Written evidence submitted by Dr Steven Conlon

The Security of 5G

Submitted by:
Steven Conlon PhD.
VP Corporate Intelligence, Rivada Networks

What are the risks to the UK's 5G infrastructure? How can these be mitigated?

5G technology is in its infancy. Mitigation strategies successful with 4G, such as barring high-risk vendors from network cores, will not be sufficient to secure 5G networks, as 5G architecture will evolve to one very different to 4G. 5G will be heavily reliant on small cell sites and software-based solutions (such as virtualised cores), that if poorly secured and engineered, will pose significant risk. Allowing high-risk vendors who employ poor software development processes (such as those identified in Huawei by the HCSEC) would make it easier for a threat actor to place malicious code or create backdoors into networks, or systems reliant upon 5G.

I refer the committee to Annex C: Mapping Risk Scenarios to Cyberthreats of the ENISA November 2019 '*Threat Landscape for 5G networks*'[1] for a comprehensive of some of the identified threats to network to date. The report identified a taxonomy of nine threat areas:

1. Nefarious activity and abuse that target systems, and network.
2. Eavesdropping, interception or hijacking.
3. Physical attacks that can destroy, alter, expose, disable or steal assets such as infrastructure or hardware.
4. Intentional damage aimed at reducing usefulness.
5. Unintentional damage that reduces usefulness.
6. Failures or malfunctions.
7. Outages resulting in unexpected disruption of service.
8. Sudden accidents or natural disasters.
9. Legal actions of third-parties designed to prohibit actions or compensate for loss.

The report further categorises the threats based on which part of the network is targeted: core, RAN, network virtualised element or generic component. It stresses that there is a real risk that any of these parts could lead to the eavesdropping, interception of data, or the hijacking of parts of the network, amongst other threats.

Testing does not guarantee quality security

The HCSEC 2019 Annual Report[2] is explicitly clear that Huawei technology has security vulnerabilities that are exploitable by a hostile actor and that the source code they examines is not the code running the UK networks. Such vulnerabilities could lead to critical damage so bad neither the carrier or Huawei could repair. Furthermore, the HSCEC has states that "it is

[1] ENISA. 2019, November. Threat Landscape for 5G Networks. Link: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

[2] HCSEC Annual Report 2019. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf

hard to be confident that different deployments of similar Huawei equipment are broadly equivalently secure"[3], meaning that coding standards in one part of Huawei's technology may be deemed secure, but other code, due to a lack of binary equivalency, cannot be guaranteed to be secure. Such sloppy engineering processes lead to vulnerability creep.

A viper in the Huawei nest

A PRC citizen working for Huawei is obliged to engage in espionage on behalf of the CCP, under the 2017 National Intelligence law. As highlighted by the HCSEC report any;

> … attacker [that] has knowledge of these vulnerabilities and sufficient access to exploit them, … may be able to affect the operation of the network, in some cases causing it to cease operating correctly[4].

The Committee should weight the possibility that the CCP could compel a PRC Huawei employee to disclose vulnerabilities, or worse, exploit one.

There is already some evidence that Huawei staff are willing to either follow instructions from, or ingratiate themselves to, the PRC Security Services. Staff members have been linked to espionage allegations with Australian Intelligence reporting in 2018 that Huawei personnel provided "access codes to infiltrate a foreign network"[5]. Huawei denies this. Polish authorities have also detained a Huawei employee on suspicion of espionage, Huawei fired the employee. The case is pending.

Moving to Chinese-manufactured processors

The globalisation of the processor supply chain provides us with a level of assurance that trusted vendors such as Intel mass-produce chips that are used across a broad spectrum of industries, and as such are unlikely to be compromised. In response to the U.S. ban on processors being sold to Huawei the company has begun to manufacture its own. This presents a new threat that cannot be easily mitigated. It is almost impossible to analyse processor coding. With the use of a 'defeat device' a processor could deceive lab tests being conducted (similar to the Volkswagen scandal). If Huawei contracts another PRC company to manufacture the processors it would be unwise to trust this supply chain. Huawei PRC supply chains have previously been compromised with malware..

