships. To develop capability in Australia and across the Indo-Pacific region, the ICPC has a capacity building team that conducts workshops, training programs and large-scale exercises for the public and private sectors.

We would like to thank all of those who support and contribute to the ICPC with their time, intellect and passion for the topics we work on. If you would like to support the work of the centre please contact: icpc@aspi.org.au

Important disclaimer

ASPI

Tel +61 2 6270 5100
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC

First published September 2020. ISSN 2209-9689 (online), ISSN 2209-9670 (print)

Cover image: Illustration by Wes Mountain. ASPI ICPC and Wes Mountain allow this image to be republished under the Creative Commons License Attribution-Share Alike. Users of the image should use the following sentence for image attribution: 'Illustration by Wes Mountain, commissioned by the Australian Strategic Policy Institute's International Cyber Policy Centre.'

No specific sponsorship was received to fund production of this report

Ensuring a trusted 5G ecosystem of vendors and technology

Rajiv Shah

Policy Brief
Report No. 30/2020

Contents

What's the problem?

5G will be the next generation of mobile telecommunications. There are differing views on how quickly it will become commonplace and exactly what form it will take, but it will ultimately transform much of what we do and how society functions. The trustworthiness, security and resilience of 5G networks will therefore be critical. A key part of this will be the partnerships that network operators form with vendors to provide and maintain the network infrastructure. There's now a good understanding that 5G will underpin critical national infrastructure in a way that previous telecommunication technologies don't, and that supply-chain trust and security are key national security issues. Australia and some other countries have eliminated specific vendors from their 5G supply chains, but the space is globally contested and there is no consensus on what happens next. There is a need for a trusted ecosystem of vendors, which may also bring enormous opportunities for states, including Australia, to develop sovereign 5G capabilities and grow their 5G market. However, barriers to entry and a lack of consensus among key 5G stakeholders across the public and private sectors are holding up progress towards these goals.

What's the solution?

It's time to move on from debates about individual vendors to understand what a trusted ecosystem of 5G vendors and technology should consist of, what needs to be done to achieve that outcome and how we still manage the residual risks associated with vendors. Rather than looking at the trustworthiness of individual vendors as a binary yes/no decision at a particular point in time, policymakers and industry need to understand the spectrum of vendor risk and put in place measures to manage different levels of risk. The highest risk vendors can be excluded, but residual risks need to be understood and mitigated. The costs of insecure systems must be recognised and better explained. Governments need to work together to build an environment that promotes a resilient supply chain with a plurality of trusted suppliers to avoid the risk of operators putting all their eggs in one basket. If the security of one vendor is compromised, that shouldn't compromise the whole network or all the networks. This will require initiatives to promote diversity and interoperability, including standards setting, testing and integration facilities, and regulation. If implemented correctly, this will not only improve cybersecurity but also provide an economic opportunity for industry. States need to find the most promising opportunities to develop key sovereign 5G capabilities, including in Australia, and take that same approach to other key enabling technologies in order to avoid similar supply-chain security challenges in the future. The window of opportunity is open now, so we need to lead by taking action now and encouraging other like-minded countries to follow and coordinate with us.

Introduction

5G is a subject that seems to come up in almost every discussion about the future of technology. Numerous networks are already advertising 5G services, on the basis that they deploy new, more efficient 5G radios at the edge of the network. However, the real transformation, in which the major security implications arise, of a merged 'core' and 'edge' operating inside a cloud environment is yet to arrive. While there may be debates about how quickly the full 5G transformation will happen and what form it will take, there's no doubt that it has the potential to transform much of what we do. As this technology becomes an integral part of our lives, the trustworthiness, security and resilience of 5G networks will become ever more critical. A key part of this is the suppliers who will build and maintain the network equipment, and this has led to numerous discussions about the trustworthiness of particular vendors and to some countries, including Australia, banning Chinese vendors such as Huawei and ZTE from their 5G network builds.

This paper aims to broaden the global discussion. Given that all 5G network operators will need to rely on vendor partnerships to build and operate their networks, what are the desired characteristics of the vendor ecosystem that supports operators and what practical policy options should be considered to help achieve that?

This paper is based on a review of existing global literature and interviews with key stakeholders from vendors, network operators and governments in Australia and overseas. The views of these stakeholders – across the public and private sectors – differed considerably in a range of areas. This, in itself, is a part of the problem– there is often not agreed consensus on key topics and therefore the right pathway forward.

This report begins with a review of what 5G is, the current state of technology and rollouts, and the implications and considerations for the cybersecurity of 5G networks, and then looks at the current vendor environment, market opportunities and barriers to entry and diversity, leading to recommendations for the way forward.

What is 5G?

New generations of mobile technology come along about every 10 years, driven by increasing volumes of data, increased variety of data and the rapid velocity of change in types of data usage. The 5th generation, or 5G, the latest one, is starting to be implemented now and will ultimately replace the 4G networks that began to appear in 2010. However, existing technologies will probably still be with us alongside 5G for many years to come. Change between each mobile generation is not always a step change, and there have been incremental updates between generations. In fact, the first mobile data devices, including the first iPhone, used a technology called GPRS, which was sometimes referred to as '2.5G'.

The internationally accepted technical standards are set by an organisation known as the 3rd Generation Partnership Project (3GPP[1]). As the name implies, this was originally for 3G mobile networks, but it's taken the lead for 4G and 5G without an update of its name.

It's generally accepted that true 5G networks require the implementation of at least R15 of the 3GPP standard.[2] In simple terms, there are three key components of 'real' 5G:

1. **Faster mobile broadband speeds:** This is generally the most common public perception of 5G—how many gigabits of speed can be provided to a mobile handset and hence how quickly you can download an ultra-HD movie to your phone. However, this is unlikely to be what delivers transformational change in how we use mobile devices; nor will it provide the revenues to justify the investment made by network operators.

