ECIPE | EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY

POLICY BRIEF

No. 8/2018

5G and National Security
After Australia's Telecom Sector Security Review

by Nicolas Botton (nicolas.botton@ecipe.org) and Hosuk Lee-Makiyama (hosuk.lee-makiyama@ecipe.org)
Research Associate and Director repectively of the European Centre for International Political Economy (ECIPE)

EXECUTIVE SUMMARY

In August 2018, the government of Australia concluded its review of the national security risks of the telecom sector with the new 5G networks. The review provides new guidance to telecom carriers, implicitly restricting Chinese vendors.

It concludes that 5G changes how the networks operate and increase the potential security risks to the point today's safeguards are insufficient. The government must therefore intervene, as foreign powers may exploit these risks by coercing vendors.

The current rise in national security restrictions in the telecom sectors are different from the typical run-of-the-mill economic protectionism as they are imposed by countries that have no domestic suppliers to protect.

Instead, the root of these measures is fundamentally about distrust between governments with conflicting geopolitical agendas, rather than just trustworthiness of the vendors. The situation is not too dissimilar to the US online services after the NSA revelations in 2013.

In effect, future security screenings will assess other governments – i.e. the ability of a foreign state to exercise control over its vendors, rather than assess the vendors themselves. Some legal frameworks, such as the US reforms of Cfius or the EU's proposed new FDI screening framework, already point towards such directions.

THE BACKGROUND

In august 2018, the government of Australia concluded its review of the national security risks of the telecom sector with the new 5G networks. The review provides new guidance to telecom carriers, implicitly restricting certain vendors from building the country's future telecom networks. The decision has an impact beyond Australia, and a number of jurisdictions that have initiated similar reviews, formally or informally – including Canada, Japan, Korea, the UK and several European countries.

The circumstances leading to the decision in Australia is by no means isolated there: The number of reported cybersecurity incidents has spiked globally in recent years.[1] On many of these occasions, involvements of government-sponsored advanced persistent threat groups (APTs) has been alleged, leading to indictments of serving officers from third countries as collusion with the government.[2] Indeed, the Australian decree points to the "involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law".[3]

The calls for intervention coincide with perhaps the biggest technological shifts in the modern information infrastructure: the deployment of the fifth generation (5G) networks, which will digitalise unprecedented amount of corporate and government data. The potential dividend of cyber espionage increases exponentially,[4] which has prompted unprecedented government action.

These developments break with the openness, inclusiveness and global competition of the rule-based free trade order.[5] However, the fundamental change in the circumstances between then and now is probably just one – the unavoidable emergence of China as a strategic power, and the reactions this has incited from the rest of the world.

While China is militarily inferior to the United States, it has other means to pursue its national interests. Its executive has a unique ability to redirect the resources in its economy, including harnessing the technological prowess of its private sector. China increasingly projects global influence by leveraging on the attractiveness of its domestic demand. Attempts to contain such power, and to resist multipolar governance,[6] has ushered the trading system into unilateral actions and new frictions.

And Chinese industries are inarguably at the receiving end of such friction. On many occasions, such reactions are often the same run-of-the-mill economic protectionism that other Asian exporters had to face in the 1970s and 80s.

While the telecom equipment industry is not void of initiatives to protect the domestic industries,[7] the new restrictions on mobile infrastructure and 5G suppliers are imposed by countries that have no domestic suppliers to protect. Economic protectionism or China-bashing are incomplete answers to why these new restrictions are affecting 5G technology suppliers.

Australia's decision has many underlying technical and legal arguments. It deems that 5G changes the way the network operates compared to previous mobile generations. Also, technology vendors

[1] Verizon. (2017), Data Breach Investigations Report, Verizon, 10th edition.
[2] Accenture. (2017), 2017 Cyber Threatscape Report, Accenture, accessed at https://www.accenture.com/t20170721T220639Z__w__/us-en/_acnmedia/PDF-57/Accenture-2017-cyber-year-threatscape-report.pdf.
[3] Ministers for Communications and the Arts, Senator the Hon Mitch Fifield. (2018), Government Provides 5G Security Guidance To Australian Carriers, 23 August 2018.
[4] Lee-Makiyama, H. (2018), Stealing Thunder, ECIPE, accessed at: http://ecipe.org//app/uploads/2018/02/ECIPE_Occasional0218_HLM_V7.pdf.
[5] Lee-Makiyama, H. (2011), Future-proofing World Trade in Technology, ECIPE, accessed at: http://ecipe.org/publications/future-proofing-world-trade-in-technology-turning-the-wto-it-agreement-ita-into-the-international-digital-economy-agreement-idea/.
[6] See inter alia Posen, Keohane, Zakharia et al. developing the concept of the end of unipolarity.
[7] Chaffin, J. (2013), EU faces up to China over 'mother of all cases', Financial Times, January 31, 2013.

must follow the rules of the markets they operate but must also comply with orders to cooperate with the intelligence agencies at home. Obviously these obligations could contradict. Chinese vendors Huawei and ZTE may be singled out in today's debate – but their situation is not too dissimilar to the US online services after the NSA revelations in 2013.