Network slicing

5G networks can be virtualised in a way that will allows segregated ecosystems to be created or 'sliced' from one major network. It will be possible to have commercial, government and retail slices all operate on one network. Isolating these networks is a cybersecurity challenge, requiring confidence in both the software and hardware. To date the HCSEC has only been able to provide limited assurances that the security risks of Huawei technologies can be managed. In such emerging technologies allowing such a risk across multiple sectors is reckless.

[3] Ibid, page 15.
[4] Ibid, page 20.
[5] ZDNet. 2018, November 5. 'Huawei denies foreign network hack reports'. Link: https://www.zdnet.com/article/huawei-denies-foreign-network-hack-reports/

The economic consequences of vulnerable 5G networks

Telecommunications networks are vital for the operation of the economy, markets and vital government services, such as first responders, hospitals and utilities; making 5G networks a non-kinetic attack vector. Latency sensitive elements of the economy such as stock trading could also be significantly impacted as wireless technologies are utilised by the markets.

Disruption to 5G managed utilities such as power in a particularly cold weather period would see the loss of life. Similarly an impact on network communications for first responders could cause serious social unrest. To mitigate against this the UK should ban all high-risk vendors.

What is the role of government in 5G cyber security?

The government plays an important role in the cybersecurity of 5G networks. Even in countries such as the USA, which traditionally practices light regulation, stringent security requirements are being placed on carriers to protect critical infrastructure.

Supply Chain Security

Supply chain security is an integral part of mitigating risk to business and government. It is highly likely more and more government systems and services will rely on 5G networks. In the USA the Federal Acquisitions Supply Chain Security Act of 2018 covers telecommunications equipment. The Act established a Council tasked with the development of supply chain risk management standards and practices. The Act empowers the exclusion of 5G equipment and parts thereof deemed dangerous or high-risk. The UK should introduce a similar entity, independent of carriers.

US Executive Order (E.O.) 13873, issued in 2019, "Securing the Information and Communications Technology and Services Supply Chain" gave the Federal Government the power to prohibit certain transactions that involve ICT 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 that pose an undue or unacceptable risk to the national security of the United States. It is imperative that the UK government continue to recognise this and introduce similar regulations/legislation.

Ensure quality standards in 5G security

Global 5G standards impact the security of all networks. China currently monopolises the 5G standards bodies. It is vital that the UK works with vendors, academics and international agencies to ensure that policies, standards and procurement strategies that reinforce vendor diversity, transparency and accountability are introduced, including a review of representation at these bodies.

To what degree is it possible to exclude Huawei technology from the most sensitive parts of the UK's 5G network while allowing it to supply peripheral components?

Huawei is **not** an essential provider to a 5G network or part thereof. There are networks globally that do not use Huawei and are more resilient and perform better. Network performance depends on the spectrum used, the terrain, weather conditions and the RF design and architecture deployed, not simply equipment. The concept of 'sensitive parts' of the 5G network is a misnomer, in 5G all parts are sensitive.

Early 5G networks will be built on legacy 4G LTE technologies, but in time this will be replaced as the 5G RAN technologies and network architectures evolve. Risks that have already been identified in 4G technologies will remain for at least 3-5 years in the 5G ecosystem and will require mitigation along with new 5G vulnerabilities, meaning UK 5G networks will rely on heavily patched Huawei technologies.

A 'facts on the ground' strategy has been successfully employed by carriers and Huawei in the UK as a result of the regulatory vacuum on the use of high-risk vendors in 5G. Policy inertia gave carriers license to proceed with Huawei and allows both Huawei and carriers to leverage public resistance to expensive and unpopular corporate bailouts such as a 'rip and replace' program to ensure politicians will not impose such a requirement on carriers. Allowing China to dictate the network policy weakens the UK and emboldens China to attempt regulatory capture in other industries of paramount importance to national security.