2. **Ultra-reliable low-latency communications:** These are needed for extremely time-sensitive and mission-critical applications, such as remote factory automation and so on. It's even been suggested that this could enable remote robotic surgery in which a surgeon is able to get real-time feedback on how the patient reacts to steps taken and can reliably make changes that are implemented in real time.

3. **Massive machine-to-machine communications:** 5G networks will enable a much greater density of transmitting and receiving devices, especially if they're sending small amounts of data. This will enable large-scale monitoring, measuring and sensing applications in which large numbers of devices directly communicate with each other without human intervention—machine-to-machine communications. This is sometimes also referred to as the 'internet of things'. While this is already starting to happen, 5G networks will enable exponential growth in the numbers of connected devices.

Other key features, depending on how networks are configured, can include 'edge computing', in which the equivalents of current cloud computing capabilities are brought closer to wireless devices to enable more rapid processing, and 'network slicing', in which different customers, applications, or both can have their own virtual slices of a common physical network.

In the underlying technology stack (see box), a key part of 5G network architecture is increased 'virtualisation', in which more and more functionality is implemented in software, including even the underlying network topology. This enables greater flexibility and agility in how they will be used, but also, as we shall see, brings greater complexity and potential security vulnerabilities.

It would be fair to say that no one really knows what 5G networks will be used for—including the service providers who will need to commercialise and monetise them. However, it's certain that they'll drive ever more usage and reliance on mobile data networks, and in particular more and more critical applications, transforming our way of life in ways not yet even imagined. Of course, this isn't unusual for new technologies—remember that the worldwide explosion in SMS messaging since the late 1990s came from an obscure engineering feature included in the 2G mobile specifications that was intended for network service messages.

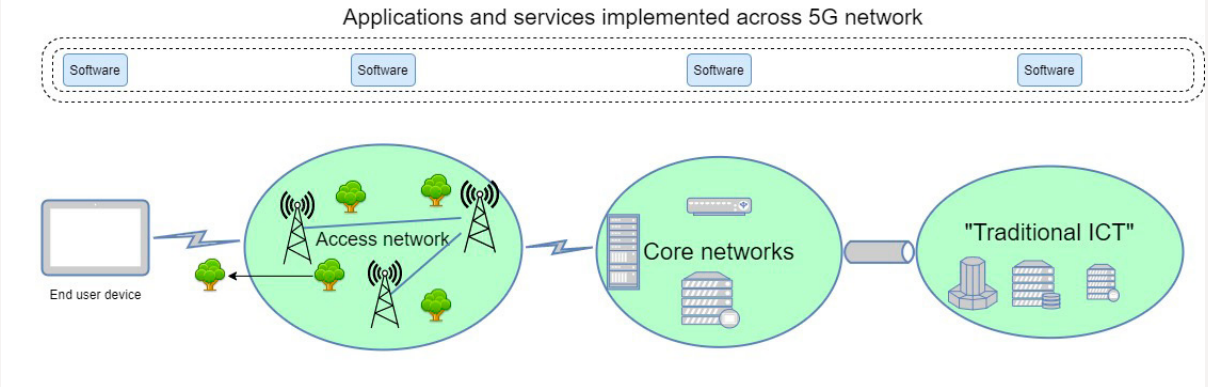
5G technology components

At the conceptual level, a telecoms network consists of:

- a radio access network (RAN)—antennas and electronics that convert between the radio signals sent to and from wireless devices and the bits and bytes sent as signals on network cables and inside computer equipment
- a core network that manages and carries the network traffic between the mobile devices and the other computer and network components, and also authenticates and provisions services to users
- traditional ICT—routers, switches and servers that provide the data transport, storage, processing and logic.

Within each of these 'black boxes' are a huge number of electronic components, some of which are specialised for the functions of 5G, such as high-density antennas and signal processing, and some of which are more generic (Figure 1).

Figure 1: A 5G network



The overall user experience is delivered by applications and services that run across the top of these components: different bits of software may run on different components of the system but work together to provide a seamless experience for the user. One of the differences in moving to 5G is that more and more will be done in software, and in order to provide the full experience the application service provider will need to run specific software on more parts of the network.

For example, today a messaging service such as WhatsApp requires specialised software running on the end-user device and on the WhatsApp servers. Tomorrow, supporting remote surgical procedures via a 5G network may require software running on the radio access nodes and servers at the edge of the network to meet the response time requirements.

This virtualisation will enable greater service customisation, scale and optimisation. The standards even envisage 'network slicing', in which there may be a dedicated 'slice' across the whole system for a particular user group and application service—effectively, computational and network resources on every box reserved just for them.

Overview of current 5G technology maturity

Preparations for 5G by telecommunications network operators are proceeding at pace. At the end of 2019, it was estimated that 348 operators in 199 countries had announced plans to invest in 5G.[3] However, implementation and take-up have been slow to date. Only 77 operators have deployed 5G technology, and 61 operators in 34 countries have launched services. Although only limited 5G-enabled devices are currently available, Ericsson estimates that there were 13 million users globally at the end of 2019, mostly driven by take-up in Korea and China.[4] The same report forecasts an estimated 2.6 billion active 5G subscriptions by 2025, but even that pre-pandemic estimate would still be less than a third of all mobile subscriptions.

While a glance at advertising material might make you think that fully featured 5G networks are commonplace in many major countries, the advertising doesn't tell you that those deployments are often only part of the overall 5G capability. Generally, operators have implemented radio interfaces that allow users to experience the faster mobile broadband speeds of 5G, but not other features. Even the radio interfaces are generally not using the cloud-based radio processing included in the 5G standards. Almost all currently deployed networks are built on top of existing 3G/4G networks (referred to as 'NSA', or non-stand-alone), which has allowed rapid rollout. That means that, while 5G coverage may be limited (for example, to just parts of major cities in Australia), users can have a seamless experience when moving in and out of 5G coverage. Chinese mobile providers had previously announced plans to deploy a stand-alone (SA) 5G network in the last quarter of 2019, but appear to have settled for an initial NSA deployment.