This paper argues the cause to the situation is fundamentally about distrust – not necessarily against certain vendors, but distrust between the governments of where tech firms originate and where they operate. Governments with conflicting goals distrust each other and the methods they deploy to achieve them – and such distrust, which is deeply rooted in core national interests, can neither be attributed to nor overcome by the tech firms.

AUSTRALIA'S ASSESSMENT OF THE 5G SUPPLIERS

In August 2018, a press release by Senator Mitch Fifield, Australia's Minister for Communications and the Arts, expressed the view that telecommunications vendors "likely to be subject to extrajudicial directions from a foreign government" may fail to "adequately protect a 5G network from unauthorised access or interference".[8]

Although the language of the declaration does not reference any country in particular, its implicit ban of Chinese firms quickly drew criticism from China's Ministry of Commerce, deploring the impact it would have on relations between the two countries.[9] Indeed, although Australia's cybersecurity assessment regime, overseen by the Australian Security Intelligence Organization (ASIO), can yield recommendations, rather than prohibitions. In practice, Australian authorities would follow any recommendations provided.

Furthermore, as the letter notes, part of Australia's Telecommunications Sector Security Reform (TSSR) includes a stricter screening mechanism, where any change to telecommunications systems "likely to have a material adverse effect on their capacity to comply with their security obligation" must be notified, so that the relevant authorities may provide direction. This means that the clear guidance that the Australian government has provided carriers regarding "how their new legal obligations apply to 5G networks".[10] is in practice a ban on procurement from certain types of telecommunications vendors.

The assessment by ASIO – which likely formed the basis of Sen. Fifield's letter – is particularly significant, because it represents a precedence for western powers with strong economic ties to China, putting their security concerns ahead of economic interests – including those of operators like Vodafone, Optus and TPG who use Chinese vendors in their networks.[11]

There are principally important discussions that follow from Australia's TSSR decision.

— The first issue is whether the architecture of 5G actually changes how the networks operate and increase the potential security risks, despite its many security features. This is first and foremost a technical question, but a question which has a bearing on which products the vendors may be allowed to supply.

— The second issue on the review is about its form. The TSSR decision is not a hard law that forbids certain vendors. Instead, TSSR introduces new measures that create new

[8] Fifield, M. (2018), Government Provides 5G Security Guidance To Australian Carriers, Ministers for Communications and the Arts, Joint Press Release, August 23 2018, accessed at: https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers.

[9] Needham, K. (2018), Australian government made 'wrong decision' over 5G ban, says China, Sidney Morning Herald, August 24, 2018, accessed at: https://www.smh.com.au/world/asia/china-australia-government-back-stabbers-over-huawei-decision-20180824-p4zzg0.html.

[10] Ibid.

[11] Smyth, J. (2018), Proposed Huawei ban seen hitting Australian 5G push. Financial Times, August 13 2018, accessed at: https://www.ft.com/content/5a22be84-9b92-11e8-9702-5946bae86e6d.

obliges for the Australian operators as well as for the government to intervene and issue directions in some instances.

— Third and finally, the decision highlights how some foreign powers may be able to exploit this technical change through the involvement of vendors.

The consequences of these three points are now further examined in the coming sections.

FIRST ISSUE: NATIONAL SECURITY IMPLICATIONS OF 5G

To begin, TSSR immediately highlights how 5G changes the way the society uses, and ultimately rely on mobile technology. The growing digitalisation of society has increased the scope and potency of cyber espionage with increasing number of incidents already before 5G: The commercial value of the corporate information carried in a 5G network will increase multifold compared to today,[12] thanks to the Internet of Things (IoT) that will enable connected manufacturing and production processes, increasing the economic risks at stake.

Australia's decision is rooted in the risks from how the 5G architecture operates differently than previous technologies. The wireless telecommunication network consists of several parts, and whereof two parts are particularly relevant in a security assessment:

> (1) the core network, which is the central element of the network connected to the broader internet, and which is constituted of routers and switches delivering information to sub-networks; and
>
> (2) the radio access network (RAN), connecting individual devices to other parts of the network and made up of radio antennas and base stations.

The theoretical basis of the security risks in the mobile networks is principally two. Firstly, if the equipment in the core network has been tampered with (and backdoors have been installed in the software), an outside entity could intercept all data and even install new software updates allowing broader access. As this is still possible to do even after the systems have been verified and passed a security screening, such a possibility would render today's policy measures (like source code disclosure and testing requirements) ineffective.

Secondly, backdoors can also be installed in specific RAN (i.e. mobile base stations deployed in the field) on strategically placed locations, which allow data theft and interception from any number of connected facilities. These kinds of attacks are hard to detect, as information could be exfiltrated as normal user traffic, or embedded in other traffic. Attacks on RAN could also lead to other national security threats, such as radio jamming, or allowing threat actors to repurpose the base stations to redirect, modify, or duplicate traffic to a shadow network, while still appearing to function normally.

As of date, Australia restricts some vendors – Chinese vendors – to supply equipment to the core network under the 4G network. Tampering on the core network could cause more extensive damage and allow broader data theft than in antennas and base stations. Restrictions on Chinese vendors in Australia (as well as Canada, France, Italy) were on the more sensitive core networks alone, while the excluded vendors were still allowed to supply antennas and base stations.