What credible alternatives are available to Huawei systems?

Any other vendor is a credible alternative to Huawei.

It is clear from the 2019 HCSEC report that there are serious security and engineering concerns with how Huawei develops its technologies and that Huawei has been unwilling or unable to improve. It paints a 'chaotic' picture of the product development lifecycle of Huawei and appears to indicate that despite oversight by the HCSEC, and its abundance of recommendations, the "character of vulnerabilities has not changed significantly between years, with many vulnerabilities being of high impact"[6].

Is it acceptable to allow a vendor into critical infrastructure where the independent body which reviews its technology warns:

> If an attacker has knowledge of these vulnerabilities and sufficient access to exploit them, they may be able to affect the operation of the network, in some cases causing it to cease operating correctly. Other impacts could include being able to access user traffic or reconfiguration of the network elements[7].

Whilst the NCSC has stated that it does not believe the litany of problems identified by the HCSEC are a result of CCP interference, it is important that the Committee weighs the possibility that a PRC citizen within Huawei, who has knowledge of these vulnerabilities, could share the information to either the PRC security services or one of a number of Chinese state-sponsored hacking groups such as APT40. The APT40 group has recently been exposed hiding behind a UK front company to recruit hackers[8].

Alternative vendors

There are a number of credible, secure and competitive alternatives to Huawei. Ericsson, Nokia and Samsung have significant market share in 5G deployments globally. 5G allows us to move away from traditional network core technologies and use virtualised cores – there are many new, innovative companies globally working in this area.

Despite the propaganda Huawei is not the global leader in 5G, Ericsson is, and Nokia has the largest and arguably higher quality 5G patent portfolio[9] - allowing a company with a low-grade patent portfolio such as Huawei[10] become the dominate player in 5G spells disaster for secure 5G. The CCP politicisation of Huawei has made it simply the most talked about company; this does not make it the best.

---

[6] HCSEC Annual Report 2019. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf - Page 18

[7] Ibid - Page 20

[8] Security Affairs. 2020, January 14. China-linked APT40 group hides behind 13 front companies. Link: https://securityaffairs.co/wordpress/96364/apt/china-linked-apt40-front-companies.html

[9] Mobile World Live, 2020, March 24. Nokia asserts 5G patent leadership. Link: https://www.mobileworldlive.com/featured-content/home-banner/nokia-asserts-5g-patent-leadership/

[10] Nikkei Asian Review, 2019, October 27. Patent king Huawei lags Intel and Qualcomm in quality, study finds. Link: https://asia.nikkei.com/Spotlight/Datawatch/Patent-king-Huawei-lags-Intel-and-Qualcomm-in-quality-study-finds

No 1, does not mean best

Evidence will be presented to the Committee of various 'independent' reports that rank Huawei as number one globally, and this may be true in some parts of the 5G equipment product range. Often these reports only refer to sales for the radio part of a network, the RAN.

For example, baseband capacity refers to the amount of data that can be supported by a single cell site at a specific signal level. Better performance allows a site to cover a larger area or carry a larger amount of traffic. If a vendor offers lower performance, the carrier may compensate by installing additional sites which increases their costs. Likewise, if a vendor has a more extensive portfolio or greater ease of installation, they can offer better customised solutions and lower installation costs, which will have a positive financial impact for the carrier.

In other words, all the indicated benefits derive from Huawei's financial position thanks to PRC support and a protected domestic market[11], rather than actual technological advantages. Carriers use Huawei because they are incentivised to do so through:

- Cheap vendor financing
- Free software
- Free maintenance and support contracts

These practices have allowed Huawei to grow in popularity with carriers who are highly leveraged by debt and has been highlighted since 2012 with evidence presented to the US-China Economic and Security Review Commission[12].