A full 5G core and SA network architecture will be needed to enable the other key features, such as low latency and massive machine-to-machine communications, and hence many of the transformational and mission-critical applications. This will require significant new investment in an environment in which network operators have had low margins from their existing businesses, even before the pandemic. The last-minute decision by China Telecom to change its deployment from an SA network to NSA probably confirms the challenges in implementing SA networks and the immaturity of the technology. That said, we are seeing some evidence of SA deployments this year despite all the disruption, for example with Telstra claiming to have made their network "standalone-ready" in May 2020[5], but it's clear that the full concepts and designs for true next-generation architectures and applications are still emerging.

5G standards and interoperability

Looking at the current 5G standards, it's clear that there's much to be defined. The current widely-implemented version of the 3GPP standard is R15, which really focuses on migration from 4G to 5G, and even for this operators have noted that different vendors have different approaches to the coexistence of the generations and to fallback from 5G to 4G when 5G isn't available. The next version of the standard, R16, issued in July 2020, starts to look at specific use cases such as industrial internet of things applications and better power consumption, but we'll need to wait for R17, the scope of which isn't even confirmed yet, in order to define some of the more critical features.

A further complication is that the agreement of standards, once considered a very dry subject in which technical experts put their heads together and collaborate to get the best technical outcomes, has now become politicised. Some nation-states have realised that there are advantages in influencing choices towards areas where they have expertise and technical leadership. This can help provide 'first mover' advantage in implementation and can also often deliver value from existing patents in the form of royalties (from manufacturers that make standards-compliant products) that can be reinvested in R&D to maintain a leading position.

As an example, in May 2018, it appears that Chinese companies were pressured into backing a Huawei proposal over one from US rival Qualcomm, and Lenovo's founder was forced to issue a statement denying the company had been unpatriotic and failed to back its compatriot in the final round of voting.[6] This is hardly surprising, given that homegrown technologies are often a matter of national pride, and China has set an explicit goal of becoming 'a standards-issuing country'.[7] The rewards for success in influencing the standards can be immense, in the form of both tangible, monetary rewards (licensing fees can be worth several billions of dollars a year to a company) and the intangible—the ability to influence how technology is used (see, for example, recent proposals by Huawei to the International Telecommunication Union for a 'New IP' internet architecture, which some have seen as an attempt introduce new, authoritarian-friendly values[8]).

Therefore, standard setting has become a key to global power and influence, but Australia and other allies don't appear to have recognised this and hence aren't currently in a position to compete in this sphere.

Although 5G is based on an 'open standard' published by the 3GPP consortium there are still factors that work against easy interoperability. Apart from the usual engineering challenge that different engineers may interpret standards differently, the standards definition process may be being manipulated, and in any case lags well behind what vendors are developing and carriers are implementing. The challenges from immature technology and the standards processes are undoubtedly a factor driving carriers to prefer single-vendor end-to-end solutions.

Although 3GPP, a body dominated by carriers and vendors, has become the de facto leader in mobile network standards, it is only one of a number of potential bodies. There is a potential overlap with the International Telecommunications Union which is an international member state, treaty based organisation, and there are also other competing standards bodies such as ISO and ETSI. Making a

choice about how and where to develop standards has became a matter of values and geopolitics, often at the expense of technology considerations.

Some carriers have recognised these challenges, in particular in relation to radio signalling and the problems of getting different base stations to work together, and have established their own initiatives, such as the OpenRAN venture under the Facebook-headed Telecom Infra Project. This initiative is intended to reduce the expense of providing internet and voice services by standardising the design and functionality of hardware and software in the RAN, increasing the number of companies that can supply components for the infrastructure that carries mobile traffic. There are a number of competing interests at play here: carriers and Facebook would like telecommunications in general to be cheaper; incumbents would prefer no increase in competition; and some states have interests in promoting national champions. Despite this, the OpenRAN initiative appears to be gathering momentum, with at least one global player, Nokia, recently committing to Open RAN interfaces[9].

Another development has been the announcement by a number of global carriers, including Telstra, of the establishment of the 5G Future Forum, which intends to produce uniform interoperability specifications, develop public and private marketplaces to enhance access to technology and share global best practice.[10]

If these sorts of initiatives don't succeed and the global 5G market ends up with different vendors dominant in different geographies, without clear standards and interoperability, there's a very real risk of long-term incompatibilities that will undermine many of the potential benefits. After all, it's happened before—in the 1990s, the major US carriers chose a technology called CDMA, while the rest of the world followed the GSM standard.[11] The current lack of a major US network equipment vendor is probably at least partially due to that bifurcation—US companies concentrated on developing a technology that no one else used and ended up in a technical dead end.

5G and cybersecurity

Why is cybersecurity seen as so critical for 5G networks? Because 5G isn't just the next natural stage in the evolution of wireless networks. 5G is about more than movie downloads. The likely applications and use cases will become critical to the functioning of governments, companies and society, including cyber-physical and safety-critical systems that will rely on the network. Not only do we need to be concerned about the confidentiality of data and users on the network, but we also need to consider the impacts of an attacker potentially compromising the availability and integrity of the systems, including the risks of the attacker being able to take down the whole network at once.