Australia's decision on 5G vendors highlights about how the sensitive functionality of core networks and RAN will overlap. The decision reads "5G is designed so that sensitive functions currently performed in the physically and logically separated core will gradually move closer to the edge of the network." [13]

[12] Lee-Makiyama (2018).
[13] supra note 8.

On the one hand, critics argue that industry standards of 3GPP clearly define the distinction between RAN and core networks. On the other hand, Australian officials argue virtualisation and shared software, making the distinction between the two parts less relevant for a national security assessment. Also, connected devices – from industrial equipment to a smartphone – will be connected to each other like a web, rather than just the network in a hub-and-spoke fashion, making the distinction between RAN and core networks irrelevant from Australia's national security perspective.

In conclusion, the approach taken by Australia must boil down to an all-or-nothing approach: Australia concludes it must either allow all vendors to bid for the entire 5G network, or to deem them to be a risk from its all parts.

SECOND ISSUE: USING A SOFT LAW APPROACH

As evident from the Australia example, national security concerns have greatly affected the market for telecom equipment even prior to the advent of 5G. Limitations on what certain vendors can sell were also imposed in countries like China, Australia, Canada, France, Israel, Italy, Taiwan and the US. In addition, A majority of the countries always maintained a certification or screening scheme in some form.[14]

Such restrictions could be comprehensively applied, or just partially, which allowed the restricted vendors to supply to a certain area. For instance, in the case of France, operators were permitted to use Chinese vendors outside the administrative capital area of Paris.[15] Restricted vendors were still allowed to supply the radio access (RAN) networks (e.g. radios and antennas) in rest of the country, but faced nationwide restrictions on mobile core networks where the sensitive functionalities occur, such as access control, authentication, routing or billing.

Also, these restrictions could be implemented *de jure* through hard law, soft law (e.g. through policy guidelines, informal administrative or party guidelines or case-by-case decisions) or mixture thereof. For instance, in the US, the 2019 National Defense Authorization Act bans Huawei and ZTE from China outright from being used in Federal networks,[16] as well as the Russian anti-virus software Kaspersky.[17] However, *de facto* restrictions were already in place, at least since the 2012 House Intelligence Committee report on these companies.[18] Private market sales (to US operators) and investments were deemed unrealistic since 2008 when Huawei was 'discouraged' from acquiring the ailing device manufacturer 3Com before the Committee on Foreign Investment in the United States (an interagency government committee with the competence to block foreign investments) could intervene in 2008.[19]

These measures are reciprocated by China, whose scale of digital protectionism is unparalleled in the world economy according to independent surveys.[20] Since 2007, China's Multi-level Protection Scheme (MLPS) for government procurement has restricted the purchase of foreign IT products within "critical information infrastructure" (CII) amongst Chinese telecom

[14] ECIPE. (2018), Digital Trade Estimates.
[15] Under Article 226 3 of Code Pénal it is illegal in France to supply, manufacture, import, hold, display, or sell any equipment that could infringe privacy rights, unless an authorisation is obtained, and Chinese suppliers are limited core mobile networks and from supplying Radio Access Networks (RAN) in greater Paris area.
[16] H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019.
[17] Johnson, D. B. (2018), More detail on why DHS Banned Kaspersky, FCW, April 30 2018, accessed at: https://fcw.com/articles/2018/04/30/kaspersky-lawsuit-bod-reason.aspx.
[18] US House of Representatives (2012), Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, US House of Representatives Report, accessed at: https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.
[19] Weisman, S. (2008), U.S. Security Concerns Block China's 3Com Deal, New York Times, February 21, 2008.
[20] ECIPE (2018), Digital Trade Estimates; Ferracane, Lee-Makiyama (2017), China and its non-negotiable rationales, ECIPE.

operators that are all state-owned enterprises (SOEs).[21] Foreign IT products and investment are restricted above level three, which is the level at which damage to the information system would cause harm to national security. While China's hard law restricts foreign vendors, its state-owned operators have always purchased European equipment for both core and RAN networks. However, a political incident 2013 limited the market shares of European suppliers were artificially capped at 33% in 2013.[22]

In addition, the Cybersecurity Law (coming into force on 1 November 2018) foresee the rollout of "secure and controllable" internet infrastructure, through screening of purchases, investments, or supply chains; private firms can also be forced to surrender source codes and intellectual property. The official Xinhua news agency reported that the new law (signed personally by President Xi Jinping) would establish "mechanisms to censor items that have or may have an impact on national security, including foreign investment, particular materials and key technologies".[23]

These security measures do not only point to an extreme reticence to foreign participation in the telecom sector. While there are cases of hard laws in the US, China and Taiwan, Hard laws do not fit all constitutional structures, or present considerable legislative or diplomatic inconveniences for most countries, including Australia, Canada, Japan or the European countries. Meanwhile, a soft law approach based on pre-existing screening or authorisation mechanisms that often already exist, and decisions like the TSSR review clarifies the criteria for approvals for issuing approvals under 5G, and such decisions can be taken on a case by case basis as administrative or commercial decisions.

