

アジアの地域統合とグローバルエコノミー：経済安全保障への布石

講演 / Presentation

Christopher FINDLAY

**Honorary Professor,
Crawford School of Public Policy, ANU**

November 21, 2019

The background of the slide features abstract, overlapping green geometric shapes, primarily triangles and polygons, in various shades of green, creating a modern and dynamic visual effect.

The case of 5G technology

Christopher Findlay

Presentation to the RIETI-ANU Symposium on
'Asian Integration and the Global Economy: Economics of Geopolitics'

21 November 2019

Outline

5G and why it matters

China, Huawei and the US

Current Threats and Responses

Implementation and Resolution

Options in a Cooperative Environment

Why 5G matters – it is ‘transformative’



High speed and capacity (first part, can be built on 4G networks)

Download more data, eg video at better quality

- Driven by growth of smartphones, leading to a very large number of devices with better screens



Low latency [or low lag] and high reliability (second part, big investment)

Set up even more devices spread over a large area in constant communication with each other

- critical for autonomous vehicles, factory automation, virtual a reality



Innovation

The new technology will thereby support the development of new things and ways of doing things that have not yet been imagined

China's first mover strategy

- No country has given 5G more attention and priority than China.
- Advantages of making great progress include
 - Demonstrating how to build successful a 'standalone' 5G network (which offers all the IOT dimensions), rather than a first-stage add-on to 4G
 - Demonstrating how the China model ('the low frequency approach') works, to other customer countries in the rest of the world
 - And a genuine advantage in exporting to other members of the BRI along the 'digital silk road'
 - Getting the system working will generate lots of data (another China advantage in any case) that will help drive innovation in new applications, the creation of more benefits and a faster return on the set up of the network

China's choice of 'low frequency'

- Mobile networks transport information at various frequencies. However, in most countries, the majority of low-frequency signals are used for things like radio, TV, satellite communications and military functions. For 5G to deliver the ultrafast data speeds promise, it will require a wide spectrum of unused frequencies that are free from competing signals. For this reason, some countries—including the US—are opting to rely more heavily on higher frequencies.
- High-frequency signals have downsides, however. They are more susceptible to interference from rain, fog, buildings, and trees. They also can't travel as far, so more antennas will be needed to maintain a signal. Instead of mounting large antennas on tall towers, wireless carriers will mount clusters of small antennas on poles and rooftops. The increased number of antennas will make switching to 5G costly for service providers.
- These higher costs could be difficult for telecom companies to swallow, especially in the short term. "The seemingly insatiable appetite for mobile connectivity has a downside for telecoms companies . . . in that it demands massive capital expenditure," argues a report by [The Economist Intelligence Unit](#). "At the same time, increased competition is forcing down prices." The report predicts that these and other pressures will cause total telecoms' revenue in the 60 biggest markets to fall by 2% in 2018, in US dollars terms.
- In order to avoid some of these issues, **China has opted to rely more heavily on lower frequencies for 5G**. China has more bandwidth available than the US when it comes to lower frequencies, according to a report by [Jefferies](#).