Australian and many other governments have already identified telecommunications networks as critical national infrastructure that's essential to the effective functioning of society and therefore requiring additional regulation and attention, and it's easy to understand why.[12] In Australia in recent months, we've seen the chaos caused by outages of electronic payment (EFTPOS) systems for a few hours, making it impossible for people to buy basic items because they're unused to carrying cash.[13] Now imagine the impact of a smart city suddenly losing all traffic sensor data and the ability to control traffic lights. An attacker could cause major accidents by maliciously changing the data being sent

to traffic lights. In fact, given some of the potential applications enabled by 5G, it could be possible to cause major disruption by more subtle changes. If applications such as remote driving of vehicles rely on ultra-low latency, what would happen if an attacker introduced a small delay to some or all network traffic?

The increasing importance of the network, combined with the increased risk that a cyber breach will cause major real-world consequences, means that the cybersecurity of 5G networks must be a critical consideration, planned and accounted for from the outset. Risk management approaches should also consider the more sensitive functions that are used by national security and law enforcement authorities, such as compliance with legislation on telecommunications interception and data retention, which may create additional security risks.

Building an understanding of 5G security requires integrating security and the 5G network architecture. Both suffer from a major skills gap in Australia[14] and globally,[15] so we would expect a major shortage of professionals with a detailed understanding of both, exacerbated by the fact that 5G architectures are complex and still evolving.

One example is the debates about the separation of the 'core' and 'edge' components of a 5G network. Can they be effectively segregated so that a threat in the edge can't affect the core? Australian authorities say they can't be effectively segregated, whereas UK authorities appear to be suggesting they can. Without getting involved in the details of the debate here, it's likely that the true answer is that it depends on architectural choices and complex overall system-level interactions. Concepts such as network slicing will make this even more complex. End users are given effective control and exclusive use of an end-to-end slice of the network, and attention will need to be paid to the security safeguards required to minimise the risk of them escaping their own virtual slice and getting access to other parts of the network.

Vendor trust and security

The issue of vendor trust and security has been prominent in discussions about 5G security. Australia and the US have announced decisions to bar certain vendors, the UK has been formulating a compromise approach,[16] (although this seems to be still evolving) and active debates in Europe are seemingly close to reaching a conclusion.

The risks from using a particular vendor can be many and varied. Much commentary on the subject talks about hardware 'backdoors' being inserted by a vendor at the factory,[17] but that's probably not the biggest issue. In fact, it's probably an unhealthy focus that can drive the debate onto specific component manufacturers, when the bigger risks probably come higher up the technology stack. A much more worrying vendor risk occurs when carriers are critically dependent on vendors for maintaining the quality of service and so give the vendors access to the live network for support and maintenance. The nature of 5G networks as 'software defined everything' also means that there are security risks throughout the network that can be hidden in the complexity of software—vulnerabilities that are deliberately introduced by the vendor, or that come from genuine errors and oversights.

Different vendors have different approaches to and cultures of security. The extent to which they use approaches such as secure software development, system integrity validation and third-party supplier checks can be a useful guide, as well as their approach to the reporting and patching of security issues.

However, the control and ownership of vendors, in particular those from nation-states in which companies may be subject to extrajudicial direction, has, to date, been the main criterion used to measure vendor risk.[18] This should be broadened to consider all sources of risk. As well as foreign ownership and control, vendor threats can come from insiders, such as rogue employees, even in a vendor from a trusted country, and also depend on the quality of the security culture and secure-by-design approaches used by a vendor. This leads to a spectrum of vendor risk levels that can be used to guide appropriate treatments. We can sensibly decide to exclude very high risk vendors, but since no vendor will be zero-risk, other mitigation measures will be needed in addition. While, given the criticality of 5G networks, we should impose a high standard of cybersecurity control and risk management across the network even for the lowest risk vendors, additional measures may be needed for intermediate levels. It's important that carriers understand these requirements and can factor the different security costs into their procurement decisions (so potentially avoiding the incentive to simply choose the cheapest supplier who isn't excluded due to being very high risk).

Independent testing of vendor equipment may be of some use to assess and mitigate risk (see, for example the Huawei testing facility set up and used by the UK over the past few years), but it's not just a matter of testing the product from the factory. For any software components, each new release will require retesting, and in a 5G world the software becomes the most critical layer. The public reports from the UK testing facility[19] show a series of damning findings and a lack of any assurance that identified flaws are resolved effectively. This means that, at best, this approach can be only a small part of a broader strategy.

In some cases, architectural approaches can be used to mitigate the risk. For example, end-to-end encryption could be used to mitigate the risk that particular network equipment could have unnecessary access to user details and data on the network. However, if we look at the risk of an adversary seeking to completely disable a network, the vendor risk is much greater, as ultimately the end-to-end network works only if every component in the chain is working—RAN, core access and routing.

This means it isn't just a matter of assessing and using a vendor with an acceptable level of risk. Any farmer will tell you to avoid monoculture—growing just one crop means that one disease can wipe you out overnight. Similarly, if a network is dependent on a single vendor and a vulnerability is found, the vendor becomes untrusted for some reason or the company collapses, the equipment will be almost impossible to replace, and entire networks can become at risk overnight.