Such legislative discretion inevitably leaves leeway for political discretion. Discretion in turn always opens the door for politicisation. China's soft law approaches where MLPS and administrative requirements under the new Cyber Security Law clearly incentivise import substitution policies. China already has two national policies – "Made in China 2025" and National IT Development Strategy – aiming at decreases the country's dependency on imports and non-domestic innovations.[24]

However, even in the case of China, politicisation is not intense enough to ban foreign vendors entirely. Also, as the French vendors (Alcatel-Lucent, which since left the market through a merger) focused on fixed network equipment, China is the only country amongst the examples that still has its own domestic production of 5G equipment to protect. Any politicisation has its cause in non-commercial rationale, even in the case of China.[25]

THIRD ISSUE: GOVERNMENT COERCION AGAINST TECHNOLOGY VENDORS

The third question raised by Australia's review concerns "extrajudicial directions" from a foreign government, where firms can be coerced to cooperate with its intelligence activities.

Breaking into a well-protected telecom network and laying out the backdoors required to grant persistent access and extract information can require years of preparation, planning, and reconnaissance. Indeed, only well-resourced actors – such as national governments –are one of the few institutions with the ability, expertise and resources to successfully perform such stealthy operations, either by using their own resources, or by possibly coercing domestic technology companies to cooperate, and there are two examples of such tie-ups.

[21] Ahrens, N. (2012), National Security and China's Information Security Standards, CSIS Report, accessed at: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/121108_Ahrens_NationalSecurityChina_web.pdf.
[22] Mozur, P. (2013), China Mobile Looks to European Suppliers, 22 August, 2013.
[23] Xinhua (2015), Xinhua Insight: China adopts new law on national security, July 1, 2015.
[24] See State Council of the P.R.C., Made in China 2025, accessed at: http://english.gov.cn/2016special/madeinchina2025/.
[25] supra note 20.

China is alleged to be the host country of several advanced persistent threat (APT) groups,[26] some which operate with commercial companies that act as fronts.[27] However, the US National Security Agency (NSA) made use of commercial over-the-top (OTT) services to eavesdrop on information and several NSA programs (including PRISM, BLARNEY and Xkeyscore) utilised their access to US-owned social media, streaming and email services to collect intelligence.

Both China and the US have recently changed their intelligence laws, that warrant a closer examination. The new National Intelligence Law of China sets a precedent by requiring its citizens and businesses to collaborate with its security agencies (article 14) under punitive sanctions.[28] This obligation includes the necessary methods to carry out intelligence work overseas "according to the law" (article 10). In addition, the law gives Chinese intelligence agencies the power to read or collect relevant files (article 16), using "communication tools" and organisations (article 17). The law clearly provides the legal basis for Chinese intelligence agencies to compel Chinese entities to support national intelligence-gathering activities under punitive sanctions.

The recent changes in US law reaffirm the broad powers of access to information held by US entities abroad. For one, the Foreign Intelligence Surveillance Act (FISA) allows US intelligence agencies to access personal data of foreigners either with or without a court order.[29] Additionally, the recent Clarifying Overseas Use of Data (CLOUD) Act allows law enforcement officials at any level (from local police to federal agents) to compel US firms (albeit with certain safeguards) to turn over the data of its own nationals regardless of where it is stored.[30] Such a broad scope has been an element of concern for countries trying to protect the privacy of their citizens and commercial interests.

Several governments have both incentives and capability to engage in cyber espionage – and other countries, including Vietnam and the UK have policies which require firms to surrender company data upon request. These requests can go as far as requiring that technical changes be made to software and systems, including the installation of backdoors to be used at their discretion. However, such provisions are carefully confined within their own territories.[31] Thus, the US and China represent two unique cases where government coercion against private entities have been codified into hard law – and with extraterritorial effect. While the US is the leading global supplier of cloud services, China is where design, development and manufacturing of 5G network equipment take place and is exported.

All governments spy – and they also enact cybersecurity or privacy laws to stop other governments from spying. This circular behaviour merely shows that some governments are simply not in a position to trust each other – and will not be for a foreseeable future. This distrust (which is deeply rooted in geopolitics) renders the question whether some commercial vendors are trustworthy completely irrelevant. It is simply not the conduct of the vendors that are under assessment, but the actions of their host governments and the judiciary system that provide oversight over them.

[26] "APT" is a label used by cybersecurity experts to describe cyber espionage groups, which are typically state-sponsored. For more on APT1 and APT3, please see Mandiant (2013), APT1, accessed at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf and Insikt Group (2017), Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3, Recorded Future, May 17, 2017, accessed at: https://www.recordedfuture.com/chinese-mss-behind-apt3/.

[27] ibid.

[28] Standing Committee of the National People's Congress (2018), National Intelligence Law of P.R.C., [English translations from LexisNexis].

[29] US Congress (1978), Foreign Intelligence Surveillance Act, Accessed at: https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf.

[30] Houser, K. (2018), Everything You Need to Know About the CLOUD Act, Futurism, March 26, 2018, accessed at: https://futurism.com/everything-need-know-cloud-act/.

[31] National Assembly of Vietnam (2013), Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information, accessed at: https://www.vnnic.vn/sites/default/files/vanban/Decree%20No72-2013-ND-CP.PDF; UK's Investigatory Powers Act of 2016 mandates that governments can issue "technical capacity notices", see also Hern, A. (2017), UK Government Can Force Encryption Removal, but Fears Losing, Experts Say, The Guardian, March 29, 2017, accessed at: https://www.theguardian.com/technology/2017/mar/29/uk-government-encryption-whatsapp-investigatory-powers-act.

THE TRUST IN CHINESE VENDORS

Inevitably, the case of national security screening comes down to the standing of two Chinese vendors, ZTE and Huawei. However, the TSSR decision builds on the assumption that some technology firms can be coerced in their home jurisdictions. Meanwhile, another government, the UK, has publicised details on Chinese vendors on whether this coercion actually takes place.

However, ZTE and Huawei are also two very different firms. ZTE, initially founded as Zhongxing Semiconductor in 1985, later changing its name to Zhongxing New Telecommunications Equipment and restructured as a private market operating SOE. It has gone through several public stock offerings, listed on the Shenzhen stock exchange in 1997 and in Hong Kong in December 2004. In April 2018, the UK cybersecurity watchdog, the National Cyber Security Centre (NCSC), warned the country's telecommunications sector against using equipment or services provided by Chinese firm ZTE.[32] In a letter, the NCSC's technical director Ian Levy warned that "the use of ZTE equipment or services within existing telecommunications infrastructure would present a risk to UK national security that could not be mitigated effectively or practicably". In fact, backdoors have been found in ZTE devices.[33]

Furthermore, the letter went on to explain that "adding in new equipment and services from another Chinese supplier would render [the NCSC's] existing mitigations ineffective." The "another Chinese supplier" is in this case is Huawei, which (unlike ZTE) already supplies a significant amount of equipment to the UK network.

While ZTE is a self-admitted SOE, Huawei's ownership is never detailed in public, beyond its status as a wholly employee-owned entity. China subjects most sectors to market forces, which means that a private enterprise like Huawei can prevail over less commercially successful SOEs like ZTE or Shanghai Bell in domestic markets and are allowed to emerge as the state's national champion.[34]

The UK market is also open to Huawei, but under the condition that its products undergo testing in the UK's Huawei Cyber Security Evaluation Centre (HCSEC), which was specifically established for them in 2010.[35] There is also much ado over Huawei's founder Ren Zhenghfei's background in the People's Liberalisation Army. However, in 1982 (when Ren was discharged from the army), the PLA had 5 million employees in various business enterprises in relatively mundane civilian businesses like textile mills, printing or hotels, that accounted for up to 8% of China's GDP.[36]

Such criticism brings little to the discussion. To use an analogy, millions of men and women served as conscripts in European military services (including one of the authors of this report) without incriminating their future employers. Such senseless accusations have allowed the Chinese government to deflect any criticism as West's ignorance about its economy. Moreover, it diverted the debate away from more serious questions on how governments take an active role in overseeing the operations of technology companies.[37]

[32] Fildes, N. (2018), Cybersecurity watchdog warns UK telcos against using equipment from Chinese supplier ZTE, Financial Times, April 16 2018, accessed at: https://www.ft.com/content/24c998b4-416c-11e8-803a-295c97e6fd0b
[33] Michael Lee, Backdoor Found in ZTE Android Phones, ZDNet, May 15, 2012, accessed at: http://www.zdnet.com/article/backdoor-found-in-zte-android-phones/.
[34] Aherns, China's Competitiveness: Case Study: Huawei 2–9 (2013).
[35] Milmo, C. (2013), Are Huawei the enemy within? GCHQ is tightening its supervision of the giant Chinese technology company's UK testing centre, The Independent, December 18, 2013, accessed at: http://www.independent.co.uk/news/uk/home-news/are-huawei-the-enemy-within-gchq-is-tightening-its-supervision-of-the-giant-chinese-technology-9013869.html.
[36] Cheung, T. M., Tai, M. C. (2001), China's Entrepreneurial Army, OUP; also Wu, H. X. (2014), China's Growth and Productivity Performance Debate Revisited - Accounting for China's Sources of Growth with a New Data Set, EPWP 14-01, accessed at: https://www.conference-board.org/pdf_free/workingpapers/EPWP1401.pdf.
[37] Wu (2016).

Although UKNCSC letter makes no reference to Huawei, it points to the findings of 2018 NCSC Annual report, which likely to form the base of its opinion.[38] For one, the report mentions problems relating to binary equivalence, a requirement stipulating that all equipment screened by the HCSEC must have repeatable builds, and therefore be identical to those sold on the market and integrated within the networks of the commercial operators. The NCSC's claim in plain speak means the software tested does not match the software used in the network, In addition, Huawei's management of third-party components, wherein the NCSC found that software critical to security used in a variety of products "was not subject to sufficient control."[39] In some instances, Huawei's long-term support of certain third party software was deemed to be insufficient, given the third parties in question are scheduled to stop providing security patches for the software in question by 2020, leaving potential backdoors unaddressed.

Based on these findings, the report goes on to state that "technical issues [...] identified in Huawei's engineering" constitute "new risks in the UK telecommunications networks." As a result, the NCSC is less confident that the HCSEC "can provide long-term technical assurance of sufficient scope and quality around Huawei in the UK", especially given the infrastructural changes that 5G will soon bring to UK networks. In this respect, the HCSEC report and the NCSC letter point to a shift towards a stricter approach to cybersecurity and investment screening.

The UK government also states that a similar screening that it conducts on Huawei products and services be ineffective with regards to ZTE – confirming the Chinse vendors are very different entities, of different origins, with different degree of internationalisation. Therefore, they have different level of willingness to cooperate with the authorities. Nonetheless, the bottom line of the Australian TSSR decision is how both operate under the same laws and obligations under Chinese law.

CONCLUSIONS

In every respect, the 5G deployment is culminating to a "Snowden" moment for China: A number of governments are unleashing policy responses against China over what they perceive as a lack of assurances that extraterritorial intelligence activities will not be taking place on their territory by coercing technology companies.

What was evident for online services in the NSA revelations in 2013 – and for 5G equipment now – is how the credibility of commercial vendors is not just a function of their behaviour, but a matter of their legal obligation at home to cooperate with their home governments.

The decision by the Australian government is builds on the analysis that the launch of 5G fundamentally changes the architecture, which renders distinctions between core networks and RAN (and today's security safeguards), quite obsolete. Moreover, 5G changes how the networks are used, with large-scale and critical machine communication that contain more corporate information, trade secrets and critical applications. 5G will be critical to government function and corporations, as well as individuals and the society as a whole.

As Australia, or any of the countries currently deciding to restrict Chinese vendors, manufacture any 5G equipment, the case is something far more ominous than the usual protectionism. These countries have no domestic producers to protect.

The tensions have more existential causes, as the old "West" seeks to maintain status quo, while China seeks to revise that order. Also, China has much less conventional strategic resources at its disposal than the US and is likely to make use of "unconventional" resources. Such instrumentation includes cyber warfare or its ability to redirect the economic resources in a dirigiste system.

[38] Huawei Cyber Security Evaluation Centre Oversight Board (2018), Annual Report, accessed at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf.
[39] Ibid.

It bears reminding that this distrust is reciprocal: China also perceives its risks in network security to be of such magnitude that they justify the most safeguards in the world. Rather than a risk-based or case-by-case approach to network security, China carves out the broadest possible safety margins in its procurement laws. Central policies in China are often black and white, with positive lists that names explicitly a few permitted firms, as more subjective and risk-based criteria may not be uniformly applied throughout all the provinces or branches of government.

In other words, today's tensions will remain. As a result, technology vendors will never be able to present convincing evidence of their innocence. Neither will governments present any "smoking gun" evidence of state espionage, as it might immediately turn a cold war into a hot one.

As a consequence, national security screenings and restrictions will remain in force by all parties of both East and West – and be expanded further. In the coming years, not just the products but a vendor's relationship with other governments (through ownership and other legal or political obligations) is inevitably going to be scrutinised. In effect, future security screenings will assess other governments – i.e. the ability of a foreign state to exercise control over its vendors, rather than assess the vendors themselves.

Such philosophy is also integrated into some legal frameworks, such as the US reforms of Cfius,[40] or the EU's proposed new FDI screening framework.[41] The EU Best Practice on sanctions names a variety of practices as indicators of state control, including vulnerability to coercion due to a financial dependency from state funding or subsidies.[42] Governments will routinely check vendors for legal obligations to foreign governments, or their ability to maintain the confidentiality of communications in their networks.

With the view of such developments in Australia, Europe and Asia, it only the government that could assist its private market players from avoid being locked out from foreign markets. This is particularly true for China on the 5G market. Reforming the national intelligence law will be a first step to change the perceptions about Chinese businesses, as well as the Chinese market governance model, in the West.

[40] US Treasury (2013), Federal Register, 73(236), December 8, 2008, accessed at: https://www.treasury.gov/resource-center/international/foreign-investment/Documents/CFIUSGuidance.pdf.
[41] European Commission (2017), Proposal for a Regulation of the European Parliament and the Council Establishing a Framework for Screening of Foreign Direct Investments into the European Union, accessed at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:487:FIN.
[42] European Council (2015), Restrictive Measures, Foreign Relations Counsellors Working Party, accessed at: http://data.consilium.europa.eu/doc/document/ST-10254-2015-INIT/en/pdf.

BIBLIOGRAPHY

Ahrens, N. (2012), *National Security and China's Information Security Standards*, CSIS Report, accessed at: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/121108_Ahrens_NationalSecurityChina_web.pdf.

Australian Government (2018), *Australian Security Intelligence Organisation Act 1979*, accessed at: https://www.legislation.gov.au/Details/C2013C00437.

Article 19 (2017), *Thailand: Computer Crime Act, Legal Analysis*, accessed at: https://www.article19.org/data/files/medialibrary/38615/Analysis-Thailand-Computer-Crime-Act-31-Jan-17.pdf.

Burton, G. (2018), *US intelligence in private briefings against Huawei and ZTE*, Computing, June 25, 2018 accessed at: https://www.computing.co.uk/ctg/news/3034723/us-intelligence-in-private-briefings-against-huawei-and-zte .