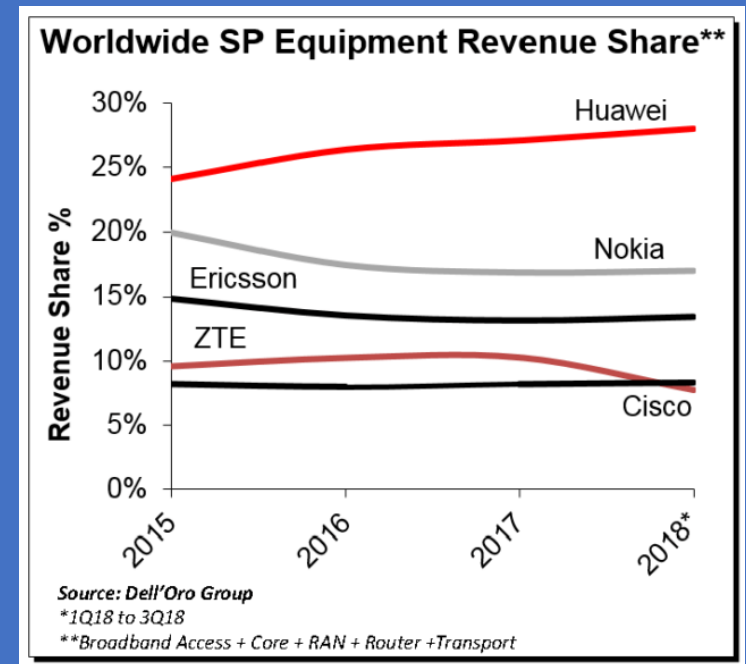
<https://technode.com/2018/03/30/5g/>

Huawei competitiveness

- Competitive pricing, good technology, meets global standards, now offers 'end to end' services
- Based on R&D (estimates [here](#))
 - so that its network equipment embodies standards which are at global level (and which drive standard setting at that level)
- Outcome is that it accounts for 55-60% of the China market for 4G equipment, likely higher in 5G given its strengths in radio access, cloud services and database software
- There are reports that globally its market share is highest, most recent estimate is 28 percent of the telecom equipment market

Equipment categories

- Broadband Access and Home Networking
- Carrier IP Telephony
- Microwave Transmission & Mobile Backhaul
- Mobile Radio Access Network (RAN)
- Optical Transport
- Router & Carrier Ethernet Switch
- Wireless Packet Core



<https://www.delloro.com/key-takeaways-telecom-equipment-market-3q-2018/>

The second layer



Huawei is regarded as a highly innovative organisation with interesting management practices, plus a positive reputation in the industry



But in policy circles in the rest of the world there are various concerns about elements of Huawei history

Huawei business practices, particularly its history in dispute with CISCO – see [here](#)

Sanctions issues, and concerns about supply of equipment to rogue states, linked to the arrest of CFO Meng Wanzhou

Origins of the company, its military connections, its access to government finance in its foundations, and lack transparency about corporate structure and governance, even the lack of public profile of CEO Ren Zhengfei



Plus the rising concern about cyber intrusion

Eg the Google intrusions in 2010, which was linked to Chinese hackers

Plus the attention given to the National Intelligence Law in China

National Intelligence Law of China (2017)

- *'Any **organisation and citizen** shall, in accordance with the **law**, support, provide assistance, and cooperate in **national intelligence work**, and guard the secrecy of any national intelligence work that they are aware of'*
- But also if Huawei was regarded as primarily providing this function its international markets would not be sustainable.
- Huawei's challenge is to prove this 'in the negative', to show that it is not the case.

Decline in US competitiveness in 5G equipment

- The context is also the decline of the US firms in the mobile technology markets, highlighting the concerns of the US military and its exposure to providers who are asserted to be subject to direction by their governments
 - 'US companies are seeking to provide 5G services but these reports indicate that they are not providers of the critical equipment.'
- 'Barely any U.S. companies manufacture the technology's most critical components. The absence of a major U.S. alternative to foreign suppliers of 5G networking equipment underscores the growing dominance of Huawei,And it throws into sharp relief the years-long retreat by U.S. firms from that market. Carriers such as [Sprint](#) and Verizon have moved swiftly to launch 5G services for consumers. But the wireless networking gear the industry relies on still comes from foreign suppliers: four companies, Sweden's Ericsson, Finland's Nokia and China's Huawei and ZTE, account for two-thirds of the global market for telecom equipment, according to analyst estimates. Some U.S. technology giants such as Cisco sell switches and routers that reside in the innermost parts of a carrier's network. But despite its size, Cisco doesn't compete in the market for "radio access," or the wireless infrastructure that allows cell sites to connect with smartphones and other mobile devices.'
- See the following for more details of the history of this sector and the decline of providers like Lucent and Motorola
- https://www.washingtonpost.com/technology/2019/04/10/us-spat-with-huawei-explained/?noredirect=on&utm_term=.8a3dc2f7037d