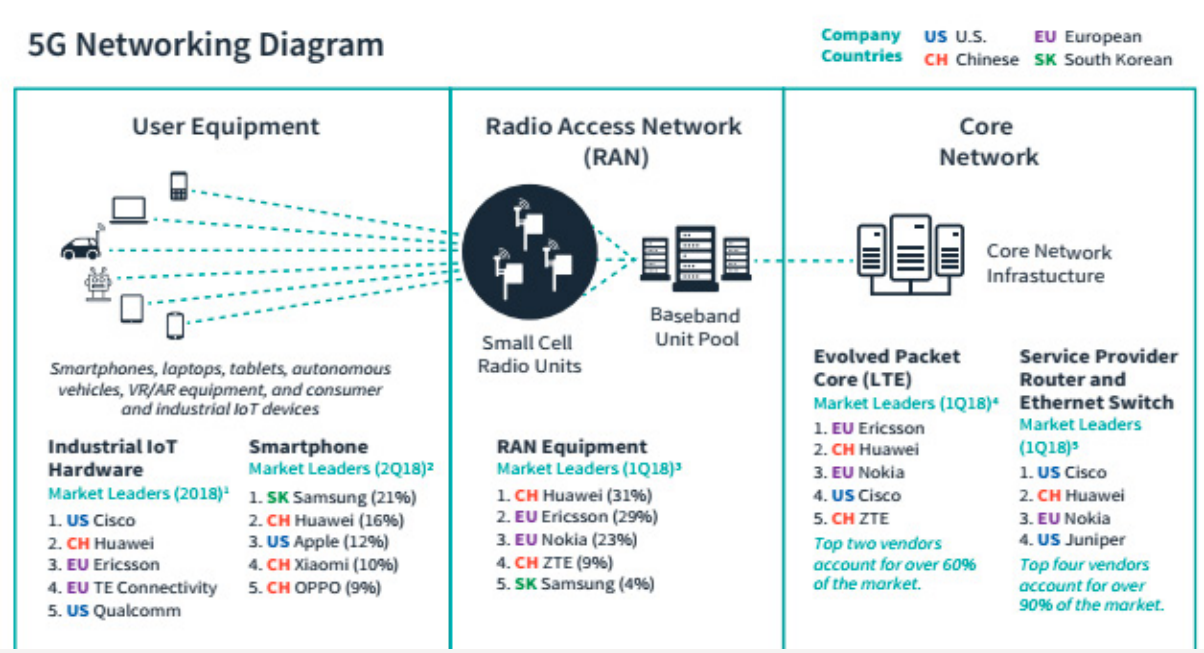
Therefore, as well as vendor trust, we need to ensure vendor diversity and redundancy in design. Operators need to have confidence that multiple vendors' equipment can interoperate, and ideally have multiple vendors' systems in service for each major function. This will provide resilience and options to reduce dependence on a particular vendor if circumstances change. In a given carrier's network, there should be at least two vendors for each key equipment type, and across the market there should be four or more viable suppliers considered acceptable to use. These are bare minimums

from a competition policy and resilience perspective; from a long-term resilience point of view, there should be as many vendors as possible, subject to ensuring that each has critical mass and is commercially sustainable in the long term.

The 5G vendor landscape

The dominant vendors in the 5G market are generally considered to be Huawei and ZTE from China, Nokia from Finland and Ericsson from Sweden. This is certainly the case in the 5G network equipment sector, although they have some competition from Samsung (Korea) for radio equipment and Cisco (US) for the network core. There's more competition in the devices market and for switches and routers. The main market players are shown in Figure 2.

Figure 2: The main 5G players



Source: Adapted with permission from James A Lewis, *How will 5G shape innovation and security: a primer*, Center for Strategic and International Studies, Washington DC, 2018, 4, online.

Figure 2 shows that Chinese companies are major players in the network equipment market, but not (yet) runaway leaders. Ericsson and Huawei have very similar shares of the RAN equipment market, and Nokia isn't far behind, and for the evolved packet core Ericsson leads Huawei. The US is also starting to have a presence among market leaders in the core network, where much of the future growth is expected. All three network equipment categories show very strong concentration: only two or three non-Chinese vendors in each category have any significant market share.

Considering the RAN in more detail, the OpenRAN initiative mentioned above is creating opportunities for new entrants. In January this year, O2, the Telefonica-owned UK mobile operator, announced plans to engage new UK- and US-based entrants, including Mavenir, DenseAir and WaveMobile, in an OpenRAN deployment.[20] In November 2018, Vodafone revealed that it had issued a request for information covering tests for OpenRAN-compatible solutions and received responses from seven

vendors, only one of which (Samsung) appears in the list above; the others were a mix of US, French and Indian companies. Vodafone then ran a request for quote process for the deployment of OpenRAN across 100,000 sites on its European networks.

Down at the component level, there's greater diversity. For specialised radio components, such as small cell antenna arrays and power amplifiers, European and US companies dominate, and for specialised field-programmable gate arrays, which are essential for high-power embedded processing, there are really only two major manufacturers: Intel and Xilinx, which are both US companies. This confirms that, if the US continues to enforce the listing of Huawei on the 'Entity List', and thus prohibit exports of US-made components to it, there would be serious impacts on Huawei's ongoing manufacturing capability, at least in the short to medium term.

If we look further up the stack to the services and applications layer, that's where many critical applications will be implemented, which also provides an opportunity to reduce dependence on the network equipment (for example through end-to-end encryption). The use cases and applications are only now being defined and implemented, so it's too early to identify the key players in this space, but it will be an important one in which to understand vendor trust and act accordingly.

Market opportunities and barriers

The 5G infrastructure spend was US$784 million in 2019 and is forecast to be US$47.8 billion in 2027.[21] This estimate didn't account for the impact of Covid-19, which is likely to cause some delays and cutbacks, but the market over the next few years is still likely to be highly lucrative as a whole, although the accessible RAN market may be less so due to the high market share of low-cost Chinese vendors . While a significant portion of the revenue will go to the established players noted above, there are still opportunities for new entrants to gain significant revenue, given that the development and building of fully featured 5G networks is still at an early stage.

Compared to earlier generations of mobile technology, 5G offers more opportunities for new entrants to the market. This is because in 5G architectures a significant number of functions become virtualised and are implemented in software. This opens up opportunities for software solution providers unconstrained by the costs and timescales of bespoke hardware development—especially if they can write efficient, fast and reliable code to implement mission-critical use cases. This world of 'software defined everything' means that innovative and potentially sovereign businesses have the opportunity to add trust and value at the software layer.

The RAN equipment market presents particular challenges—it traditionally requires specialist hardware for antennas, radio signal generation and reception, and signal processing. Significant investment and time are needed to develop new hardware for the new frequencies, higher speeds and more devices that 5G will need to support. However, the 5G architecture does mean that, even for radio processing that's traditionally done using specialised hardware at the antenna site, signals can be digitised and processed in software at remote sites.