China Law Translate (2016), *2016 Cybersecurity Law*, accessed at: https://www.chinalawtranslate.com/cybersecuritylaw/?lang=en.

Ersin, B. T. & Solak, A. U. (2016), *Turkey Completes Final Step In Approving Data Protection Legislation, Mondaq*, April 7, 2016, accessed at: http://www.mondaq.com/turkey/x/480822/Data+Protection+Privacy/Turkey+Completes+Final+Step+in+Approving+Data+Protection+Legislation.

European Centre for International Political Economy (2018), *Digital Trade Estimates Database*, accessed at: http://ecipe.org/dte/database/.

Fifield, M. (2018), *Government Provides 5G Security Guidance To Australian Carriers, Ministers for Communications and the Arts*, Joint Press Release, August 23 2018, accessed at: https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers.

Fildes, N. (2018), *Cyber security watchdog warns UK telcos against using equipment from Chinese supplier ZTE*, Financial Times, April 16 2018, accessed at: https://www.ft.com/content/24c998b4-416c-11e8-803a-295c97e6fd0b.

Global Trade Alert (2013), *United States of America: Procurement of Chinese IT equipment contingent on FBI certification*, accessed at: https://www.globaltradealert.org/state-act/4340.

Ha, B. (2018), *Vietnam says cybersecurity law needed to ensure national security*, VN Express, June 12 2018, accessed at: https://e.vnexpress.net/news/news/vietnam-says-cybersecurity-law-needed-to-ensure-national-security-3762377.html.

Hern, A. (2017), *UK Government Can Force Encryption Removal, but Fears Losing, Experts Say*, The Guardian, March 29, 2017, accessed at: https://www.theguardian.com/technology/2017/mar/29/uk-government-encryption-whatsapp-investigatory-powers-act.

Houser, K. (2018), *Everything You Need to Know About the CLOUD Act*, Futurism, March 26, 2018, accessed at: https://futurism.com/everything-need-know-cloud-act/.

Huawei Cyber Security Evaluation Centre Oversight Board (2018), *Annual Report*, accessed at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf.

India Department of Telecommunications (2010), *Template of the agreement between Internet Service Provider (ISP) and vendor of equipment, product and services Template Letter*, accessed at: http://www.dot.gov.in/isplicense/template-agreement-between-internet-service-provider-isp-and-vendor-equipment-product-and.

Insikt Group (2017), *Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3*, Recorded Future, May 17, 2017, accessed at: https://www.recordedfuture.com/chinese-mss-behind-apt3/.

Invest in China (2001), *Provisions on the Administration of Telecommunications Enterprises with Foreign Investment*, accessed at: http://www.fdi.gov.cn/1800000121_39_2273_0_7.html.

Investment Policy (2013), *Italy Establishes review mechanism for transactions in strategic industries*, May 11, 2012, accessed at: http://investmentpolicyhub.unctad.org/IPM/MeasureDetails?id=443&rgn=&grp=&t=&s=&pg=29&c=&dt=&df=&isSearch=false.

Johnson, D. B. (2018), *More detail on why DHS Banned Kaspersky*, FCW, April 30 2018, accessed at: https://fcw.com/articles/2018/04/30/kaspersky-lawsuit-bod-reason.aspx.

Kaizen (2018), *Taiwan Statute for Investment by Foreign Nationals*, accessed at: http://www.bycpa.com/html/news/20106/1472.html.

Katrenakes, J. (2018), *Trump Signs Bill Banning Government Use of Huawei and ZTE*, The Verge, August 13, 2018, accessed at: https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump.

Knight, B. (2017), *Surveillance: German police ready to hack WhatsApp messages*, DW, July 25 2017, accessed at: http://www.dw.com/en/surveillance-german-police-ready-to-hack-whatsapp-messages/a-39830250.

Lee-Makiyama, H. (2018), *Stealing Thunder*, ECIPE, accessed at: http://ecipe.org//app/uploads/2018/02/ECIPE_Occasional0218_HLM_V7.pdf.

Legislation.gov.uk (2018), *Companies Act 2006*, accessed at: http://www.legislation.gov.uk/ukpga/2006/46/contents.

Legislation.gov.uk (2018), *Enterprise Act 2002*, accessed at: http://www.legislation.gov.uk/ukpga/2002/40/contents.

Mandiant (2013), *APT1*, accessed at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

Marks, J. (2018), *House Passes Bill Expanding DHS' Power to Block Risky Contractors from Government Networks*, Nextgov, September 5, 2018, accessed at: https://www.nextgov.com/cybersecurity/2018/09/house-passes-bill-expanding-dhs-power-block-risky-contractors-government-networks/151012/.

Milmo, C. (2013), *Are Huawei the enemy within? GCHQ is tightening its supervision of the giant Chinese technology company's UK testing centre*, The Independent, December 18, 2013, accessed at: http://www.independent.co.uk/news/uk/home-news/are-huawei-the-enemy-within-gchq-is-tightening-its-supervision-of-the-giant-chinese-technology-9013869.html.