So what is the threat associated with 5G



System failure

More data moving about so it is more difficult to identify 'bad data'

Lot of activity will be in the cloud so the 'attack surface' (or opportunity) is greater

Lot of devices connected so more potential points of connection for 'bad devices'

- Rising dependence on these systems, so the scale of the impact of a bad event is much greater



Privacy and confidentiality

'Back doors' in switches and the use of triggers to capture data involving loss of privacy, loss of valuable information



Defense

Military systems use private telecom network, so there is a concern about a 'big red button' risk impeding operations. Or some sort of trigger to deflect information in the context of a military operation.

US response

- The US has sought to
 - Stop US firms selling to Huawei and others (the application of the entity list)
 - Stop US firms buying from Huawei (the Executive Order related to ICT chain security)

The Entity List

- **AGENCY:** Bureau of Industry and Security, Commerce.
- **SUMMARY:**
 - In this rule, the Bureau of Industry and Security (BIS) amends the Export Administration Regulations (EAR) by adding Huawei Technologies Co., Ltd. (Huawei) to the Entity List. The U.S. Government has determined that there is reasonable cause to believe that Huawei has been involved in activities contrary to the national security or foreign policy interests of the United States.
 - BIS is also adding non-U.S. affiliates of Huawei to the Entity List because those affiliates pose a significant risk of involvement in activities contrary to the national security or foreign policy interests of the United States. Huawei will be listed on the Entity List under the destination of China. This final rule also adds to the Entity List sixty-eight non-U.S. affiliates of Huawei located in twenty-six destinations
- **Background**
 - The Entity List (Supplement No. 4 to part 744) identifies entities reasonably believed to be involved, or pose a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States. The Export Administration Regulations (EAR) (15 CFR, subchapter C, parts 730-774) imposes additional license requirements on, and limits the availability of most license exceptions for exports, reexports, and transfers (in-country) to, listed entities. The license review policy for each listed entity is identified in the “License review policy” column on the Entity List, and the impact on the availability of license exceptions is described in the relevant **Federal Register** notice adding entities to the Entity List.

Entity List – temporary licenses

- When the ban was imposed, temporary general licenses (to sell to Huawei) were made available, they expired on 19 November but they are expected to be extended for the third time
- Apparently business pressure against a ban on selling to Huawei has been intense – discussions are continuing on specific licenses which might be granted, responding to ‘more than 200 requests’
- Others have sought to rely on exemptions – eg no constraint if a piece of technology has less than 25% of its origins in the US – others may be selling via third countries. The outcome of the ban may therefore be higher transactions costs.

Executive Order

- The EO instructed the Commerce Department to ban purchases when ‘the transaction involves information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary’
- Commerce (via its Bureau of Industry and Security (BIS)) was given 150 days to come up with the regulations on implementation – the deadline would have been 12 October – they still have not been seen.
 - The idea is that Commerce release regulations to implement the purchase ban would ‘cut across’ the trade negotiations between the US and China – the US at least seeks to coordinate their application with the negotiations.
- Trump announced on 11 October that China and the US had reached an initial agreement on a trade deal.
 - Some commentators have said that there is ‘not a lot of daylight between’ national security and trade policy, with respect to these regulations.
- Sources of the delay include – the links to the trade negotiations, differences of opinion on how to define the task and how busy is the Bureau
 - The regulations may be written to apply case by case - see below on risk management
 - That also opens the scope for China to make a deal with the US on their application
 - But industry sources are concerned that using the regulations as bargaining chips ‘undermines’ the regulations (adds to uncertainty as well).

Related developments

- Meanwhile the FCC has proposed to stop rural telecoms from using subsidy funds to buy Huawei equipment – this will be confirmed on 19 November. Some reports are that Commerce will release its regulations (in the form of an ‘interim final rule’ at that time as well).
- The following area regarded as responses to the view that China has procured technology ‘illegitimately’.
 - BIS is working on a list of foundational technologies which will be subject to the Export Control Reform Act – expected by the end of the year (building on notice of a list of emerging technologies (14 areas) issued in November 2018)
 - The issue here is how to define technologies that if available to others would affect US security – and how to deal with technologies which anyway China could buy elsewhere.
 - BIS has published an ‘interim rule’ which expanded the jurisdiction of the (inter-agency) [Committee on Foreign Investment](#) as part of the implementation of the Foreign Investment Risk Review Modernization Act
- Other reports are that the US is seeking to subsidise Huawei’s European competitors.

Big costs if the bans proceed, including for the US

- In the US
 - In the short term
 - lower sales of chips, less profit, less R&D investment: some US firms are highly reliant on Huawei business
 - In the long term,
 - Creates a perception of political risk in purchasing US inputs including Google services,
 - Adds to the reluctance to place R&D activities in the US, and the US runs the risk of being 'blindsided' by the next round of innovation
 - Ends the position of the US oligopolists in the chip design business and cede ground to competitors in other areas
 - Reduces the number of competitors in the global markets, drive up prices to consumers
 - Disconnects US from Asian-China linked ICT supply chains (sales and purchases from)
- In China
 - more difficult for those in China in favour of integration with world markets to make their case, lack of trust in world markets.
- Overall, there is a risk of a 'digital iron curtain' (see below on standards)
 - though note company to company cooperation apparently continues

A tweet by Donald Trump has raised interest in the notion of 6G, and that US strategy may be to 'jump' to that and in a more self reliant manner, so the burden of lack of access to some 5G capability in the shorter term is lessened. However, what 6G actually means is not yet clear, other than a better version of 5G. And the time lines are long (2030). See the assessment here:

<https://www.techinasia.com/forget-5g-china-working-6g>

And here

https://www.washingtonpost.com/technology/2019/02/21/trump-says-he-wants-g-even-g-wireless-tech-what-is-g/?utm_term=.ad50a794997f

@realDonaldTrump

I want 5G, and even 6G, technology in the United States as soon as possible. It is far more powerful, faster, and smarter than the current standard. American companies must step up their efforts, or get left behind. There is no reason that we should be lagging behind on..... something that is so obviously the future. I want the United States to win through competition, not by blocking out currently more advanced technologies. We must always be the leader in everything we do, especially when it comes to the very exciting world of technology!


11:25 PM - Feb 21, 2019

Of interest is the reference to competition in this tweet, which is at odds with recent events. See also the comment at <http://fortune.com/2019/02/21/trump-twitter-5g-6g/>

China views however are positive:

'5G has three application scenarios: large bandwidth, low latency, and wide connection – I think 6G can achieve better application in all three scenarios': Su Xin, head of 5G technology working group at China's Ministry of Industry and Information Technology

Standard setting process

- 
- The process is that the ITU lays out components of the system and creates a list of standards.
 - Meeting some standards may require access to a patented technology (SEP)
 - Companies present their technologies to meet the standard, and the best technology wins in a merit based system: if selected they receive a royalty as others incorporate their technology into components that meet the standard.
 - Competitors from Europe, China, Japan, Korea, US
 - Huawei has a strong reputation in this process in relation to meeting cybersecurity goals, interestingly.
 - Chinese firms may hold about 40% of the 5G SEPs – a big increase over the 4G world, based on R&D and the investments of the first mover strategy.
 - Apparently, therefore, Huawei can get royalty income but may not build the products if the ban proceeds (see below about licensing).
 - However another scenario is that Huawei also gets pushed out of the ITU standards process, causing China to lead the set up of an alternative standards system, and a bifurcated '5G' world, like Japan tried to do earlier with cell phones.



Scenarios

- One scenario is that licensing systems will be put in place, and business allowed to continue but with the threat of a withdrawal in the context of bad behaviour such as
 - the series of issues linked to Huawei previously, were those behaviours to be confirmed
- The analogy is the circlet on the head of the Monkey King

Scenarios (cont.)

- As noted, one scenario is that of the Monkey King's Head Circlet
- Another is a link to the US-China trade negotiations – that the bans have been introduced as chips in the bargaining process
 - Huawei has sought to test this by offering to license its technology to US firms, including reference to being able to change code for security purposes
 - But the responses is that 'bugs' will be hard to find, can always be activated after installation etc. (and Huawei code has been criticised by UK authorities for some weaknesses)

China responses

- Correlated with these decisions by the US are actions by China with respect to the US
 - Issuing the White Paper
http://english.gov.cn/archive/white_paper/2019/06/02/content_281476694892692.htm
 - Drawing up its own list of unreliable entities (not yet released but referred to)
 - Issuing a travel warning for tourists to the US, and for students
 - Demonstrating support for the rare earth sector
 - Providing tax incentives for the technology sector
 - Drafting its own new regulations on procurement for information infrastructure (see below)
- Chinese businesses are also reporting to be building new value chains (eg Japanese suppliers)

Some commentary also links an anti trust action against Ford to this list, but others observe that China is rationally seeking to minimise the cost of its responses and to 'go after' FDI providers may not meet that criterion.

See

<https://www.reuters.com/article/us-china-ford-changan/china-fines-fords-changan-venture-24-million-for-antitrust-violations-idUSKCN1T60AC>

This situation
is difficult to
resolve...since
its about more
than Huawei...

- Difficult to resolve, given the history of the interaction of the parties with respect to other issues – the punch and counter-punch observed to date
 - And because of the debate in the US about if and how to integrate with ‘China’s state-led economy’, in the context of differences in ideology and concerns about the distribution of power.
- The tragedy is that significant success for those who really want to impede China is not likely,
 - Instead China will reorient internally and within the region
 - the legacy of this strategy is likely an outcome which is worse than now, with slower growth for all, including the US
 - though in relative terms the US position may improve

Imagine
another
world..

- Lets at least rehearse a path to resolution that might be found in an environment of cooperation, should that emerge.
 - Cooperation provides more space in which to find a solution, given the sensible application of a 'public policy approach'.
- Starting point: what is China's position on cybersecurity? Does it have parallels with the US? Could it be imagined that in other world these two parties have a lot in common?
 - Yes – China's position does have parallels with the US!



Personal information protection

The Cybersecurity Law clearly states requirements for the collection, use and protection of personal information.



Critical information infrastructure

The Cybersecurity Law frequently mentions the protection of "critical information infrastructure".



Network operators

"Network operators" are the owners and administrators of networks and network service providers. The Cybersecurity Law clarifies operators' security responsibilities.



Preservation of sensitive information

The Cybersecurity Law requires personal information/important data collected or generated in China to be stored domestically.



Certification of security products

Critical cyber equipment and special cybersecurity products can only be sold or provided after receiving security certifications.



Legal liabilities

Enterprises and organisations that violate the Cybersecurity Law may be fined up to RMB1,000,000.

China Cybersecurity Law

KPMG

Chinese Cybersecurity Policy

New draft regulations were issued in May 2019 for a review regime for IT products and services which are linked to national security.

This spells out how 'critical information infrastructure operators' will complete a security review when buying inputs that may affect national security.

There are parallels with, and links with, US concerns: the review mechanism ...

Refers to the protection of the IP of the providers (response to concerns expressed wrt China in the past)

Spells out that a trigger for a review of this type could be the risk of a loss of a lot of personal data and..

...situations of supply disruption, due to 'non-technical factors' such as 'politics, diplomacy and trade' or where providers are funded/controlled by foreign governments


Steps to take

Go to the WTO? No.

- To do so runs the risk of formalising the security grounds for intervention. To ask the WTO to rule on that application and thereby endorse its use diminishes WTO credibility.

A political solution is therefore required which involves actions by the US and by China

- For the US, back off the absolutist approach and adopt the small yard high fence model (globally relevant approach – China's new regulations may be a model!)
- For China, link to SOE reform and manage the perception of interference in corporate operations, make transparent ownership structures, corporate governance, performance expectations
- In cooperation, codify the agreement to take a risk based approach, eg along the lines of Article 19.15 of the USMCA.



‘Higher fences around fewer items’

- Where is the risk, manage it efficiently? This is the public policy approach. More specifically in this context:
 - Consider the components: network core, equipment (like handsets) and the radio communications.
 - Identify the risks at each area: most of the risks are in ‘the core’ (though there is debate in the 5G world of the value of distinguishing the core and the rest)
 - Consider options to manage that risk and choose the most efficient.
 - In some cases, the answer will not be policy but will be process or technology
 - UK and Germany have cybersecurity research centres, to test software (but lots of software to test, difficult to establish equivalence with software in use, resources involved)
 - When the response is a policy intervention, the most efficient will generally also be the least trade distorting.

Robert Gates

- The reference to higher fences around fewer items comes from efforts by former Defense Secretary Robert Gates to reform the export control system - https://www.armscontrol.org/act/2010_05/Exports
- Gates also recalls 'Frederick the Great's famous maxim that he who defends everything, defends nothing....'.



There is a framework – eg USMCA 19.15

Article 19.15: Cybersecurity

The Parties recognize that threats to cybersecurity undermine confidence in digital trade. Accordingly, the Parties shall endeavor to:

- (a) build the capabilities of their national entities responsible for cybersecurity incident response; and
- (b) strengthen existing collaboration mechanisms for cooperating to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks and use those mechanisms to swiftly address cybersecurity incidents, as well as the sharing of information for awareness and best practices.

Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats.

Accordingly, each Party shall endeavor to employ, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.

Working Areas

- Sam Sacks in her testimony to the Senate in March 2019 had more specific suggestions of complementary talking points:
 - **Research:** both parties to recognize the presence of an existing interconnected system in which they have complementary strengths
 - **Regulations:** seek China to 'revise regulations and standards that pressure U.S. companies to disclose source code, encryption keys, and other sensitive information such as proprietary product specifications in exchange for market access.' China has a new FDI law which includes this issue.
 - **Data flows:** The Chinese government is yet to define "personal information" "important data" and "critical information infrastructure": discuss these definitions and ask China to sign onto APEC's Cross Border Privacy Rules System (CBPRs)
 - **IP protection:** China to strengthen its IP protection system and agree to a regime where disputes over information requests can be handled.
 - **AI:** longer term a talking point is the principles for the application of AI processes wrt ethics, privacy and safety

Events in other countries

- Australia has [effectively banned](#) Huawei from participating in the 5G rollout.
 - 'The Government considers that the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference.'
 - As has [New Zealand](#).
- Britain has a research centre (Huawei Cyber Security Evaluation Centre (HCSEC)) that examines risks in Huawei gear: it has found no 'backdoors' but has identified [other weaknesses](#)
- The EU is building a [toolbox of measures](#) for cyber security risks at national and regional levels.
 - Germany apparently plans a regime in which all 5G vendors should prove they are trustworthy.
- In Canada, there is apparently a struggle between one agency which supports a ban and another which believes '[the risks can be mitigated with robust testing and monitoring of equipment](#)'
- A [range of approaches](#) are evident in Southeast Asia, some committing to Huawei (Laos, Cambodia), others not banning but engaging (Singapore, Malaysia, Indonesia) and one banning (Vietnam).