In other network equipment classes, there will still be barriers to entry. The established players can be expected to compete strongly to maintain market dominance. They'll also use the immaturity of standards to persuade service providers that it's lower risk to use a single end-to-end provider. From discussions with providers for this report, this could resonate, especially given consumers' focus on service quality. Telecoms companies nowadays prefer to buy managed services from vendors rather than build and integrate systems themselves. This means that when there are service outages they have a 'single throat to choke' (their vendor's), rather than having to referee finger-pointing between vendors. A shortage of systems engineering skills has also been identified as a major barrier to enabling telecoms companies to consider developing multivendor environments, along with the challenge of needing to develop expensive interoperability testing facilities.

The third area of opportunity is in developing and running applications and services across the network to implement 5G use cases. In this case, the market for software to implement new applications is wide open, given that the applications have often not even been defined, or in some cases probably not even imagined yet. [22] However, we can still expect the leading network equipment vendors to compete strongly, given their obvious adjacency and the opportunity to grow their businesses. Revenue streams from network equipment sales, in addition to any state subsidies, can be used to fund major R&D budgets and aggressive pricing. Antidumping provisions are especially difficult to manage for software, given the low cost of production, and carriers will always have financial drivers to choose the cheapest option without necessarily paying heed to broader requirements for vendor diversity and risk management.

Established vendors, wherever they're from, can be expected to promote the perceived benefits of their end-to-end integration, critical mass and established brand recognition. They may use their control of the platform to seek to set up trusted ecosystems (think of Apple iOS devices and the App Store) in the name of security and openness, while in practice setting up barriers to entry. We can also imagine groups of platform, software and hardware vendors from one country, with implicit or explicit encouragement from their government, looking to set up collective monopolies. Carriers will see advantages in single-vendor solutions, in reducing performance risks, reducing their requirements for system integration skills etc. The challenge will be to persuade major carriers to look at the broader risk landscape, to be willing to integrate multi-vendor solutions and to put faith in emerging companies for what would be expected to be a long-term investment.

Recommendations for developing the trusted vendor market

We've noted that there are significant opportunities for vendors from Australia and allied countries to develop critical technology. However, they face significant competition from established players with economies of scale, and in some cases direct or indirect foreign government support. Appropriate policy actions will be needed to overcome the barriers in order to open up genuine opportunity for a broader range of vendors and provide the diversity that we need to improve the security and resilience of our 5G ecosystem.

Take a graduated approach to risk assessment and mitigation

There is a need for appropriate market signals to encourage carriers to choose lower risk vendors. There's already, in Australia and some other countries, an outright ban on very high risk vendors, but, given the spectrum of risk, regulation should also ensure that the increased security costs of choosing a higher risk option sit with the carrier, rather than, for example, national cyber authorities being responsible for extra costs as they seek to protect carrier networks against vendor threats and mitigate risk.

The Australian Cyber Security Centre should develop a comprehensive framework of recommended vendor risk ratings based on various factors. The ratings should be used to define mandated risk-mitigation actions based on risks, which could include tailored levels of isolation, control and monitoring of any access that vendors are given to live networks for support and maintenance purposes, along with limitations on offshore managed service provision and offshore data storage. Another example could be ensuring that sensitive and critical functions (such as lawful interception and audit logging) are segregated and can be separately managed using highly trusted solutions independent of the main network equipment vendors.

Regulate competition

Competition and merger policy levers should also be used to ensure fair opportunity for new entrants by limiting consolidation, preventing cross-subsidies of existing major vendors when selling new capabilities, and perhaps even mandating major vendors to subcontract a portion of the work. This could include identifying where companies may be receiving subsidies from nation-state governments, and whether trade and international agreements provide remedies to address unfair competition impacts.

These restrictions should apply to all existing major vendors, not just those from high-risk jurisdictions. It wouldn't be an appropriate approach to just pick one or two 'winners' from the existing major European and US vendors—a rich, diverse, vendor pool is needed to ensure the long-term resilience of our 5G networks.

Expand industry development policy and invest in key technologies

We've seen that building 5G vendor diversity can also be an economic opportunity for Australia. Therefore, we should ensure that industry policy promotes this. While we have a strong start-up culture, we need to ensure that successful companies are able to scale up rapidly to credibly compete and serve the global market.

Regulatory barriers that prevent or slow scale-up should be identified and addressed, and action is also needed to address the problem of access to capital. The Australian Government should establish an investment fund that can fund key technologies critical to our national security. It could be modelled, for example, on the National Security Strategic Investment Fund set up by the UK.[23] Its remit would probably be broader than the scope of this paper, but it could certainly help to support the scale-up of 5G technologies. Another model to consider could be the recent proposal from a group of US senators for a US$1.25 billion proposal to fund new R&D and a multilateral project fund for 5G technologies.[24]

Encourage a more open network equipment market

Given the desired objective of vendor diversity, we need to ensure that carriers have both the right incentives and the confidence to move away from the single-vendor environment. To assist this, the government should establish, fund and manage an independent test facility for 5G networks. This should be fully modular to allow the testing of different components from different vendors (as an example of how this can be done, see, for example, the Open 5G Core project[25]). As well as enabling interoperability testing, this would also enable security and vulnerability research and testing at the overall 5G system level, which we've noted is currently a poorly understood area. Potentially, this could be a joint undertaking with other allied countries, such as Canada and New Zealand, to reduce costs, but we caution that it should be ensured that Australia is a major contributor to this and hence able to use influence to achieve our own national security objectives.