Milton, L. J. (2013), *Foreign Bid for Telecom Carrier Blocked on National security Grounds*, Lexology, accessed at: http://www.lexology.com/library/detail.aspx?g=10e30b5a-3fc4-42d9-a3e2-f30e14353620.

Ministry of Commerce and Industry of India (2014), *Consolidated FDI Policy*, accessed at: http://dipp.nic.in/sites/default/files/FDI_Circular_2014%20%201_0.pdf.

Ministry of Commerce of People's Republic of China (2011), *Circular of the General Office of the State Council on the Establishment of Security Review System Regarding Merger and Acquisition of Domestic Enterprises by Foreign Investors*, accessed at: http://english.mofcom.gov.cn/article/policyrelease/aaa/201103/20110307430493.shtml.

National Assembly of France (2018), *Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, accessed at: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006053177.

National Assembly of France (2018), *LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*, accessed at: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&date.

National Assembly of Vietnam (2013), *Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information*, accessed at: https://www.vnnic.vn/sites/default/files/vanban/Decree%20No72-2013-ND-CP.PDF.

Needham, K. (2018), *Australian government made 'wrong decision' over 5G ban, says China*, Sydney Morning Herald, August 24, 2018, accessed at: https://www.smh.com.au/world/asia/china-australia-government-back-stabbers-over-huawei-decision-20180824-p4zzg0.html.

Negishi, M. (2018), *Japan Scrutinizes China's Huawei, ZTE Over Spying Fears*, Wall Street Journal, August 30, 2018, accessed at: https://www.wsj.com/articles/japan-scrutinizes-chinas-huawei-zte-over-spying-fears-1535630378.

Nelson-Daley, R. (2016), *Costa Rica: Data Protection Amendments Reflect Country's "Digital Maturity"*, DataGuidance, December 15, 2016, accessed at: https://www.dataguidance.com/1947-2/.

Panda. A. (2015), *The Truth About China's New National Security Law*, The Diplomat. July 1 2015, accessed at: https://thediplomat.com/2015/07/the-truth-about-chinas-new-national-security-law/.

Parliament of Canada (2018), *Statutes of Canada 2013: Bill C-60*, accessed at: http://www.parl.ca/DocumentViewer/en/41-1/bill/C-60/royal-assent.

Poddar, D. (2013), *Foreign investment regulation in Australia, Clifford Chance*, May 16, 2013, accessed at: https://www.cliffordchance.com/briefings/2013/05/foreign_investmentregulationinaustralia.html.

Public Works and Government Services Canada (2018), *Security Agreements Template*, accessed at: http://ssi-iss.tpsgc-pwgsc.gc.ca/pdf/msi-ism/anx-3g-eng.pdf.

Quartz (2017), *What you need to know about China's intelligence law that takes effect today*, June 28, 2017, accessed at: https://qz.com/1016531/what-you-need-to-know-about-chinas-intelligence-law-that-takes-effect-today/.

Refworld (2018), *China: State Security Law of 1993*, accessed at: http://www.refworld.org/docid/3ae6b4dd0.html.

Reuters (2018), *SAP, Symantec, and McAfee let Russia probe software widely used by U.S. government*, VentureBeat, January 25, 2018, accessed at: https://venturebeat.com/2018/01/25/sap-symantec-and-mcafee-let-russia-probe-software-widely-used-by-u-s-government/.

Rogers, M. & Ruppersberger, D. (2012), *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, US House of Representatives Report, accessed at: https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

Roudik, P. (2016), *Russia: New Electronic Surveillance Rules, Library of Congress*, July 18, 2016, accessed at: http://www.loc.gov/law/foreign-news/article/russia-new-electronic-surveillance-rules/.

Segal, A. (2016), *China, Encryption Policy, and International Influence*, Hoover Institution, Series Paper No. 1610, accessed at: https://www.hoover.org/sites/default/files/research/docs/segal_webreadypdf_updatedfinal.pdf.

Smyth, J. (2018), *Proposed Huawei ban seen hitting Australian 5G push*. Financial Times, August 13 2018, accessed at: https://www.ft.com/content/5a22be84-9b92-11e8-9702-5946bae86e6d.

Thomson, A. (2015), *French government weighs in on proposed Dailymotion sale to PCCW*, Financial Times, April 1, 2015, accessed at: https://www.ft.com/content/b103fd26-d877-11e4-ba53-00144feab7de#axzz3d7yYWxS0.

UNCTAD (2015), *Investment Monitor*, 13, January 2015, accessed at: http://unctad.org/en/PublicationsLibrary/webdiaepcb2015d13_en.pdf.

US Congress (1978), *Foreign Intelligence Surveillance Act*, Accessed at: https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf.

US Congress (2018), *Defending U.S. Government Communications Act*, accessed at: https://www.congress.gov/115/bills/hr4747/BILLS-115hr4747ih.pdf.

US Department of State (2014), *Investment Climate Statement Greece*, accessed at: https://www.state.gov/e/eb/rls/othr/ics/2014/228812.htm/.

US Treasury (2013), *Federal Register*, 73(236), December 8, 2008, accessed at: https://www.treasury.gov/resource-center/international/foreign-investment/Documents/CFIUSGuidance.pdf.