The non-interoperability problem

It is best practice to use multiple vendors for networks. However, interoperability – the ability of one vendor's technology to work with the technology of another is a problem. Huawei's technology allegedly notoriously non-interoperable. This is either by design (so as to ensure dependence) or incompetence. Ericsson and Nokia have been working to resolve the issue of interoperability with Huawei, but according to AT&T's CEO Huawei has no intention of making their equipment interoperable:

> If you have deployed Huawei as your 4G network, Huawei is not allowing interoperability to 5G — meaning if you are 4G, you are stuck with Huawei for 5G[13].

If the UK wants to have sovereign control over its 5G networks and beyond, it is imperative only companies that have shown interoperability good faith be allowed into its networks.

[11] Financial Times. 2020, April 3. China Mobile picks Huawei and ZTE to build its 5G network. Link: https://www.ft.com/content/78f172db-7e02-450a-a1c7-8e9c260c2034?desktop=true&segmentId=7c8f09b9-9b61-4fbb-9430-9208a9e233c8

[12] McCarthy, M. 2012, June 6. Background Material for US-China economic and Security review Commission. Link: https://www.uscc.gov/sites/default/files/6.14.12McCarthy.pdf

[13] Reuters. 2019, March 20. AT&T CEO says China's Huawei hinders carriers from shifting suppliers for 5G. Link: https://www.reuters.com/article/us-att-ceo-huawei-tech/att-ceo-says-chinas-huawei-hinders-carriers-from-shifting-suppliers-for-5g-idUSKCN1R12TX

To what extent was the UK Government's decision on Huawei driven by political rather than technical factors?

A sovereign UK decision made by China

What should have been a sovereign national security decision made by the UK has instead been taken by carriers, Huawei and the CCP and any discussion of a ban on Huawei has been politicalised. This politicisation, coupled with the 'Facts on the Ground' strategy leaves the government with two options:

1. reject Huawei technology, and fund an expensive 'rip and replace' bailout or;
2. accept Huawei 5G despite the HCSEC warning that it would be "difficult to appropriately risk-manage"[14].

Political and economic threats by China on 5G

Over the last 18 months it has become evident that China is willing to threaten economic consequences on countries that ban or significantly limit Huawei's access to 5G deployment contracts. Some of the countries threatened include:

- Australia[15]
- Canada[16]
- Denmark[17]
- Faeroe Islands[18]
- France[19]
- Germany[20]
- India[21]

This further underscores the close political links between the CCP and Huawei. Why is the CCP is so defensive of Huawei? What strategic objective is worth fighting for so aggressively? Is Huawei so critical to the CCP's plan to present an alternative to western democracies, and what role does Huawei play in this political alternative in the digital space? All independent evidence suggests that Huawei is not a normal corporation, and is either heavily influenced by, or under the control of, the CCP. In late 2018 the CCP issued a directive to all Chinese 5G manufacturers banning further announcements, declaring them national security sensitive. For a period of

[14] HCSEC Annual Report 2019. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf

[15] Financial Review. 2019. April 16. China warns Australia that Huawei ban will undermine trade. Link: https://www.afr.com/world/asia/china-warns-australia-s-huawei-ban-will-undermine-trade-20190416-p51egx

[16] CBC, 2019, January 18. Chinese envoy to Canada warns of 'repercussions ' if Ottawa bans Huawei from 5G mobile phone network. Link: https://www.cbc.ca/news/politics/china-envoy-warning-huawei-ban-1.4982601

[17] Forbes, 2019, December 16. China Just Crossed A Dangerous New Line For Huawei: 'There Will Be Consequences'. Link: https://www.forbes.com/sites/zakdoffman/2019/12/16/china-just-crossed-a-dangerous-new-line-for-huawei-there-will-be-consequences/

[18] Associated Press. 2019, December 11. China reportedly threatens tiny Faeroe Islands over Huawei. Link: https://apnews.com/80b5f194806665fea89bc210aa6f8d8a

[19] Forbes, 2020, February 9. China Just Issued Stark New Threats Over Huawei: This Time Nokia And Ericsson Are In Its Sights. Link: https://www.forbes.com/sites/zakdoffman/2020/02/09/china-just-issued-stark-new-threats-over-huawei-this-time-nokia-and-ericsson-are-in-its-sights/#2019d17819d7

[20] Bloomberg, 2019, December 16. China Threatens Retaliation Should Germany Ban Huawei 5G. Link: https://www.bloomberg.com/news/articles/2019-12-14/china-threatens-germany-with-retaliation-if-huawei-5g-is-banned

[21] Taipei Times. 2019, August 8. China threatens retaliation if India bans Huawei. Link: http://www.taipeitimes.com/News/front/archives/2019/08/08/2003720120

two months no contract was announced until Mobile World Congress (MWC) in Barcelona in February 2019. MWC 2019 was a victory parade for both Huawei and the CCP with numerous NATO and UK allies announcing 5G deployment contracts to Huawei or ZTE. Is this the act of an independent company?

Huawei strategically operates in sectors the CCP deems vital

It is my opinion that Huawei is the practical implementor of CCP global policy to redefine personal liberties, internet[22] and freedom of speech and movement. It exports surveillance technologies across the world, in states where human rights abuses are rampant. Huawei is also strategically important to the CCP's *Made in 2025* plan[23]. Huawei has a strong portfolio in nine of the ten key sectors outlined in the plan:

Sector	Huawei Portfolio
New Information Technology	Cloud Data Centres, Artificial intelligence.
High-end numerically controlled machines tools and robots	Wireless Smart Factory solution based on eLTE. Predictive maintenance solutions.
Aerospace equipment	Airport cloud systems, Smart Airport agile networks, eLTE Visualised Operations.
Ocean engineering equipment and high-end vessels	Unknown.
High-end rail transportation equipment	Urban Rail Cloud platforms, Operational Communications systems.
Energy-saving cars and new energy cars	Autonomous vehicles, radar systems, LTE and 5G navigation, fleet tracking, traffic control.
Electrical equipment	Power Distribution Automation Communication Systems, Power Transmission Communications Networks, FusionSolar Smart PV, Fiber Powered by Grid.
Farming machines	Huawei researching carrier roles in smart agricultural including Farm Management Systems (FMS) and Variable Rate Technologies. Signed agreement with Sunrise and Agroscope to develop 5G farming technologies[24]
New materials	Huawei have numerous products in the oil and gas industry, including HPC and Operations Management, Oilfield Production IoT and digital monitoring systems for pipelines.

[22] Financial Times. 2020, March 27. China and Huawei propose reinvention of the internet. Link: https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2

[23] PRC. 2015, May 19. 'Made in China 2025' plan issued. Link: http://english.www.gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.htm

[24] Huawei. 2019. Sunrise and Huawei enter into strategic partnership with Agroscope for 5G farm. Link: https://www.huawei.com/en/press-events/news/2019/9/sunrise-huawei-strategic-partnership-agroscope-5g-farm

Bio-medicine and high-end medical equipment	eHospital agile networks, Regional Healthcare Information Networks, Multi-channel HD telemedicine; end-to-end biomedicine solutions for storage of and analysing bio-medicine data, genomic sequencing and genetic testing.

Table 1: Huawei Portfolio/support activities in the Made in China 2025 Plan

Huawei also has technologies in artificial intelligence, facial recognition, smart cities and banking.

How will the UK Government's decision impact the UK's geopolitical position?

The UK is home to the world's experts on Huawei, the HCSEC. The 2019 report is clear that only limited assurance can be provided that Huawei technology is secure and robust. The UK is in the unique position that it has a transparent review process for Huawei technology. That review process has provided a glimpse into the serious security issues and potential impact the leveraging of these security issues would have on critical infrastructure. Ignoring the report invites scepticism in the credibility of the UK government and sends a clear signal that 'shoddy' technology is acceptable in UK critical infrastructure.

Failing to act to curtail the growth of PRC influence in 5G and the IoT ecosystem will dilute the West's ability to maintain a free and open internet. The West must be unified in its resistance to CCP attempts to create two standards of the internet.

How will the UK's allies, particularly those in Five Eyes, respond to this decision?

The Five Eyes Alliance will become increasingly important as the PRC becomes more aggressive in the South China Sea and continues to debt-leverage emerging markets. Failing to support the Five Eyes Alliance, will sow the seeds of distrust amongst the member-states on the ability to rely on the UK to support the alliance on ICT matters. Emerging 5G technologies such as quantum, Artificial Intelligence, crypto currencies and biotechnologies can be weaponised through the use of vulnerable 5G systems. It is short-sighted to believe that 5G is simply about telecommunications.

How will this decision impact the UK's security and defence capabilities and the UK's interoperability with allies?

Interoperability at a technical level should remain unaffected, in the medium term. Networks used for intelligence sharing are not the commercial networks and are more robustly encrypted and protected. However there is no guarantee this will remain status-quo as 5G technologies evolve and edge devices become vector points and weaknesses in systems.

It is vital that governments make evidence-based decisions. The HCSEC has made it clear that it does not have full confidence in Huawei technologies. To ignore this is to ignore the intelligence services. What does this say about the UK government's confidence in those services, in the cybersecurity sector? Should the UK's allies trust these sources too, if the UK government will not give proper weight to their reports?

NATO implications

In a significant intervention in 2019, the commander of NATO forces in Europe, General Scaparotti, suggested that the risks with Huawei were so severe as to potentially require NATO to cease communication with German colleagues if they chose Huawei as an infrastructure provider. This was echoed by NATO Secretary General Jens Stoltenberg, who said that the alliance took the threat from Huawei "very seriously"[25]. Stoltenberg says that the Alliance is consulting widely to gain further understanding of the full extent of the potential threat from Huawei.

[25] Defence News, 2019, March 15. NATO weighing Huawei spying risks to member countries. Link: https://www.defensenews.com/global/europe/2019/03/15/nato-weighing-huawei-spying-risks-to-member-countries/

Q9. How important it is for the UK, separately or with allies, to maintain industrial capability in this field?

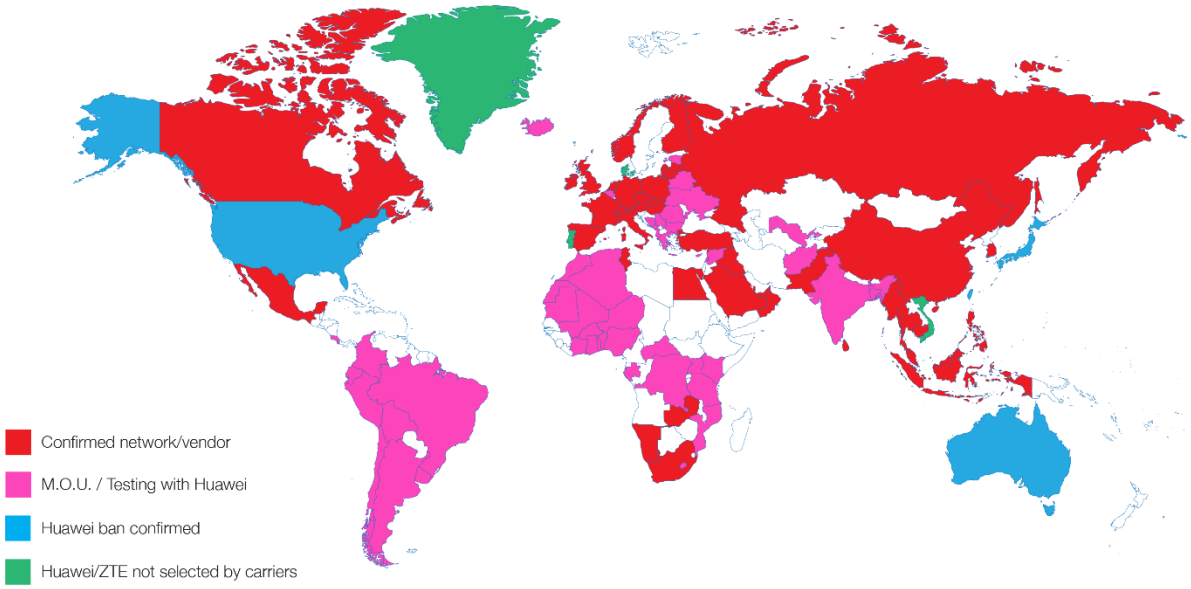

Figure 1: Chinese 5G testing and deployment contracts (as of April, 2020)

Maintaining Western industrial capability in telecommunications is vital. A diverse vendor market makes the leveraging of critical vulnerabilities in high-risk vendors much less impactful on networks. In the case of Huawei, the HCSEC pointed out that if the identified vulnerabilities were leveraged by a hostile actor Huawei itself may not be in a position to repair the damage. The downtime of networks would have enormous impact on economic and social stability.

Protecting the future marketspace

The above map illustrates the current footprint of Huawei and ZTE in 5G. It is highly probable there are more deployment contracts not declared. As Chinese-controlled 5G networks mature and the ecosystem cultivates more and more cloud-based operations and industries the ability of Western companies and nations to operate within a free and transparent 5G ecosystem dwindles. If the 5G marketplace is dominated by a single player to such an extent, and that player is subservient to laws of an undemocratic country can we expect such a company to adhere to free-market behaviours once dominance is achieved, and countries all over the world are dependent on them for their 5G-powered critical infrastructure? As the world moves into virtual trading, and cloud-supported technologies and services grow what impact will this have on the rules governing a free market?

Huawei dominance impacts competitors ability to invest in R&D

As the market share of Huawei increases decreased sales for competitors will see reduced R&D budgets, impacting vendor diversity. If Huawei is allowed to control 5G patents its competitors will have to rely heavily on these patented technologies into new generations of telecommunications. The consequence of which is that 6G etc will be controlled by Huawei and the UK will be subject to licensing agreements and other disclosure agreements for the use of its technology. The figure below shows Huawei R&D spend compared to other vendors from the period 2005 to 2018.

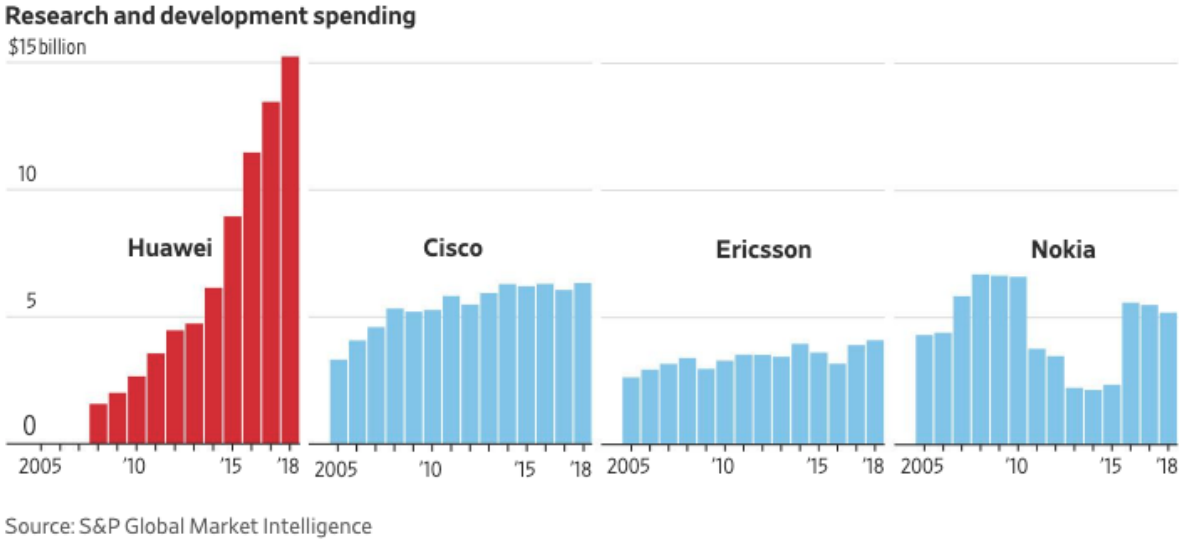

Figure 2: Huawei research spend comparison to other telecoms vendors[26]

Vital to protect the 5G IoT ecosystem

The Chinese state has been extraordinarily aggressive in protecting an alleged private company. Huawei is also becoming a major player in the management and storing of highly sensitive data on private citizens held by governments. Is China's aggression because Huawei is so important in its desire to control as many aspects of the global supply chain in emerging technologies; which western nations will be highly dependent on? Whoever controls 5G controls the ecosystem of technologies that are built upon it; robotics, Artificial Intelligence and machine learning – these technologies will be utilised by both the private sector and public sector (including military).

Ensuring transparent 5G standards

5G standards are important to ensure security across all networks globally. Concern has been expressed that 5G standards bodies are dominated by Chinese companies and supported by China-sponsored affiliated countries. According to the Wall Street Journal:

> Representatives from Chinese companies now hold 10 of the 57 chairman and vice chairman positions on decision-making panels at 3GPP, the France-based industry group overseeing the standard-setting process, according to Jefferies Group researchers.[27]

The slowdown caused by COVID-19 may result in a desire to quickly push ahead with agreeing standards that are not properly examined. It is important that global 5G networks operate on accepted standards and not operate on divergent ones. Such a scenario would be catastrophic.

[26] WSJ: 2019, May 25. Huawei's Years long Rise Is Littered With Accusations of Theft and Dubious Ethics. Link: https://www.wsj.com/articles/huaweis-yearslong-rise-is-littered-with-accusations-of-theft-and-dubious-ethics-11558756858

[27] WSJ. *China's Huawei Is Determined to Lead the Way on 5G Despite U.S. Concerns.* March 30, 2018. Link: https://www.wsj.com/articles/washington-woes-aside-huawei-is-determined-to-lead-the-way-on-5g-1522402201?mod=article_inline

A number of security officials have highlighted the dangers of Huawei and CCP-sponsored engineering groups pose to the security of 5G networks. As reported by Bloomberg in February 2019[28]:

> Chinese firms and government research institutes accounted for the largest number of chairs or vice chairs in the International Telecommunication Union's 5G-related standards-setting bodies, holding eight of the 39 available leadership positions, according to the U.S.-China Economic and Security Review Commission that advises Congress.

Weaponization of Intellectual Property (IP)

The withdrawal or refusal of IP licenses at the direction of the CCP is a real threat to the stability of 5G networks. The impact of the refusal to allow other vendors use standards-based IP developed by Huawei and other PRC companies presents a real danger to both the ability of western companies to develop and manufacture, but also in the ability of countries to continue to maintain and secure networks that would no longer be able to patched due to the withdrawal of IP licenses in the direction of the CCP. Heavy reliance on IP and standards from a country with no separation between business and government is dangerous and could lead to significant global disruption.

17 April 2020

[28] Bloomberg. *Huawei's Clout Is So Strong It's Helping Shape Global 5G* Rules. February 1, 2019. Link: https://www.bloomberg.com/news/articles/2019-02-01/huawei-s-clout-is-so-strong-it-s-helping-shape-global-5g-rules