Consideration should be given to mandating that network providers use multiple vendors for key components. This may be difficult to implement, and network providers may have concerns over the burden that it imposes. However, doing so would go a long way towards overcoming the possibility of 'monoculture' security risk. Other countries, such as the UK, have discussed going in a similar direction, and that may allow Australia to learn lessons from their experience and devise an appropriate approach for our circumstances.

We need to ensure active engagement with 3GPP on standards setting to avoid politicisation and ensure that choices that maximise overall security and resilience, and market opportunity for new entrants, are made. This will include the identification of the key use cases for priority development, seeking to avoid choices reliant on foreign patents, and preference for the best technical choices based on open standards and implementation. Current responsibility for such engagement is diffused among different organisations, so one organisation needs to be given the mandate and funding to lead this work.

We've noted the challenges with standards-setting bodies, so, if engagement there doesn't prove effective, there may be a need for local regulations to mandate open interfaces for the most critical functions, especially where they're needed to provide the option to segregate critical functions to be carried out by sovereign vendors. As an example, for lawful interception, open internal interfaces, referred to as X1, X2 and X3, would allow the administration of warrants and the intercepted data to be partitioned securely. Ideally, we could seek to align such regulations with those of other like-minded countries, but in the absence of agreement Australia may need to act alone in our own interest.

Address RAN equipment supply

Even though the RAN forms only one part of the overall 5G network, the small number of suppliers and its criticality to the overall availability of the network indicate that equipment supply should receive some focus from policy-makers. Although it does not seem likely to lead to security or diversity benefits in the short term, if the OpenRAN initiative gains more momentum it will also provide opportunities for new entrants. Australia should work with allies and other countries that do not have domestic suppliers or interests in promoting their national champions to encourage further adoption of the OpenRAN standard to allow more vendors into this marketplace using appropriate combinations of grants and incentives to carriers to encourage them to adopt this standard.

Invest for the future

Finally, action needs to be taken to prepare for the future to avoid a repetition of this situation with other emerging technologies. Australia needs to invest in developing and commercialising technologies for artificial intelligence, 6G, quantum computing and other emerging fields. In building the right skills pipeline, we should also address current perceived skills gaps. We need systems engineers who can design and build systems bringing together components and technologies from different companies.

Conclusions

5G networks are the next generational uplift in mobile communications technology. They'll enable not only fast speeds but more reliable, low-latency communications and massive machine-to-machine communication, enabling new applications for which security will be critical. While there are significant identified risks to the privacy and confidentiality of data on the network, and the users, there are also risks from an adversary seeking to completely take down a communications network or compromise its integrity. There are a number of potential causes, but a significant one is trust in the vendors whose equipment is used. Various countries have made differing decisions on excluding specific vendors considered to be high risk, but the discussion needs to move on, as reliance on one or two 'not high risk' vendors will still create major security risks. Long-term security and resilience depend on a diverse vendor ecosystem.

Fortunately, the technology and rollout plans for 'real' 5G are still developing, so now's the time to take appropriate action. We recommend that urgent action be taken to identify opportunities for developing new capabilities, the barriers to market entry, and policy actions to encourage new entrants and build a diverse 5G vendor ecosystem. Table 1 summarises our findings and recommendations.

Table 1: Findings and recommendations

Market segment	Barriers to entry	Recommended actions
RAN equipment	Timescales and costs for specialist hardware	Incentives to promote OpenRAN technology
Other network equipment	Telcos reluctant to integrate multivendor systems	Establish interoperability testing facility Consider mandating multiple vendors in networks
	Immaturity of standards	Engagement with 3GPP standard setting Local regulations where needed to promote interoperability
	Lack of market incentives for more trusted suppliers	Graduated risk assessment and mitigation framework for vendors
Application software	Competition and cross-subsidies from network equipment vendors	Regulations to stop anticompetitive behavior and dumping
	Start-ups can't scale up to be credible contenders for long-term, large-scale rollouts	Address regulatory barriers Access to funding, including investment capital and targeted R&D grants
Market-wide	Lack of focus on developing strategically important technologies	Identify future areas, such as artificial intelligence and 6G, and build fundamental sovereign capability now

We should seek to work in coordination with our allies and other like-minded countries for maximum impact. However, if we wait to first build global consensus it's likely that we'll miss the window of opportunity. Australia took the lead in making the decision to exclude the highest risk vendors and now needs to lead in taking the next set of actions required for the long-term security and stability of 5G infrastructure, and in parallel encourage others to work with us in this endeavour.

Notes

1 For more information on 3GPP membership and activities, see ***About 3GPP home***, 3GPP, 2020, online.

2 *Release 15*, 3GPP, 26 April 2019, online.

3 GSA market snapshot, January 2020.

4 Patrik Cerwall (ed.), *Ericsson mobility report*, Ericsson, November 2019, online.

5 https://www.itnews.com.au/news/telstra-readies-its-mobile-network-for-standalone-5g-use-547609

6 Ma Si, Cheng Yu, 'Lenovo rebuts rumor it failed to back Huawei on 5G issues', *China Daily*, 18 May 2018, online.

7 Lindsay Gorman, 'The US needs to get in the standards game—with like-minded democracies', *Lawfare*, 2 April 2020, online.

8 Martin Joseph, 'Inside China's controversial mission to reinvent the internet', *FT*, 28 March 2020, online (paywall).

9 https://www.techradar.com/au/news/nokia-to-integrate-open-ran-in-2020

10 Jonathan Nally, 'Telstra and other firms form 5G Future Forum', *Technology Decisions*, 16 January 2020, online.

11 CDMA = code-division multiple access; GSM = global system for mobile communications.

12 Critical Infrastructure Centre, Australian Government, online.

13 Shoba Rao, Nicole Pierre, 'Australian consumers hit by EFTPOS outage', *News.com.au*, 11 July 2019, online.

14 AustCyber, *Australia's Cyber Security Sector Competitiveness Plan 2019*, 2019, online.

15 Kelly Hill, '5G deployment faces a skills gap', *RCR Wireless News*, 4 April 2019, online.

16 UK Government, 'Coronavirus (COVID-19): what you need to do', *Gov.UK*, 28 February 2020, online.

17 See, for example, Peter Bright, 'Bloomberg alleges Huawei routers and network gear are backdoored', *ArsTechnica*, 5 January 2019, online.

18 Scott Morrison, Mitch Fifield, 'Government provides 5G security guidance to Australian carriers', joint media release, 23 August 2018, online.

19 'Huawei cyber security evaluation centre oversight board: annual report 2019' UK Cabinet Office, 28 March 2019, online.

20 Bevin Fletcher, 'UK's O2 taps non-traditional vendors for O-RAN project', *FierceWireless*, 16 January 2020, online.

21 '5G Infrastructure Market by Communication Infrastructure, Core Network, Network Architecture, Operational Frequency, End User & Geography - Global Forecast to 2027', *MarketsandMarkets*, Oct 2019, online.

22 As an example, in the late 1990s some companies made huge revenues from developing software to send short service messages around 2G networks—which was ultimately used for the explosion in SMS communication.

23 'British Business Bank launches £85m National Security Strategic Investment Fund (NSSIF) Programme to support development of advanced dual-use technologies', news release, British Business Bank, 31 July 2018, online.

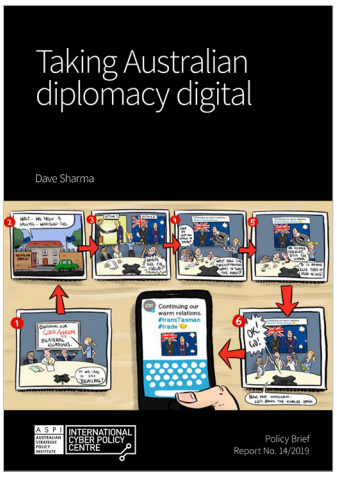
24 Mark R Warner, 'National security senators introduce bipartisan legislation to develop 5G alternatives to Huawei', press release, 14 January 2020, online.

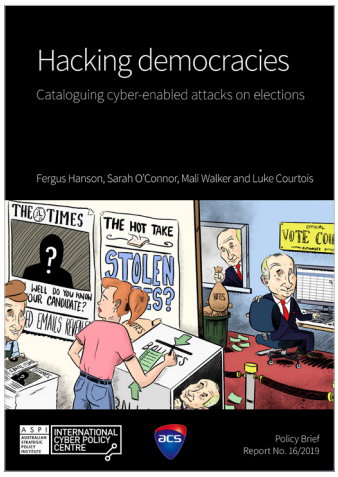
25 https://www.open5gcore.org/

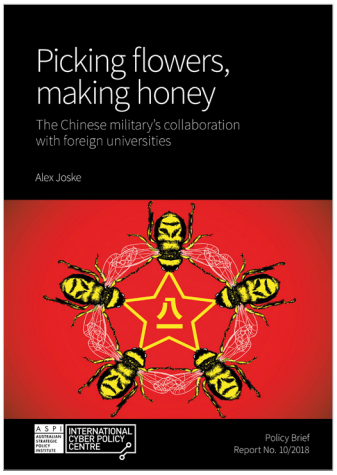
Acronyms and abbreviations

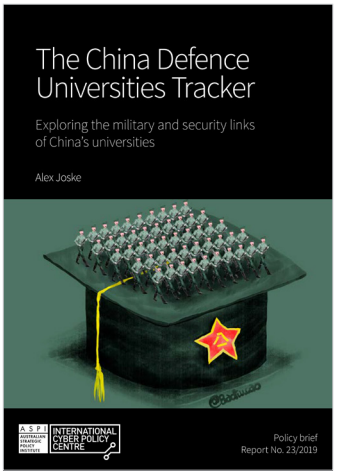
3GPP	3rd Generation Partnership Project
ICT	information and communications technology
NSA	non-stand-alone
R&D	research and development
RAN	radio access network
SA	stand-alone

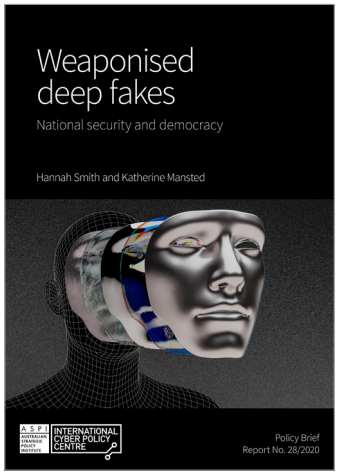
Some previous ICPC publications

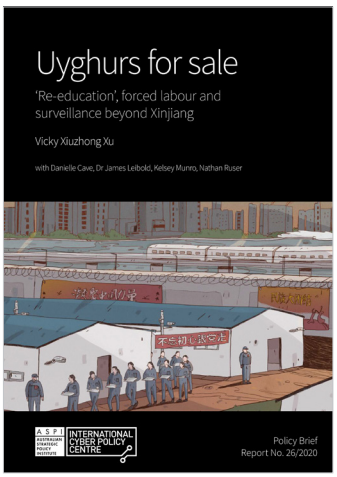


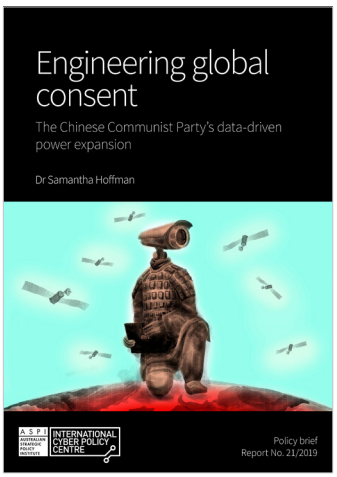












ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE