DEFENDING OUR DATA: HUAWEI, 5G AND THE FIVE EYES

BY BOB SEELY MP, DR PETER VARNISH OBE
& DR JOHN HEMMINGS

HJS Henry Jackson Society

ASIA STUDIES CENTRE

DEMOCRACY | FREEDOM | HUMAN RIGHTS

May 2019

Published in 2019 by The Henry Jackson Society

The Henry Jackson Society
Millbank Tower
21-24 Millbank
London SW1P 4QP

Registered charity no. 1140489
Tel: +44 (0)20 7340 4520

www.henryjacksonsociety.org

Title: "DEFENDING OUR DATA: HUAWEI, 5G AND THE FIVE EYES"
Authors: Bob Seely MP, Dr Peter Varnish OBE & Dr John Hemmings

Cover Photo: Server room in datacenter. Hosting services. Photo by aleksanderdnp (ID: 77016305)
https://depositphotos.com/77016305/stock-photo-server-room-in-datacenter.html

DEFENDING OUR DATA: HUAWEI, 5G AND THE FIVE EYES

BY BOB SEELY MP, DR PETER VARNISH OBE
& DR JOHN HEMMINGS

HJS
Henry
Jackson
Society

ASIA
STUDIES
CENTRE

DEMOCRACY | FREEDOM | HUMAN RIGHTS

May 2019

FOREWORD

The greater part of my thirty-eight-year career in the British Intelligence and Security Community was defined by meeting the threat to the UK's national security from Communist states. The fact that the British Government now appears to have decided to place the development of some its most sensitive critical infrastructure in the hands of a company from the People's Republic of China (PRC) is deeply worrying. The PRC uses its sophisticated technical capabilities not only to control its own population (to an extreme and growing degree) but it also conducts remotely aggressive intelligence gathering operations on a global scale.

No part of the Communist Chinese state is ultimately able to operate free of the control exercised by its Communist Party leadership.

This is a simple statement of fact, not an opinion, about the inherent nature of the PRC and no amount of sophistry can alter it.

Therefore, we must conclude the engagement of Huawei presents a potential security risk to the UK. The key question that follows is can that risk be sufficiently mitigated to render it negligible?'

This important and timely paper sets out to give a balanced and detailed answer to this question. It examines Huawei's character as the PRC's leading telecommunications company, its record as a technology provider, its global engagement, its security performance hitherto and the judgement that three of the UK's Five Eyes partners have made about the risk that Huawei may present. In each of these areas of careful analysis there is a clear absence of the certainties that could lead us to conclude that our concerns about the company are either exaggerated or misplaced.

The British Government's relationship with Huawei dates back almost twenty years. I recall that the security concerns that were raised at the start of the relationship were then dismissed by the UK Government. Consequently, the argument that is presented now is that Huawei is so deeply embedded in the UK's telecommunications sector that the extension of the relationship to 5G will not make a great deal of difference. We have learned how to live with and manage the risk and can continue to do so. However, the introduction of 5G networks signals a very large technological step change which will have far reaching implications for the UK's national security and almost every aspect of the country's civic life.

What worked for 4G has only limited relevance to 5G and in parallel we should remind ourselves that China's military strategists perceive a world in which the military and the civilian will be fused into a single plane of conflict. The ability to control communications and the data that flows through its channels will be the route to exercise power over societies and other nations.

To place the PRC in a potentially advantageous exploitative position in the UK's future telecommunications systems therefore is a risk, however remote it may seem at the moment, we simply do not need to take. We should also not be influenced by the threat of the economic cost of either delaying 5G or having to settle for a less capable and more expensive provider.

I very much hope there is time for the UK Government, and the probability as I write of a new Prime Minister, to reconsider the Huawei decision. Furthermore, a post-Brexit government must not worry about giving offence to China by going back on the decision.

If Australia can black ball Huawei as its 5G provider the UK can certainly do so the same without undue concern about the consequences.

This measured and balanced paper concludes with sensible sound policy advice about how to manage this change of direction, offering both national and alliance policy suggestions. In my opinion, the Prague Proposals hold some very sound principles around defining risk, but I believe we must go further and follow through with legislation on the BEIS White Paper on Investment and National Security. Not doing so, ensures that our critical national infrastructure will remain vulnerable to further intrusion by potential threats from authoritarian powers.

Sir Richard Dearlove KCMG, OBE, *Head, Secret Intelligence Service, 1999-2004*

ENDORSEMENTS

If we make the wrong decision about allowing hostile agencies access to our critical national infrastructure, history will judge us harshly. This authoritative and alarming Report should help us to reach the right conclusion about companies operating under the aegis of the Communist Chinese state.

The Right Honourable Julian Lewis MP, Chair of the Defence Select Committee

We have to hope that the National Security Committee will revisit the decision it seems to have made on permitting Huawei into the periphery of the UK's future 5G system. When at least four senior ministers (of foreign affairs, defence, home affairs and development) oppose the decision, it is clear that it greatly prejudices our national security and interests. If the decision is revisited, everyone involved should read this report by the Henry Jackson Society. It sets out, with great lucidity, the reasons why allowing Huawei into even the periphery of this vital piece of critical national infrastructure would be a massive mistake. It is clear on the technological reasons and, more importantly perhaps, on the imperative of not putting long term trust in a company so close bound up with the Chinese Communist Party and its long term aims.

Charles Parton, Adviser to the House of Commons Foreign Affairs Committee 2017-9, Senior Associate Fellow at RUSI and author of 'China -UK relations: where to draw the border between influence and interference' (RUSI 20 Feb 2019)

GLOSSARY

ACFTU	All-China Federation of Trade Unions
ASD	Australian Signals Directorate
ASPI	Australian Strategic & Policy Institute
AU	Africa Union
CIA	Central Intelligence Agency (US)
CCP	Chinese Communist Party
CCCS	Canadian Centre for Cyber Security
CDB	China Development Bank
CEO	Chief Executive Officer
CMF	Civil-Military Fusion (PRC)
CSE	Communications Security Establishment (Canada)
CSIS	Centre for Strategic & International Studies
DCMS	Digital, Culture, Media, Sports (UK)
EXIM	Export-Import (Bank)
FCC	Federal Communications Commission (US)
HCSEC	Huawei Cyber Security Evaluation Centre
ICT	Information & communications Technology
ICFTU	International Confederation of Free Trade Unions
IOT	Internet of things
IP	Intellectual property
MSS	Ministry of State Security (PRC)
NBN	National Broadband Network (Aus)
NCSC	National Cyber Security Centre
NSA	National Security Agency (US)
PLA	People’s Liberation Army (PRC)
PRC	People’s Republic of China
OFDI	Outbound foreign direct investment

CONTENTS

EXECUTIVE SUMMARY

The movement of information and communications technology (ICT) toward the fifth generation of wireless networks (5G) will deliver a profound change in latency, data speed and volume, allowing for new technologies – such as agricultural or delivery drones, self-driving vehicles, and other data-driven tech. It will revolutionize Western societies and play a major part of our economic and national security.

It is in this context that the Government of the United Kingdom has been pressed to deliver on its 2017 Digital Strategy and in this context that the Chinese telecommunications giant, Huawei, has entered the debate. Much has been written both for and against the inclusion of the Chinese telecommunications giant into the UK's 5G network. On the one hand, it is set to become the world's largest ICT provider and has much to offer in terms of investing into the UK. On the other hand, the company has been viewed as complicit in both China's geopolitical ambitions and its intelligence-gathering operations.

The UK Government has approached the relationship carefully, with an institutional framework that has – it claims – helped mitigate any risks toward network control or data access. However, this does not appear to have been a unified position and it has become one of the most contentious and technical issues in Whitehall, with one minister losing his position after an apparent leak from the National Security Council. Considering the importance of 5G, we sought to answer five major questions. These were:

- Is Huawei a private corporation or state-owned / influenced?
- Does Huawei have institutional links to China's intelligence and military agencies?
- Is the current system – the Huawei Cyber Security Evaluation Centre (HCSEC) – sufficient in mitigating potential risks of including Huawei components in the construction of the UK's 5G network?
- Is the Government's apparent decision to limit Huawei components to the periphery a good way to mitigate further risks?
- What impact will the UK decision to include Huawei in its 5G network have on the Five Eyes intelligence alliance?

Using a mixed methodology of open-source materials, interviews, and expert opinion, we put forward the following as our findings:

- **Huawei is a product of the Chinese national eco-system,** constrained, influenced and directed by China's legal and political environment. When considering Huawei's inclusion into the UK market, Chinese law, Chinese Communist Party (CCP) influence, and Government economic and industrial policy must be factored in.
- **China's Civil-Military Fusion (CMF) doctrine** emphasises closer links between China's tech companies and its military industrial enterprises. Its military doctrine emphasises warfare as conflict between systems.

- **Huawei's subordination to the 2017 National Intelligence Law** mean that it is obliged to assist China's intelligence agencies in operations and research and development. Despite claims to the contrary, it is likely to be compelled to act in Beijing's interests by the CCP leadership.
- **Huawei's organisational structure** is opaque. Its claims to be a private company are highly problematic, as it is 98% owned by a trade union committee. Under Chinese trade union law, trade union officials are paid by the state according to civil servant pay scales, and are subordinate to, and answerable to, the Chinese Communist Party (CCP).
- **Huawei acts like – and is treated like – a state-owned enterprise** by Chinese state-banks. There are claims that it has a credit line of £77 billion to expand its operations into the global supply chain, which it has done with remarkable speed. This and a "lock-in" approach toward network-building presents risk to global supply chains.
- **Huawei has long been accused of espionage,** and while there are no definitively proven cases, many countries – including Australia and the United States – have categorised it as a "high-risk vendor" and excluded it from 5G infrastructure because of national security concerns.
- **Huawei is an ICT partner to security forces in Xinjiang,** at a time of increasing authoritarianism in the region. This situation embodies China's authoritarian values and approach toward technology and surveillance, and the company could be used by the CCP to export these abroad.

Therefore, we believe that Huawei's inclusion into the UK's 5G network does present some risks. Moving to the UK policy, we put forward the following findings:

- **Whilst the UK Government still insists that it can "mitigate the risk",** it is no longer consistent in its confidence on this. The Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board – responsible for overseeing Huawei's engineering in the UK – issued a damning report in March 2019, which is at variance with the apparent government decision.
- **The UK Government says Huawei will be kept out of the "core" of 5G,** but engineers and experts interviewed for this project say that 5G is likely to see the core/periphery distinction disappear as the technology matures, leading to significant security challenges. It is also clear that our allies in Australia and the US hold a different position with regards to the core/periphery issue as 5G matures.
- **The UK Government says Huawei will be limited to "dumb" components like antennas,** but our technical advisors have indicated that antennas can be modified at both the hardware and software level. Indeed, as 5G means moving more and more to software-networking, the ability of a manufacturer to repurpose an antenna without detection will increase.
- **The impact on our Five Eyes is still to be determined,** but could be significant. There will be damage to the symbolic unity of the Western alliance, but there are also additional dangers of Chinese-led cyber interference operations inside the UK. The "hacking" of parliaments in Australia, New Zealand, and the UK are likely to have been about hacking democracy as they were about hacking the institutions.

Chapter 1
INTRODUCTION

"We need to decide the extent to which we are going to be comfortable with Chinese ownership of these technologies and these platforms in an environment where some of our allies have taken a quite definite position. We need to have a conversation. It's not wholly straightforward."

Alex Younger, *Chief, Secret Intelligence Service, 3 December, 2018*

Data is power, and whoever controls communications will have great power over our societies in the future. Ownership of those communications structures, access to information flows and attitudes toward human freedom, will be paramount in shaping our nation in the twenty-first century and beyond. The impact 5G is likely to have on society, on government, on regulation, our way of life, and even, the global order – is still to be determined, but is likely to be highly significant. Because it and the Internet of Things (IoT) will impact so many facets of life, and drive the next stages of innovation, industry, and economy, it has been rightfully recognised as a strategic industry of the future, par excellence. Along with China, the United States, Germany, France, Japan, South Korea, Singapore, and Canada, the United Kingdom has initiated a number of government-corporate programmes, strategies, and test-bed & trials to help kick-start 5G. The Government's primary document is the Digital Strategy, which was published by the Department for Digital, Culture, Media, and Sport (DCMS) in March 2017 [1]. The strategy contains a £1 billion commitment to help roll-out 5G across a range of applications – such as smart farming with drones, healthcare in the home, manufacturing productivity, and self-driving cars – across the whole of Britain.

For nearly a year, a debate about Chinese telecommunications companies has raged in the West, started by the US decision to ban American firms from selling components and software to the Chinese telecommunications firm ZTE in April 2018. While this situation was ultimately resolved, it was followed shortly after by the arrest of Huawei's Chief Financial Officer Meng Wanzhou, the daughter of the company's founder, Ren Zhengfei. The Chinese Government's swift response to her arrest – including the arrest of two Canadian former diplomats – seemed to indicate that the company, long-seen as a 'national champion', has the full political support of Beijing. Given the reputation China has as a source of cyber-espionage, the prospect of including Huawei in the building of the UK's 5G network raises a number of questions about the company's independence from Beijing, and potential risks inherent in including its hardware and software in the network.

In attempting to determine the risk posed by Huawei or ZTE (or any other Chinese corporation, for that matter) taking a large role in the UK's digital infrastructure, it is clear that we are at an unusual crossing-point in the history of great power relations and in the history of technology. The People's Republic of China has developed not only into an economic and military power but also into a cyber-power and now wishes to become a "high-tech" power. This introduces new dynamics into and exerts new pressures on the international system.

[1] "UK Digital Strategy", *Department for Digital, Culture, Media & Sport*, 1 March, 2017, available at: https://www.gov.uk/government/publications/uk-digital-strategy (last visited 30 April, 2019).

Earlier this year, GCHQ Chief, Jeremy Fleming asserted that "there's something definitely unique about the combination of uncertain doctrine, hyper technology change and a new form of ungoverned space that is making [cyber] particularly challenging." [2] General Michael Hayden, former Director of the CIA and NSA has gone so far as to say that "this [cyber] is the most disruptive thing to happen to us as a species probably since the European discovery of the new world."[3] Add to that the complexity of China's hybrid capitalist-socialist model, its geo-strategic ambitions, the recent Civil-Military Fusion (CMF) doctrine, which requires that Chinese tech companies work much more closely than they have traditionally with the Chinese military, and the subsidising of Chinese companies to expand globally in strategic sectors, and it is clear that we are confronted by new hybrid challenges that are emerging across multiple sectors simultaneously.

The apparent[4] decision by the NSC to limit Huawei to the periphery of the UK's 5G network is one that is worth greater investigation and understanding. Have we penalized Huawei unfairly for its connections to China? After all, the company's has resolutely declared that it would not take part in espionage and declared that its supposed relationship with People's Liberation Army is only limited to the early part of its founder's career. Or have we not gone far enough and risked much even in including Huawei at all within a system that many describe as a "paradigm shift"[5] in technology? After all, there have been many who believe that Huawei is not merely another company. As we have all learned over the debate spawned by Huawei's entry into the Western 5G market, Chinese law requires all companies to support China's intelligence agencies, both at home and abroad. And while Huawei claims to be a private company and carries out much legitimate private business, its opaque ownership structure and longstanding ties to the Chinese state mean that it operates in the national interests of China. According to a report by the Australian Strategic Policy Institute (ASPI) – contributing co-authors to this report – Huawei has "prominent roles in a number of state-directed industrial policy initiatives to develop China's national communications capabilities." The company has, the author argues, "a dual function: it is both a profit-seeking enterprise and an instrument of Chinese national strategy."[6] This hybridity is a strong mark of how authoritarian powers are challenging the rules-based order below the threshold of war.

Assessing the Debate on Huawei in the UK

We determined to write this report to help inform the debate in the UK over the future of 5G, to try and to develop a consensus over the use of Chinese tech in the building of the UK's 5G network, and finally to understand how democracies might deal with the rise of tech companies that come from authoritarian states. The debate is not clear cut, however, and even on Huawei there are a number of contradictory positions representing the UK Government.

[2] "Director's Speech on Cyber Power – as delivered", *GCHQ*, available at: https://www.gchq.gov.uk/speech/jeremy-fleming-fullerton-speech-singapore-2019 (last visited 15 April, 2019).

[3] Adam Janofsky, "Gen. Michael Hayden: Overclassification of Cyber Threats Puts Businesses at Risk", *The Wall Street Journal*, October 31, 2018, available at: https://www.wsj.com/articles/gen-michael-hayden-overclassification-of-cyber-threats-puts-businesses-at-risk-1541018014 (last visited 1 May, 2019).

[4] "Apparent" because we have no way of verifying the information that was leaked as true.

[5] Simon Yeung, "Getting ready for 5G and the paradigm shift it will bring," *RCR Wireless News*, 19 March, 2018, available at: https://www.rcrwireless.com/20180306/opinion/readerforum/getting-ready-for-5g-and-the-paradigm-shift-it-will-bring-reader-forum-Tag10 (last visited 7 May, 2019).

[6] Rick Umback, "Huawei and Telefunken: Communications Enterprises and Rising Power Strategies,", *ASPI, Strategic Insights*, 17 April, 2019, available at: https://www.aspi.org.au/report/huawei-and-telefunken-communications-enterprises-and-rising-power-strategies (last visited 6 May, 2019).

Whilst Alex Younger, Chief of MI6 warned of the challenges of using Huawei in December 2018, others like Robert Hannigan, former chief of GCHQ, criticized blanket bans in February 2019. Hannigan wrote "we should accept that China will be a global tech power in the future and start managing the risk now, rather than pretending the west can sit out China's technological rise" [7]. Shortly after this, the National Cyber Security Centre (NCSC) announced[8] that it could "mitigate the risk" of having Huawei in the UK's 5G network. However, within a matter of weeks, the HCSEC Oversight Board produced a report, warning that it could only offer "limited assurance" that it could mitigate the risks of including Huawei in the (4G) network and that "repeated shortfalls" in "Huawei engineering practices and processes" would cause long-term increased risk in the UK.

Tom Uren, a Senior Analyst in ASPI's International Cyber Policy Centre and a co-contributor to this report, notes the significance of this past report, writing: "the trend across the four oversight board reports suggests that as HCSEC has improved capability, confidence that the security evaluation process will sufficiently mitigate risks has declined – the more HCSEC learned, the less confident they were." [9] In other words, the more we know, the more we realise what we do not know.

Central to the debate in the UK has been a number of questions that have been raised again and again in the media without satisfactory resolution. They are:

- Is Huawei a private corporation or state-owned / influenced?
- Does Huawei have institutional links to China's intelligence and military agencies?
- Can the Huawei Cyber Security Evaluation Centre (HCSEC) mitigate the potential risks of including Huawei components in the construction of the UK's 5G network?
- Would a Government's policy of limiting Huawei components to the periphery be a good way to mitigate further risks?
- What impact would a UK decision to include Huawei in its 5G network have on the Five Eyes intelligence alliance?

It is difficult to answer these questions without first recognizing the nature of China's rise over the past few decades. This is because the debate about Huawei is not just about Huawei, but rather, it is also a debate about the state behind it, its future intentions and how it seeks to reshape the global order. Those who have argued in favour of allowing Huawei into the UK's 5G network, assume that Huawei's rise is a metaphor for China's; acceptance of one requires the other. However, the debate properly understood is also about how different political systems apply technology to governance. In this sense, it is a debate between closed versus open societies, between how the UK and other Western states treat the personal data of their citizens and how China (and other authoritarian regimes including Russia) treat the personal data of their citizens. Ultimately, in writing this report, we have come to believe that it is impossible to look at Huawei's involvement in the UK's 5G network as a purely technical or purely commercial issue.

[7] Robert Hannigan, "Blanket bans on Chinese companies like Huawei make no sense", *Financial Times*, February 12, 2019, available at: https://www.ft.com/content/76e846a4-2b9f-11e9-9222-7024d72222bc (last visited 30 April, 2019).

[8] Demetri Sevastopulo, David Bond, "UK says Huawei is manageable risk to 5G", Financial Times, 17 February, 2019, available at: https://www.ft.com/content/619f9df4-32c2-11e9-bd3a-8b2a211d90d5 (last visited 6 May, 2019).

[9] Tom Uren, "Huawei: lessons from the United Kingdom," ASPI: The Strategist, 25 July 2018, available at: https://www.aspistrategist.org.au/huawei-lessons-from-the-united-kingdom/ (last visited 30 April, 2019).

While it is clear that the NCSC or the DCMS could not be expected to include these wider issues in the supply chain security review, it is imperative that the National Security Council put them front and centre. The inclusion of Huawei into the UK's infrastructure does not happen in a vacuum. It also occurs as China develops a strong strategic posture toward the world that we are only just now coming to understand. It occurs as a million or more Uighur disappear into Chinese camps[10]; as Chinese influence campaigns enter liberal societies through the United Front Work campaigns[11]; as China develops a new type of economic statecraft that undermines the will of states to not only defend their own principles, but to defend their own interests[12].

China under Review

China has achieved remarkable things in recent decades. Regardless of whether or not it becomes the world's largest economy in coming years, it has retaken a significant place in world affairs that it had lost over the previous two centuries. By abandoning socialism and embracing market economics – albeit without many of the legal and political norms of Western society - it has raised half a billion people out of poverty, a defining event in the 21st Century. However, to only consider the inclusion or exclusion of Huawei into our 5G system would be to overlook the background to the debate, which is not primarily commercial, but instead encompasses some significant and profound questions, including:

- What effect will Chinese infrastructure have on Chinese espionage capability in the West?
- What effect will Chinese infrastructure have on our ability to withstand Chinese political and military pressure?
- What effect will Chinese infrastructure have on individual freedoms?
- What effect will Chinese infrastructure have on Western security and military information sharing – in particular, the Five Eyes information sharing agreement?

Building from the assumption that one cannot consider the inclusion of Huawei into an integral part of the UK economy and infrastructure with just a narrow technical risk assessment system, we also believe that how technology is applied to harness data for authoritarian ends is of paramount importance to the debate.

For the moment, at least, authoritarian states are on the rise. Indeed, the defining political struggle of the twenty-first century is, in part, between open and closed societies. Twenty years ago, in the wake of defeating the Soviet Marxist states, liberal-democracy was the unchallenged, default position of the future. Today, however, Russia and China have re-ordered domestic politics around authoritarian systems with quasi-capitalist economics. China has a one-party system where criticism of the state, above a certain level, is not tolerated and where the rule of law comes second to the rule of Party. China's social credit system, while in part a practical tool for dealing with life online, amounts to 'virtual Big Brother'. In the words of Sigmar Gabriel, former Foreign Minister of Germany; "China

[10] Stephanie Nebehay, "UN says it has credible reports that China holds million Uighurs in secret camps" *Reuters*, 10 August, 2018, available at: https://uk.reuters.com/article/uk-china-rights-un/u-n-says-it-has-credible-reports-that-china-holds-million-uighurs-in-secret-camps-idUKKBN1KV23P (last visited 6 May, 2019).

[11] Anne-Marie Bradie, "Chinese interference: Anne-Marie Brady's full submission", *Newsroom*, available at: https://www.newsroom.co.nz/2019/05/08/575479/anne-marie-bradys-full-submission (last visited 10 May, 2019).

[12] Nick Miller, "China undermining us 'with sticks and carrots': Outgoing German minister," *Sydney Morning Herald*, 19 February, 2018, available at: https://www.smh.com.au/world/europe/china-undermining-us-with-sticks-and-carrots-outgoing-german-minister-20180219-p4z0s6.html (last visited 6 May, 2019).

is developing a comprehensive system alternative to the Western one, which, unlike, our model, is not based on freedom, democracy and individual human rights." [13] As the dominance of Chinese companies in fields like 5G occur, do they not present other risks to Western societies and values?

Structure of Report

As it proceeds, the report is structured as follows: the **second chapter** attempts to understand the wider legal and regulatory national system in which Chinese companies – such as Huawei – must operate.

The **third chapter** attempts to understand Huawei's own internal structure, its sources of potential state direction and financing, and indications of this in its approach towards technological strategy and policy.

The **fourth chapter** examines the potential risks from including Huawei inside the UK's 5G network, and reflects the concerns and worries of a number of technical experts consulted for this project.

Given the importance of the Five Eyes, and the fact that their real-time intelligence-sharing arrangements have given them both deep interests and leverage in this debate, the next three chapters are short case-studies about the 5G debate in the United States, in Australia, and in Canada. [14]

Chapter five is written by Brigadier General Robert Spalding, a former National Security Strategy advisor to the White House on 5G.

Chapter six is authored by Tom Uren and Danielle Cave from the Australian think tank, ASPI, and reflects Canberra's own debate deliberations and its resolution.

Chapter seven is by Jonathan Berkshire Miller, a Distinguished Fellow at the Asia Pacific Foundation of Canada, and outlines the debate in Ottawa.

Finally, our **conclusion** summarizes the discussion and our findings and puts forward some modest policy suggestions that we hope the Government will consider going forward

[13] Nick Miller, "China undermining us 'with sticks and carrots': Outgoing German minister," Sydney Morning Herald, 19 February, 2018, available at: https://www.smh.com.au/world/europe/china-undermining-us-with-sticks-and-carrots-outgoing-german-minister-20180219-p4z0s6.html (last visited 6 May, 2019).

[14] Time restrictions prevented the inclusion of a New Zealand chapter though efforts to secure an author were made.

Chapter 2
THE NATURE OF THE CHINESE ECONOMY UNDER XI

"We're entering an era in which we'll be fused together. It might be that there will be a request to establish a (Communist) Party committee within your company, or that you should let state investors take a stake…as a form of mixed ownership. If you think clearly about this, you can really resonate together with the state. You can receive massive support. But if it's your nature to go your own way, to think that your interests differ from what the state is advocating, then you'll probably find that things are…more painful than in the past."

Wang Xiaochuan, *Sogou CEO*[15]

One of the primary concerns over the UK Government's possible decision to allow Huawei to take part in the construction of the UK's 5G network is the perception – rightly or wrongly – that it was based on a narrow technical risk assessment system, driven by strong commercial interests. Huawei officials have even raised it in their efforts to lobby against a ban, saying at a Chinese New Year banquet in London, "The open attitude of the UK and its support of free markets and enterprise are values that are respected worldwide and are admired by us at Huawei…we trust Britain to maintain its openness and inclusiveness and make the wise choices that serve the interests of UK citizens.[16]" But is allowing Huawei a foothold in the UK's critical national infrastructure in the interest of free market principles? Does Huawei itself even operate using those principles? At a recent 5G Conference in Prague where 32 nations discussed issues relating to supply chain security and 5G[17], discussions focused on how to make realistic supply-chain risk assessments in an area where national security and economic security are so vital. "The overall risk of influence on a supplier by a third country should be taken into account", noting that there are numerous ways that suppliers can be influenced.[18]

In those discussions, state-sponsorship, subsidies, and financing were discussed, as were the wider legal environment in which communications companies sit. Therefore, this chapter will attempt to discern whether or not successful high-tech companies like Huawei receive strategic direction, legal compulsion, or state-financing from the Chinese state, which are of direct import to their inclusion into the UK's 5G network.

Is Huawei influenced by the Chinese Party-State?

A fundamental question in past Henry Jackson Society research – and one that is pertinent to the current debate over Huawei in the UK – is the extent to which Chinese companies are controlled or beholden to the Chinese state. In *Safeguarding Our Systems*, a previous report by the Henry Jackson Society on Chinese State Capitalism, Freidolin Strack, Head of Department of International Markets at the BDI, the German business association, is

[15] Elsa Kania, "Much ado about Huawei", *The Strategist*, ASPI, 28 March, 2018, available at: https://www.aspistrategist.org.au/much-ado-huawei-part-2/ (last visited 26 March, 2019).

[16] Nic Fildes, "Telecoms Groups to Stand by Huawei Despite Scrutiny," *The Financial Times*, 5 February, 2019, available at: https://www.ft.com/content/3103e21a-2870-11e9-88a4-c32129756dd8 (last visited 1 May, 2019).

[17] Prague 5G Security Conference, Government of the Czech Republic, 1 May, 2019, available at: https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-173333/ (last visited 6 May, 2019).

[18] Shelby Brown, "Countries draft 5G security proposals as US warns of Huawei threat", CNet, 3 May, 2019, available at: https://www.cnet.com/news/countries-draft-5g-security-proposals-as-us-warns-of-huawei-threat/ (last visited 6 May, 2019).

quoted as saying, "There is no distinction, nor should we seek to make one…for one thing, you never know their connections…for another, all Chinese companies have access to state finance through the large Chinese banks."[19]

His point is an important one: party connections are significant in China because they allow for informal avenues of state direction as well as easy financing. It is worth noting that since 2012, Xi Jinping has been driving ever-closer ties between China CCP and China INC. According to Trey McArver, a co-founder of the consultancy Trivium/China, "No company, private or state-owned, gets ahead in China without aligning itself with the party's larger goals and strategies."[20] Under Xi, we've seen this become exaggerated with high-tech firms becoming increasingly directed under policies like *Made in China: 2025*, the Belt and Road Initiative (BRI), and State Council plans on artificial intelligence[21] and national informatisation[22].

The Conference Board, a lobby group which operates in China on behalf of large Western conglomerates – such as Nestlé SA and Walmart Stores, Inc., asserts, "As the Communist Party of China takes an increasingly active role in policy design and implementation, multinational companies need to think anew about government affairs strategies"[23]. This has led to an interesting dynamic which sees Chinese tech firms specifically recruiting party members and setting up party committees within the companies to help facilitate this fusion[24]. In 2006, 178,000 party committees had been established in private companies, but by 2016, this has increased to around 1.3 million[25]. According to *Mapping Chinese Tech Giants*, "Internet and technology companies are believed to have the highest proportion of CCP party committees in the private sector."[26]

Huawei and Civil-Military Fusion

The idea that Huawei might receive strategic direction from the Chinese state does have a basis in policy. After all, the PRC has made what officials call "civil-military fusion (CMF) a major part of its national strategy since 2014. According to the Council on Foreign Affairs, an influential American think tank, CMF is intended to "bolster the country's innovation system for dual-use technologies in various key industries like aviation, aerospace, automation, and information technology through 'integrated development'". [27] This has seen the state urge private companies and research institutes to work more closely with large defence enterprises, and has been written into the

[19] Interview, 6 July, 2017, for *Safeguarding our Systems*, Henry Jackson Society report in 2017.

[20] Emily Feng, "Chinese tech groups display closer ties with Communist Party", *Financial Times*, October 10, 2017, available at: https://www.ft.com/content/6bc839c0-ace6-11e7-aab9-abaa44b1e130 (last visited 9 May, 2019).

[21] Such as the "New Generation Artificial Intelligence Development Plan", released July 2017, available at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/ (last visited 16 April, 2019).

[22] State Council releases five-year plan on informatization, *The State Council Website*: http://english.gov.cn/policies/latest_releases/2016/12/27/content_281475526646686.htm (last visited 16 April, 2019).

[23] "Multinationals are Rethinking How They Lobby Xi's China", *Bloomberg*, 13 March, 2017, available at: https://www.bloomberg.com/news/articles/2017-03-13/as-xi-empowers-party-foreigners-lobby-secret-communist-panels (last visited 1 May, 2019).

[24] Emily Feng, "Chinese tech groups display closer ties with Communist Party", *Financial Times*, October 10, 2017.

[25] Mapping China's Tech Giants: *ASPI*, available at: https://www.aspi.org.au/report/mapping-chinas-tech-giants (last visited 23 April, 2019).

[26] Ibid.

[27] Lorand Laskai, "Civil-Military Fusion: The Missing Link Between China's Technological and Military Rise," *Council on Foreign Relations*, 29 January 2018, available at: https://www.cfr.org/blog/civil-military-fusion-missing-link-between-chinas-technological-and-military-rise (last visited 6 May, 2019).

"[Huawei] is also a major participant in initiatives to develop dual-use technologies that will have significant implications for warfighting, including 5G, quantum cryptography, and artificial intelligence."

Rick Umback, *ASPI*

constitution by President Xi Jinping[28]. This policy has become a major signature policy for Xi in his attempts to modernize the PLA and turn China's technological gains into military gains. One area where Huawei has already cooperated with the PLA is in the building of the military communications network in the early 1990s, which one company official described as "small in terms of our overall business, but large in terms of our relationships."[29] This initial contract is said to have encouraged further military orders and other large government contracts and cemented Huawei's position as a 'national champion'.

Another aspect of the environmental conditions for Chinese tech companies is the emphasis that Chinese military has begun to put on warfare as a conflict between opposing *operational systems* rather than armies, where victory is gained not through ground warfare but by destroying "the operational capability of the enemy's operational system."[30] In 1999, two PLA colonels, Colonel Qiao Liang and Colonel Wang Xiangsui, published a seminal book on warfare *Unrestricted Warfare*[31]. The book opened a whole range of possibilities to Chinese military forces in an imagined battle against a technologically superior opponent like the United States. Their analysis was that that success could come by fighting another state's system, through financial means, electronic means, and through cyberspace. Twenty years later and China's 2009 Defence White Paper only mentions mechanization of forces seven or eight times; informatisation – by contrast – is mentioned 50 times[32]. According to recent US defence studies on China's military doctrine, the PLA is working hard on information and informitised warfare, placing increasing emphasis on deception, on taking the offensive, on "achieving victory before the first battle", and on increased integration of China's civilian and military technology sectors[33].

The PRC and the National Intelligence Law 2017

As many cyber-security experts have noted, the PRC's National Intelligence Law has a direct impact on Huawei's relationship with China's intelligence organs. Article 7 states,

"All organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of.[34]"

[28] Katrin Hille, Richard Waters, "Washington unnerved by China's 'military-civil fusion', Financial Times, 8 November, 2018, available at: https://www.ft.com/content/8dcb534c-dbaf-11e8-9f04-38d397e6661c (last visited 6 May, 2019).

[29] Rick Umback, "Huawei and Telefunken: Communications Enterprises and Rising Power Strategies,", *ASPI, Strategic Insights*, 17 April, 2019, available at: https://www.aspi.org.au/report/huawei-and-telefunken-communications-enterprises-and-rising-power-strategies (last visited 6 May, 2019).

[30] Jeffrey Engstrom, *Systems Confrontation and Systems Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*, The Rand Corporation, 2018, available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1708/RAND_RR1708.pdf (last visited 6 May, 2019).

[31] Qiao Liang, Wang Xiangsui, *Unrestricted Warfare*, (Beijing: PLA Literature and Arts Publishing House, 1999), available at: https://www.c4i.org/unrestricted.pdf (last visited 6 May, 2019).

[32] Timothy L Thomas, *The Dragon's Quantum Leap: Transforming from a Mechanised to an Informatized Force*, (FMSO, Fort Leavenworth, 2009), p.239.

[33] Ibid.

While much has been made of the National Intelligence Law, is the attention is has brought to Huawei deserved? After all, Huawei commissioned a 37-page legal opinion from Zhong Lun, a Chinese law firm, and submitted it to the US Federal Communications Commission, in which it makes four claims[35], (i) there is no law demanding Huawei implant backdoors; (ii) there are safeguards in Chinese law that defend businesses' "legitimate interests"; (iii) Huawei's subsidiaries are not subject to Chinese law outside of China; and (iv) Beijing can only demand assistance in order to meet 'clear and specific [counter-espionage] goals. However, there are questions as to whether the Chinese government is actually constrained by Chinese law[36]. There have also been serious questions raised about the independence of the Zhong Lun Law Firm, as its founding and managing partner, Zhang Xuebing is a senior Party Secretary and Chairman of the Beijing Lawyers Association. According to Sinopsis, which writes about China in Europe, the Beijing Lawyers Association has allegedly been used by the Xi Government to disbar and persecute human rights lawyers in China[37] as part of the crackdowns on liberal groups that began after he took power in 2012.

One of the most important trends in China's political economy is the fact that reforms have stalled, and that though the regime continues to talk of "opening up", it has begun a major campaign to re-emphasise CCP leadership in every facet of society and the economy. Even wealthy corporate heads are becoming increasingly under the rein of the party. In December 2017, the Chinese state linked financial risk to national security, launching a wave of arrests of prominent business tycoons. According to Fraser Howie, author of *Red Capitalism* (2012) and an expert on China's banking and financial system, "Private capital is welcome as long as it's in the service of the Party"[38].

Strategic Economic Policy

In addition to strong party networks, the Chinese state exerts both control and strategic direction over tech companies such as Huawei through its Five Year Plan, which provides for government research grants and state funding and non-competitive loans from Chinese state banks in key strategic sectors which the PRC wishes to prioritize. The current Plan[39] (2016-2020) prioritises *next-generation information technology* and the particular technologies within this group[40] mirror exactly Huawei's own research and development

[34] National Intelligence Law of PRC (2017), on China Law Translate website, available at: https://www.chinalawtranslate.com/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E5%9B%BD%E5%AE%B6%E6%83%85%E6%8A%A5%E6%B3%95/?lang=en (last visited 28 May, 2019).

[35] Yuan Yang, "Is Huawei compelled by Chinese law to help with espionage?", *Financial Times*, March 5, 2019, available at: https://www.ft.com/content/282f8ca0-3be6-11e9-b72b-2c7f526ca5d0 (last visited 29 April, 2019).

[36] Francis Fukuyama, "Reflections on Chinese Governance", *Journal of Chinese Governance*, Vol 1, Issue 3, 2016, pp.379-391.

[37] Jichang Lulu, "Lawfare by proxy: Huawei touts 'independent' legal advice by a CCP member", Sinopsis, 2 August, 2019, available at: https://sinopsis.cz/en/lawfare-by-proxy-huawei-touts-independent-legal-advice-by-a-ccp-member/ (last visited 9 May, 2019)

[38] Lucy Hornby, "Chinese crackdown on dealmakers reflects Xi power play," *Financial Times*, 9 August, 2017, available at: https://www.ft.com/content/ed900da6-769b-11e7-90c0-90a9d1bc9691 (last visited 29 April, 2019).

[39] The 13th Five-Year Plan for Economic and Social Development of the People's Republic of China (2016-2020), Central Compilation and Translation Press, available at: http://en.ndrc.gov.cn/newsrelease/201612/P020161207645765233498.pdf (last visited 23 April, 2019).

[40] These include cultivating integrated circuit industrial systems, new display technologies, smart mobile terminals, 5G mobile communications, advanced sensors, and wearable devices

line[41]. While it's true that the *Made in China: 2025*[42] has been de-emphasised as a result of Western pressure[43], the US Trade Representative has found that China is still providing both state direction and financing for favoured areas of technological development through the *Industrial Transformation and Upgrading Fund* and the *Made in China 2025 Key Area Technology and Innovation Greenbook – Technology Road Map*, which replaced the *Made in China: 2025* in February 2018[44]. Indeed, Chinese leadership in the 5G area is down to strong state intervention with the Ministry of Industry and Information Technology (MIIT) publishing a "Consideration of spectrum 5G" report in 2016 and a "5G Promotion Plan (2013-2020)[45]. Such has been the weight of government intervention in the sector, that shortly before he resigned as Chairman of Alibaba, Jack Ma complained of it to the World Artificial Intelligence Conference, saying in a speech that it "would be the most important factor in destroying innovation."[46]

Huawei by the Numbers

£7.5 billion: loans extended to Huawei customers by China.

£77 billion: credit made available to Huawei customers

£145 million: in Chinese government grants (since 2016)

18–30%: the amount Huawei undercut its European competitors (2016)

2.5-25% market growth between 2006 and 2014.

The Question of Chinese Bank Loans

Huawei has grown very quickly over the past four years, moving from $.4.6 billion in sales revenues in 2014 to $105 billion in 2018[47]. Much of this is pushed back into research and development which is a credit to the company's long-term strategic ambitions, however it should be noted that Huawei's growth is also – at least, in part – state supported as it is a beneficiary of Chinese state-bank lending. Indeed, it is the Chinese tech firm of choice for expanding China's technological footprint abroad in key Chinese foreign policy platforms, such as the Belt and Road Initiative.

The primary conduit through which Huawei receives this funding is the China Development Bank (CDB), which holds more than £1.26 trillion in loans abroad, more than the World Bank. The CDB's largest shareholder is the PRC Ministry of Finance and it is led by a cabinet minister at the Governor level, under the jurisdiction of the State Council, implementing a

[41] "Research & Development", Huawei Website, available at: https://www.huawei.com/uk/about-huawei/corporate-information/research-development (last visited 23 April, 2019).

[42] "Update Concerning China's Acts, Policies and Practices Related to Technology Transfer, Intellectual Policy, and Innovation," Office of US Trade Representative, November 20, 2019, available at: https://ustr.gov/sites/default/files/enforcement/301Investigations/301%20Report%20Update.pdf (last visited 29 April, 2019).

[43] Sidney Leng, Zheng Yangpeng, "Beijing tries to play down 'Made in China: 2025' as Donald Trump escalates trade hostilities," South China Morning Post, June 26, 2018, available at: https://www.scmp.com/news/china/policies-politics/article/2152422/beijing-tries-play-down-made-china-2025-donald-trump (last visited 29 April, 2019).

[44] "Update Concerning China's Acts, Policies and Practices Related to Technology Transfer, Intellectual Policy, and Innovation," Office of US Trade Representative, November 20, 2019, available at: https://ustr.gov/sites/default/files/enforcement/301Investigations/301%20Report%20Update.pdf (last visited 29 April, 2019).

[45] David Abecassis, Chris Nickerson, Janette Stewart, "Global Race to 5G – Spectrum and Infrastructure Plans and Priorities," Analysys Mason, April 2018, available at: https://api.ctia.org/wp-content/uploads/2018/04/Analysys-Mason-Global-Race-To-5G_2018.pdf (last visited 29 April, 2019), p.56.

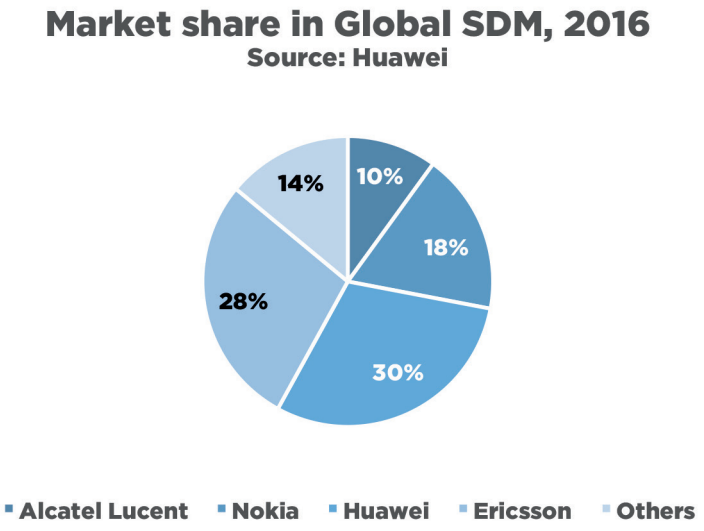
[46] Yoko Kubota, "Alibaba's Jack Ma Says Government Should Stick to Governing," Wall Street Journal, 17 September, 2018, available at: https://www.wsj.com/articles/alibabas-jack-ma-says-government-should-stick-to-governing-1537183483?mod=article_inline (last visited 28 April, 2019).

[47] Interview with author, Huawei spokesman, 9 May, 2019.

government core strategy of the *going out* of Chinese firms into the global market[48]. The *Financial Times* has written that CDB "exists to protect China's national interests, and it works under the strategic guidance of the Chinese government."[49] According to Philippe Le Corre, author of *China's Offensive in Europe,*

"The whole edifice of expansion beyond Chinese borders is connected above all to the role played by the China Development Bank (CDB), the largest development bank in the world…it lends colossal sums to clients such as Huawei in the form of trade financing, thereby facilitating the expansion plans and market share increase of this telecom giant" [50].

According to a risk profile from RWR Advisory Group from 2018, Chinese state-owned banks have lent Huawei and/or Huawei's customers up to £7.5 billion[51]. A leaked report[52] from the White House in 2018 claimed it had a further credit line of up to £77 billion at its disposal, though this has been disputed by Huawei, which claims it received a £6 billion credit line from CDB in 2004 and a £26 billion credit line in 2009[53].



It is also guaranteed a significant market share inside China, giving it large sums to finance its research and development. With sums like this, Huawei has been able to undercut its European competitors by 18 to 30% (less than actual production cost at times). Naturally, these state subsidies might have been used to facilitate the Chinese tech firm's sudden expansion in the European market, which went from 2.5% to 25% between 2006 and 2014[54]. Despite these aggressive state-subsidized practices, Europe has been slow to respond. In 2014, EU Trade commissioner Karel De Gucht criticized Beijing in an anti-dumping investigation on Huawei and ZTE, noting in an interview with the Financial Times that "they get subsidies… if you have a line of a couple of tens of billions with the bank that you can use at your discretion, this is a huge subsidy"[55]. And CDB is not the only bank lending to Huawei. The Export-Import (EXIM) Bank of China is – according to its own website – "a state bank solely owned by the Chinese government" which has as its main mandate the facilitation of "the export and important of Chinese mechanical and electronic products".

[48] China Development Bank website, available at: http://www.cdb.com.cn (last visited 15 April, 2019)

[49] Simon Rabinovitch, "Q&A: (Almost) all you need to know about the China Development Bank", *Financial Times*, May 29, 2013.

[50] Philippe Le Corre, Alain Sepulchre, *China's Offensive in Europe*, (Washington DC: Brookings Institute, 2016), p88.

[51] A Transactional Risk Profile of Huawei, *RWR Advisory Group*, February 13, 2018, available at: https://www.rwradvisory.com/wp-content/uploads/2019/03/RWR-Huawei-Risk-Report-2-13-18.pdf (last visited 19 April, 2019).

[52] Jonathan Swan, David McCabe, Ina Fried, Kim Hart, "Scoop: Trump teams considers nationalizing 5G network," Axios, January 28, 2018, available at: https://www.axios.com/trump-team-debates-nationalizing-5g-network-f1e92a49-60f2-4e3e-acd4-f3eb03d910ff.html (last visited 29 April, 2019).

[53] Doug Palmer, "Huawei rejects Eximbank chief's China aid claim", *Reuters*, 16 June, 2011, available at: https://www.reuters.com/article/us-usa-china-huawei/huawei-rejects-eximbank-chiefs-china-aid-claim-idUSTRE75F71220110616 (last visited 9 May, 2019).

[54] China's Offensive in Europe, p.13.

This support reveals itself in Huawei's massive global expansion, facilitated through the Digital Silk Road, a part of China's Belt and Road Initiative, helping it deploy more than 10,000 5G-operable base stations abroad[56]. Huawei is also involved in a large number of ICT projects throughout the Belt and Road Initiative, including constructing an overland fibre-optic cable between Xinjiang and the strategic port of Gwadar in Pakistan, as well as ICT projects in Turkmenistan, Kyrgyzstan, Russia, Djibouti, Somalia, Kenya, with a number of submarine cables in the Indian Ocean and South Pacific[57]. EXIM provides funding to states to purchase Chinese digital infrastructure, thus passing risk from Huawei to the borrower. In September 2018, for example, the Bank lent Nigeria £252 million to improve its telecoms infrastructure with Huawei equipment.[58] According to a recent US Government study, "these efforts will allow China to promote its preferred standards and specifications for 5G networks and will shape the global 5G product market going forward."[59]

Findings:

This chapter has sought to understand the space within which tech companies – such as Huawei must operate within the Chinese Party-State. We have sought to allude only briefly to Huawei's own unique internal structure, leaving that until the next chapter. Instead, we have sought to sketch out how centralized the high-tech economy is becoming in the PRC and how this influences corporate decision-making. This is particularly important because it shows not only strategic direction, but also financing, two sides of the same coin, which bind successful Chinese companies to Beijing.

1. Having considered China's push for closer Civil-Military Fusion in key areas that Huawei operates – such as 5G, quantum cryptography and artificial intelligence – it is likely that Huawei will be pushed to work more closely with defence firms.

2. China's current military doctrine emphasises warfare as conflict between systems rather than armies. In any future conflict, it would seek sudden and decisive attacks on the networks of a potential enemy, to win without fighting.

3. Huawei seems to be treated by Chinese state banks as if it were a state-owned enterprise, with some claiming that it has borrowed £7.5 billion and holds a £77 billion credit line to help facilitate its global expansion in the Belt and Road Initiative (BRI) and helping it undercut European telecoms by 18-30%.

4. Deploying 5G technologies abroad allows the Chinese state to promote its preferred standards and specifications for global 5G networks and will heavily shape the future of the 5G global market.

[55] Shawn Donnan, "EU Commissioner attacks China's Telecoms Subsidies", *Financial Times*, March 27, 2014, available at: https://www.ft.com/content/d6d0bcc6-b5cb-11e3-b40e-00144feabdc0 (last visited 1 May, 2019).

[56] Isao Horikoshi, Takashi Kawakami, "Telecom's 5G revolution triggers shakeup in base station market," *Nikkei Asian Review*, December 2018, available at: https://asia.nikkei.com/Business/Technology/Telecom-s-5G-revolution-triggers-shakeup-in-base-station-market (last visited 29 April, 2019).

[57] Rick Umback, "Huawei and Telefunken: Communications Enterprises and Rising Power Strategies,", *ASPI, Strategic Insights*, 17 April, 2019, available at: https://www.aspi.org.au/report/huawei-and-telefunken-communications-enterprises-and-rising-power-strategies (last visited 6 May, 2019).

[58] Louis Lucas, James Kynge, "Huawei continues global push despite setbacks in West" *Financial Times*, December 16, 2018.

[59] Milo Medin, Gilman Louie, "The 5G Ecosystem: Risks & Opportunities for DOD," Defence Innovation Board, April 2019, available at: https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF (last visited 29 April, 2019).

Chapter 3
ASSESSING HUAWEI'S RELATIONSHIP WITH THE PRC

"I think it really boils down to an issue of will the company take some steps to make themselves more transparent about their operations, and what their ultimate goals is, especially this relationship with the Chinese Government, and the Chinese Communist Party and with the People's Liberation Army." [60]

Chris Johnson, *former CIA analyst, 2012*

According to its website, Huawei describes itself as "a leading global provider of information and communications technology (ICT), infrastructure and smart devices… with integrated solutions across four key domains – telecoms networks, IT, smart devices, and cloud services" [61]. While one constantly sees comparisons between Apple and Huawei in Western media, they are misplaced as Huawei provides services across a broad spectrum of what Western tech firms normally handle. For example, Huawei provides the handsets of Apple, the telecoms architecture of BT, and the ICT and cloud-data storage of Google. In the last two services – relevant to arguments laid out in this report – Huawei's achievements are impressive, as the Chinese company has come to provide subscriber data management (SDM[62]) services to up to 300 carriers in over 130 countries[63], a stunning achievement for a company that was little-known in the West only ten years prior. It has become the world's leading vendor, with a 28% share of the global market, and have gone from (since 2010) from 3% to 46% in the Asia Pacific and 17 to 30% in Europe[64]. Such a spectacular rise is all the more puzzling, when one considers how little we know about the company. It is not publicly listed, and nor do we have much more than basic outlines of its internal structure and inner workings, which include its Shareholders Meeting, its Board of Directors (BOD), the BOD's Executive Committee, and the Supervisory Board[65]. Indeed, such is the secrecy of Huawei that when the US House of Representatives Intelligence Select Committee invited the company to submit documents in 2012 to ameliorate US concerns, Huawei "refused, apparently because to turn over internal corporate documents would potentially violate China's state-secret laws" [66].

[60] Foreign Involvement in the Critical National Infrastructure, *Intelligence and Security Committee*, June 2013, available at: https://www.parliament.uk/documents/other-committees/intelligence-security/Critical-National-Infrastructure-Report.pdf (last visited 29 April, 2019), p.6-7.

[61] "Corporate Introduction", Huawei Website, available at: https://www.huawei.com/en/about-huawei/corporate-information (last visited 16 April, 2019).

[62] According to the Frost & Sullivan report, "SMD allows operators to consolidate and manage their cross domain subscriber data encompassing access preferences, authentication, services, identities, location, and presence into unified data repositories".

[63] "Global Subscriber Data Management", *Frost and Sullivan, Market Research White Paper*, available at: http://www.frostchina.com/wp-content/uploads/2017/09/Final-Report_Globa-SDM-Market-Research-White-Paper_FS_09272017.pdf (last visited 20 April, 2019)

[64] Stephane Teral, Mobile Infrastructure Market Tracker, *IHS Markit*, April 9, 2019, available at: https://technology.ihs.com/597910/mobile-infrastructure-market-tracker-q4-2018 (last visited 1 May, 2019).

[65] "Corporate Governance Overview", *Huawei Website*, available at: https://www.huawei.com/en/about-huawei/corporate-governance/corporate-governance (last visited 18 April, 2019).

[66] "Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE," U*S House of Representatives, Permanent Select Committee on Intelligence*, available at: https://www.hsdl.org/?view&did=722516 (last visited 20 April, 2019).

Links to the China's Security Forces

One of the primary issues related to Chinese allegations of hacking is not so much that Chinese government-linked hackers carry out mass intrusions into Western defence institutions, but that they seem to appear to target technical and economic sectors too. The BfV, Germany's domestic intelligence unit, reported in June 2017, that Chinese spying focuses on "industry, research, technology and the armed forces, as well as policies which – from a Chinese perspective – threaten national unity and the Communist Party's monopoly on power" [67]. Naturally, Huawei's refusal to turn over documents to the US Congress only added fuel to the concerns around Huawei's opaque nature and potential connections to the Chinese Party-State. According to the aforementioned National Intelligence Law of 2017, there is even a requirement in Article 11, that cooperation with intelligence officials take place outside China,

"National Intelligence work organs launch intelligence work inside and outside of the borders on the basis of work requirements, and by using the necessary methods, means and channels according to the law." [68]

This has led many to believe that Huawei regularly cooperates with China's intelligence and military organs. In 2013, the Intelligence Bureau (IB) of India, reported to its National Security Council that Huawei was part of a Chinese army project called "PLA-863", which mandated the company build army switches and routers, while ZTE worked on mobile and fibre networks. The article stated concerns among India's agencies that, "malicious hardware or software implants could be a potent espionage tool for penetrating sensitive and strategic Indian national security sectors which could be exploited in any future conflict with India." [69] As an RWR report indicates, Huawei should not be able to take part in China's military procurement due to strict regulations regarding the acquisition of PLA equipment from non-government sources. This indicates that Huawei has some sort of special status with the PLA.

Perhaps the most damaging claims have come from *Forbes*, which claimed that Huawei was working with Bo Yu Guangzhou Information Technology Co (Boyusec) [70]. This company has been linked by cybersecurity researchers to one of the more advanced Chinese government-sponsored espionage groups. This company is listed in a US Department of Justice indictment, which claims that the group targeted trade secrets related to technology. According to an unnamed US official, Boyusec is "closely connected to the

> *"Boyusec is closely connected to the [Ministry of State Security] and they are developing a start-up program with Huawei that will use malware allowing for capturing and controlling devices."*

[67] "Brief summary of the 2016 Report on the Protection of the Constitution",*Verfassybgsschutz website*: available at: https://www.verfassungsschutz.de/download/annual-report-2016-summary.pdf (last visited 2 May, 2019), p.32.

[68] National Intelligence Law of PRC (2017), on *China Law Translate* website, available at: https://www.chinalawtranslate.com/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E5%9B%BD%E5%AE%B6%E6%83%85%E6%8A%A5%E6%B3%95/?lang=en (last visited 28 May, 2019).

[69] Joji Thomas Philip, "NSC points to Huawei, ZTE's links with Chinese military," *The Economic Times*, May 15, 2013, available at: https://economictimes.indiatimes.com/news/politics-and-nation/nsc-points-to-huawei-ztes-links-with-chinese-military/articleshow/20056800.cms (last visited 2 May, 2019)/

[70] Thomas Brewster, "Chinese Trio Linked to Dangerous APT3 Hackers Charged with Stealing 407GB of Data from Siemens", *Forbes*, 27 November, 2019, available at: https://www.forbes.com/sites/thomasbrewster/2017/11/27/chinese-hackers-accused-of-siemens-moodys-trimble-hacks/#76d5253919ef (last visited 9 May, 2019).

[Ministry of State Security] and they are developing a start-up program with Huawei that will use malware allowing for capturing and controlling devices." [71] While Huawei confirmed that it had a relationship with Boyusec, it insisted that this was limited to Boyusec providing evaluations of Huawei's internal corporate internet.

The Nature of Huawei Ownership

One of the most significant arguments made by Huawei founder Ren Zhengfei has been that Huawei is a private company[72]. However, there are telling signs beyond those described above which indicate strong state support. In addition to the sudden detention of two former Canadian diplomats in China after the arrest of Huawei Chief Financial Officer Meng Wanzhou – Ren's daughter – there is also the fact that she possessed eight passports, including a valuable 'public affairs' passport[73], which are only traditionally issued by China to diplomatic staff, those working in foreign affairs offices, state-owned enterprises, and financial institutions where the state is a controlling interest[74].

When asked if Huawei would ever go public, Huawei's founder has said that going public would be "bad for morale" [75]. However, there are other possible reasons which might also be factored in, which include wanting to avoid legal requirements to report company structure, auditing data, and financial statements relating to cash flow, equity, and balance sheets to the public, to public shareholders, and to authorities such as the US Securities and Exchange Commission. While Huawei founder Ren Zhengfei's close links to the People's Liberation Army (PLA) and Chinese Communist Party (CCP) membership of has been discussed widely in the media[76], there has been little said about Huawei's other ties to the CCP. According to the ASPI website, *Mapping China's Tech Giants* [77], Huawei counts 12,000 CCP members among its employees and had established 300 CCP branches by 2007. Its Chairwoman from 1999 to 2018, Sun Yafang, previously held senior posts in the Ministry of State Security as well as Chinese Government research centres[78].

Huawei has based its claim to be a private company on its Employee Stock Ownership Programme (ESOP), also called the "silver handcuffs" [79] programme by insiders. While Huawei's claim to be a privately-owned has been vigorously defended by the company, a recent report by two scholars[80] on China's political economy indicates another avenue

[71] Bill Gertz, "Pentagon Links Chinese Cyber Security Firm to Beijing Spy Office", *The Washington Free Beacon*, November 29, available at: https://freebeacon.com/national-security/pentagon-links-chinese-cyber-security-firm-beijing-spy-service/ (last visited 1 May, 2019).

[72] Sophie Curtis, "Ex-CIA chief accuses Huawei of industrial espionage", *The Telegraph*, 19 July, 2013, available at: https://www.telegraph.co.uk/technology/news/10191154/Ex-CIA-chief-accuses-Huawei-of-industrial-espionage.html (last visited 1 May, 2019).

[73] Michael Mui, "How Meng Wanzhou's 'P' passport works", *The Star: Vancouver*, 23 January, 2019, available at: https://www.thestar.com/vancouver/2019/01/23/how-meng-wanzhous-p-passport-works.html (last visited 1 May, 2019)..

[74] "Huawei: Communist Party Activities", Mapping China's Tech Giants: *ASPI*, available at: https://chinatechmap.aspi.org.au/#/company/huawei (last visited 23 April, 2019).

[75] Tian Tao, et al, Huawei: *Leadership, Culture, and Connectivity* (New Delhi: Sage Publications, 2017), p.68.

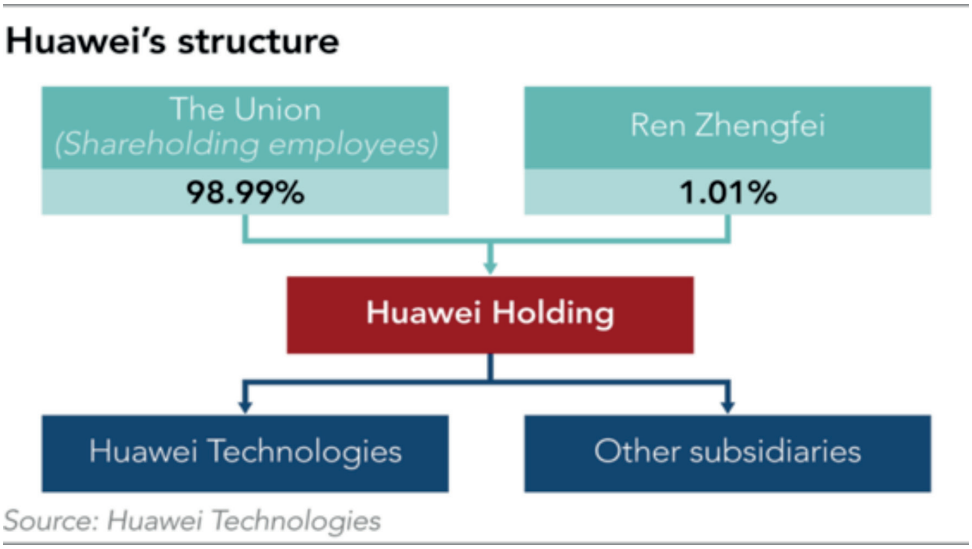
[76] See Chua Kong Ho, "Huawei founder Ren Zhengfei on why he joined China's Communist Party and the People's Liberation Army," *South China Morning Post*, 16 January, 2019; Eamon Barrett, Huawei Founder Ren Zhengfei Breaks Silence as Global Pressures Mount, Fortune, 18 January, 2019;

[77] "Huawei: Communist Party Activities", Mapping China's Tech Giants: *ASPI*, available at: https://chinatechmap.aspi.org.au/#/company/huawei (last visited 23 April, 2019).

[78] Ibid.,

[79] Tian Tao, et al, *Huawei: Leadership, Culture, and Connectivity* (New Delhi: Sage Publications, 2017), p.81.

[80] Christopher Balding, Donald Clarke, "Who owns Huawei?" *SSRN*, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3372669 (last visited 7 May, 2019).



for influence between the Party State and the company. Christopher Balding and Donald Clarke have questioned the company's argument that shares in the organization are evidence of its "private" nature In reality, "employee shares were not typical of a registered Chinese company's shares: they were not transferable, carried no votes, and could not be retained if employees ceased to work at the firm" [81]; their stock is in fact contractual interests in a profit-sharing scheme. What's more, if one looks at ownership structures, then a more troubling picture emerges. Huawei – also known as Huawei Technologies, Inc. – is owned 100 percent by Huawei Investment & Holding, a much smaller company with only a few hundred employees. This holding company is in turn co-owned by founder Ren Zhengfei, with "nearly 1.01%" and a state-operated trade union, called Huawei Investment & Holding Company Trade Union Committee (HHTUC), with the remaining 98.99%. Given its massive ownership of Huawei Holdings, the question of who controls HHTUC is of paramount importance in understanding Huawei. This committee, Balding and Clarke argue, is governed by Chinese labour law, which dictates that trade union officers are appointed by superior trade union organizations, which in turn report up to the All-China Federation of Trade Unions (ACFTU).

Trade Union Ownership

It is important to briefly discuss both Chinese trade union law and the place that Huawei Holding Trade Union Committee holds under the ACFTU, as it reveals Huawei's connections to the Party-State bureaucracy. Feng Chen, a Hong Kong-based scholar in Chinese political economy asserts that trade unions in China are part of the government bureaucracy, subject to the same pay scales and administrative salaries as state employees and paid from the public treasury: "union bureaucracies' power and operations are decisively reliant on their formal government status" [82]. All trade unions are obliged to belong to this government federation and previous attempts by workers to create independent trade unions – including those in 2018 – have been met with massive police cracks downs[83]. In

[81] D Cheng, L Liu, *The Truth About Huawei*, (Beijing: Dangdai zhongguo chubanshe, 2004), p.116.

[82] Feng Chen, *Union Power in China Source, Operation, and Constraints*, Journal of Modern China, Vol. 35, Issue 6, (2009), pp.662-689.

[83] "Chinese workers demand release of labor rights activists", *The Japan Times*, April 22, 2019.

China, the Trade Union Law of 1992[84] governs how trade unions are organized and how they interact with the CCP. While Huawei's recent statements regarding the trade union "it is not involved in any decisions connected to Huawei's business and operations...and oversees activities such as badminton and hiking", the Trade Union Law is very clear on the trade unions relationship with the Party-State:

(i) the system is to be homogenous and presided over by ACFTU;

(ii) the CCP shall have supremacy over the unions and the latter shall accept the leadership of the Party;

(iii) the organizational levels of trade unions shall be related to one another in terms of Lenin's concept of democratic centralism, which makes lower-ranking unions subordinated to higher-ranking ones;

(iv) the trade unions shall shadow the Party and the state administration at all levels;

(v) grassroots (enterprise unions) shall have dual membership[85]

"Trade unions in China are part of the government bureaucracy, subject to the same pay scales and administrative salaries as state employees and paid from the public treasury."

According to Zana Bugaighis, an expert on China trade union law, the "the ACFTU governing members are closely aligned with the CCP" [86] and that "major changes in the 2001 amendment to the Trade Union Law show that motivation behind the amendment came from a desire for trade unions to play a more active role in helping the CCP control workers" [87]. According to Jeffrey Henderson, Professor Emeritus of International Development at the University of Bristol, "Huawei has a Party branch, currently headed by Zhou Daiqi. Although Mr Zhou is Huawei's Director of Ethics and Compliance, it might be in his role as Party Secretary that he serves as a member of Huawei's Executive Committee" [88]. It might well be that such positions allow for the Party to influence decision-making within the company.

One of the defining characteristics of the ACFTU is that trade union officials hold high-ranking positions in the CCP, with the current ACFTU chairman, Wang Dongming, having held positions on the 19th Central Committee and the Chinese People's Political Consultative Conference (CPPCC)[89]. Worryingly, the CPPCC has been called the "highest-ranking entity overseeing the United Front system" by the US-China Economic and

[84] Trade Union Law (promulgated by the Standing Committee National People's Congress, April 3, 1992, amended by Standing Committee National People's Congress, October 27, 2001, translated in CHINA LAWS FOR FOREIGN BUSINESSES (CCH) 12-501 (2004) (PRC), available at: http://www.acftu.org.cn/unionlaw.htm [hereinafter the Trade Union Law].

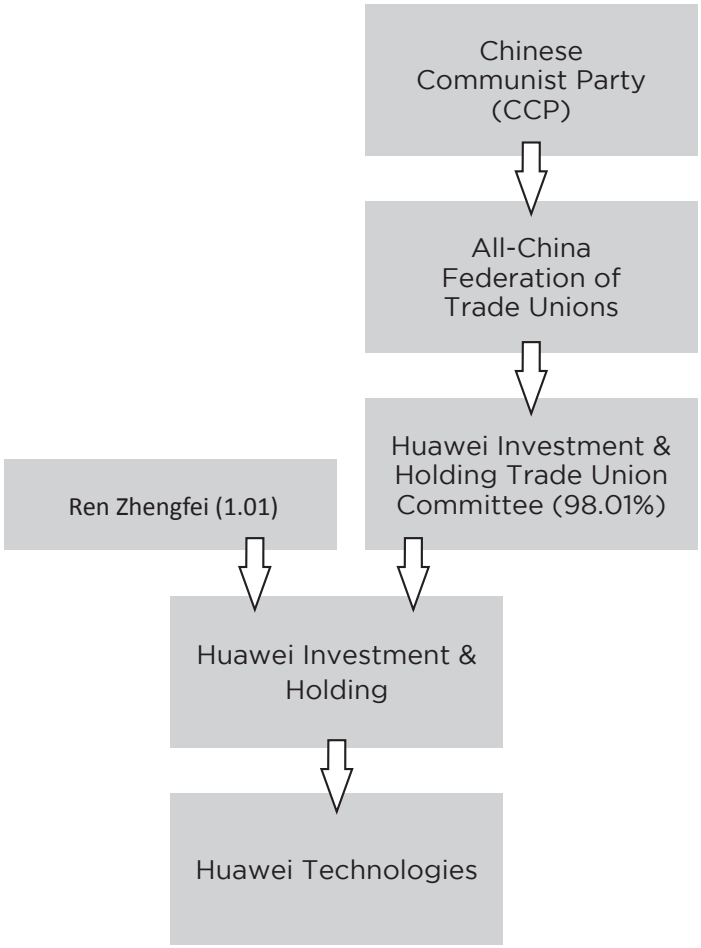
[85] Trade Union Law (promulgated by the Standing Committee National People's Congress, April 3, 1992, amended by Standing Committee National People's Congress, October 27, 2001, translated in CHINA LAWS FOR FOREIGN BUSINESSES (CCH) 12-501 (2004) (PRC), available at: http://www.acftu.org.cn/unionlaw.htm [hereinafter the Trade Union Law].

[86] Zana Z. Bugaighis, "What Impact will the Revised Trade Union Law of China have on foreign business?", *Pacific Rim Law and Policy Journal Association,* Vol. 16, No.2 (2007), p.409.

[87] Bugaighus, (2007), p.414.

[88] Interview with author, 26 April, 2019.

[89] This was found on his Wikipedia site:



Security Review Commission[90]. The United Front – called one of three "magic weapons" by Chairman Mao Zedong – is a propaganda and influence department has been recently received a boost in support and funding from President Xi Jinping.[91] While no one believes Huawei to be connected to the United Front, it is troubling that in Chinese trade union leadership, those connections exist. The idea that the ACFTU's traditional role of exerting political influence on international labour movements as an arm of the "United Front" is also found in 2006 report by the International Confederation of Free Trade Unions (ICFTU)[92]. Huawei has issued a rebuttal[93] of the claim that it is owned by a trade union, saying that while Huawei employees are not registered shareholders as defined by law, they are the actual owners of the company, as their shares give dividends, give employees a voting interest in the company's governance, and would translate into a share of the company's assets if liquidated. In response, Balding has stated that Huawei

[90] Alexander Bowe, China's Overseas United Front Work: Background and Implications for the United States, US-China Economic and Security Review Commission, available at: https://www.uscc.gov/sites/default/files/Research/China%27s%20Overseas%20United%20Front%20Work%20-%20Background%20and%20Implications%20for%20US_final_0.pdf (last visited 23 April, 2019)

[91] Bowe (2018), p.5.

[92] "International Trade Union Guide to Contacts with China and the All-China Confederation of Trade Unions (ACFTU)", *International Confederation of Free Trade Unions, Global Union Federations*, Available at: https://www.ftf.dk/fileadmin/multimedia/eu_og_internationalt/No_E_36_ICFTU_and_GUF_China_Guide_May__2006.pdf (last visited 17 April, 2019).

[93] Li Tao, "Huawei fights back against claim in research paper that it is government controlled," South China Morning Post, 25 April, 2019, available at: https://www.scmp.com/tech/big-tech/article/3007649/huawei-fights-back-against-claim-research-paper-it-government-funded (last visited 29 April, 2019).

have not denied the central claim of trade union ownership. "They actually admit the point we make that employees do not legally own the company." [94] It is clear from this that more clarity about Huawei's ownership structures is required.

Findings:

In looking at the relationship between Huawei and the Chinese Party-State, we have sought shed light on whether or not the allegations of close links were verifiable. Pursuing this, we have shown that indeed there are strong signs of economic and political linkages, which seem to indicate that Huawei plays a part of the PRC's wider technological and global supply-chain ambitions. While the recent allegations made by the Central Intelligence Agency (CIA) asserting[95] that Huawei has been funded by the Ministry for State Security are of importance, we have sought to show that the place that Huawei holds in the Chinese polity is of more interest. In essence,

1. Huawei is alleged to have a special relationship with the PLA, which allows it to take part in procurement tenders. It also alleged to have a relationship with the state-sponsored hacking groups.
2. Huawei is owned 100% by a holding company, which in turn is co-owned by Ren Zhengei (1%) and a trade union committee (99%).
3. Chinese trade unions are not trade unions as recognized in the West, but a part of the Chinese party-state bureaucracy, subject to its pay scales, paid from the treasury, and requiring CCP representation in all leadership positions.
4. It is clear that Huawei's claims to be a private company are highly questionable and need clarification.

[94] Zach Coleman, Huawei hits out at claims of state control through 'employee' stake," *Nikkei Asian Review*, April 25, 2019, available at: https://asia.nikkei.com/Business/Companies/Huawei-hits-out-at-claims-of-state-control-through-employee-stake2 (last visited 1 May, 2019).

[95] Steven Musil, "CIA reportedly says Huawei funded by Chinese state security", *CNet*, April 21, 2019, available at: https://www.cnet.com/news/cia-reportedly-says-huawei-funded-by-chinese-state-security/ (last visited 1 May, 2019).

Chapter 4
RISKS ASSOCIATED WITH HUAWEI IN THE UK'S DIGITAL INFRASTRUCTURE

"Overall, the Oversight Board can only provide limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks can be sufficiently mitigated long-term." [96]

Huawei Cyber Security Evaluation Centre, *Annual Report, March 2019*

In attempting to understand the importance of the UK debate over Huawei, this report seeks to assess the security risks presented by Huawei's participation in the building of the UK's 5G digital infrastructure. It must be noted that Huawei already participates in the UK's digital infrastructure, which it does under the auspices of the Huawei Cyber Security Evaluation Centre (HCSEC). The HCSEC is governed by an independent Oversight Board, which reports to the National Cyber Security Centre (NCSC) and the Department for Digital, Culture, Media, and Sports (DCMS).

It is extremely difficult to properly assess the ability of the UK Government agencies and HCSEC to mitigate the risk of having Huawei participate in the current 4G network. Representatives from the NCSC met with the authors of this report to explain the principles around which they operate in their efforts as the UK's first line of defence. As explained by Ian Levy, the NCSC's Technical Director, design principles include assuming defence in depth, using multiple vendors in each part of the network, and subsectors, so that single failures don't lead to whole-of-system failure. Levy notes that how the network is run is pivotal to network security, including constant monitoring, in-house auditing of third-party SDM providers, network privilege, and basic password security. His comments highlight an important point: network architecture can contribute to resilience and minimise risk if one avoids overreliance on a single vendor.

"Having looked into Huawei quite a bit a few years ago, I realized the challenges of even having a mitigation plan or strategy for the 4G structure; given the generational shift between 4G and 5G, I am not aware of anything that would give us security against the challenges it would impose upon us."

Katheryn Wheelbarger, *Acting Assistant Secretary of Defense for International Security Affairs, US Department of Defense - March, 2019*

Despite this, the Oversight Board of HCSEC itself has made clear that Huawei's inclusion into the UK's digital infrastructure presents "significantly increased risk to UK operators which requires ongoing management and mitigation"[97]. Three further findings stand out: First, that the Oversight Board could only provide "limited assurance that the long-term security risks can be managed in the Huawei equipment currently deployed in the UK"[98]; Huawei has done nothing to remedy its problematic approach toward software development since the previous 2018 report. Second, the Oversight Board

[96] "Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board: Annual Report 2019," *HCSEC Oversight Board*, March 2019, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf (last visited 20 April, 2019).

[97] *Ibid.*,

[98] "Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board: Annual Report 2019," *HCSEC Oversight Board,* March 2019, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf (last visited 20 April, 2019).

"In a 5G network, these core functions will be largely virtualized, that is rather than propriety hardware they will be software running on standard processors and moved to the end of the network in order to improve latency and increase latency and increase network capacity and speed."

Malcolm Turnbull, *former Prime Minister, Australia (on Australian concerns)*

has no confidence in Huawei's "capacity to successfully complete the elements of its transformation programme"[99]. Third, there are also indications from both the private sector and from US military leaders[100] that cast doubt on the UK's ability to mitigate risks related to using Huawei components. As we have learned from the leaked National Security Council meeting, the UK may intend to allow Huawei access to "non-core" functions such as antennas and other "dumb" components[101]. In networks, there are core or control planes, which handle sensitive data and manage traffic and there are non-core planes, boxes and antennas that handle data without reading it. There are two problems with the argument that Huawei can be kept out of the "core".

First, the "core" concept is becoming less relevant as 5G technology matures. Security can no longer be thought of as protecting a fixed perimeter as the global industry transitions to software defined networking (SDN) and network function virtualisation (NFV) standards that will enable more open, interoperable networks. Moving to inherently modular and software based systems will make it easier to replace damaged or compromised components. With regard to this new ability to re-purpose parts of the network, one US official told the *Financial Times* in March 2019, "While a huge opportunity, it is also deeply concerning to us from the perspective of national security"[102].

Second, the manufacturer could "manage" these the so-called "dumb" components, such as antennas, thereby preventing the communication link between base stations or users. It should be noted that in the case of 5G, an 'antenna' is not an old-fashioned whip antenna, extending out of a radio case. It is instead a massive multiple-input/multiple-output (MIMO) antenna, closely integrated with the hardware and software required for transmission and reception of radio signals, and signal processing algorithms to support the execution of the entire system. The antennas are advanced and allow for electronic beam steering with no moving parts. The signals receive in devices will be more like a pencil beam than a broadcast, allowing for a more consistent experience.

Network Control: This is quite a wide band of risk, ranging from mild interference to complete architectural shut-down. Obviously, this report does not predict the Chinese state readily and easily demanding that Huawei use that capability, but the high damage such a possibility would lead to demands serious discussion and consideration. The leaked solution proposed by the National Security Council has been to relegate Huawei components to the peripheral elements, such as antenna. However, this solution is

[99] *HCSEC Annual Report*, March 2019.

[100] National Security Challenges and US Military Activities in Europe, Full Committee Hearing, *US Congress, Armed Services Committee*, March 13, 2019, available at: https://armedservices.house.gov/2019/3/national-security-challenges-and-u-s-military-activities-in-europe (last visited 20 April, 2019).

[101] Steven Swinford, Charles Hymas, "Theresa May defies security warnings of ministers and US to allow Huawei to help build Britain's 5G network", *The Telegraph*, 24 April, 2019, available at: https://www.telegraph.co.uk/politics/2019/04/23/theresa-may-defies-security-warnings-ministers-us-allow-huawei/ (last visited 25 April, 2019).

[102] Kiran Stacey, David Bond, "Trump officials warn that UK's 5G approach imperils security", *Financial Times*, 19 March, 2019, available at: https://www.ft.com/content/12e42a00-499b-11e9-8b7f-d49067e0f50d (last visited 29 April, 2019).

"The NCSC – the first line of defence of the UK – can be easily bypassed. There is nothing in computer science right now that can detect an errant piece of code or a malicious piece of code if it wants to be hidden. The only time we get to see it, is when it's activated. So there is no fool-proof way of ensuring that every strand of code that is written into hardware and software by Huawei is 100% secure."

Telecom engineer, *interview with author, 21 March, 2019*

really no solution at all for the very simple reason that a manufacturer of hardware can introduce modifications into the circuitry of a system – called a hardware Trojan (HJ) – which passively carries out its normal functions unless triggered. In the case of a Huawei-built antenna, there is a high-level of risk that:

a. UK cyber experts could not find such hardware Trojans[104] even if they searched for them. There are documented cases where governments have searched for such Trojans and still not found them all after two years of searching.

b. UK cyber experts would not be able to remove them using conventional antivirus software, even if they did find them.

c. Even if a third-party introduced such malicious code, Huawei itself would have trouble removing it because their engineering product cycle is not consistent[105].

Some worry about the possibility of system shutdowns be used in case of severe conflict between the UK and China. While one might argue this set of circumstances is unlikely, it's also rather dangerous providing such a major lever to a foreign power that is well-known for cyber espionage.

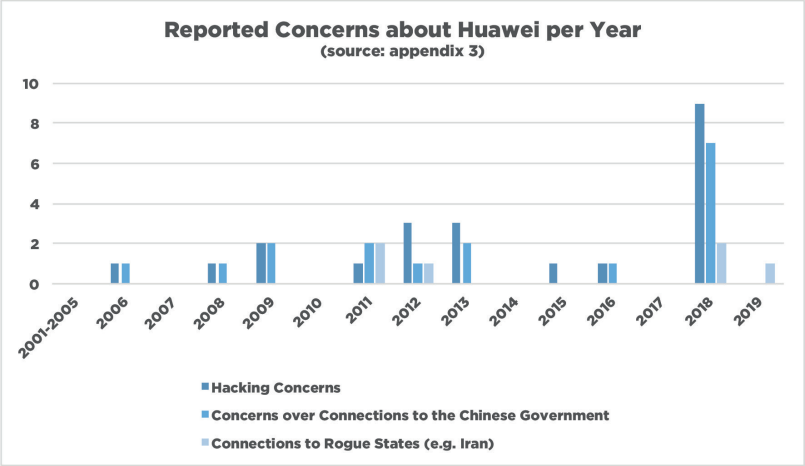
Data Breach: the most obvious risk to the UK in having a Chinese-directed company build 5G for British telecoms companies is that of espionage or data-tracking. Of course, cyber hacks exist all the time, but there is a substantial difference in preventing attacks from external sources and preventing (or even noticing) attacks from within. The primary risk is of course the access to UK data that Huawei would gain as an ICT service provider. This means that it would need to be informed of vulnerabilities in the regular maintenance of the system and would need to provide British carriers with patches. These patches could be designed to introduce new functionality over a number of updates, using code that is completely different from that tested in the laboratory conditions of HCSEC. In other words, a company could upload a bit of code that is harmless in the first patch, but which becomes malicious in a later patch. That company could also add patches or new code to network hypervisors, which are a particularly important element of a 5G network. These hypervisors allow for network slicing and virtualization and would be vital to managing the virtual core slices of the network.

"it is just impossible to go through that much – over a million lines of code and be absolutely confident you have found everything."

Oral evidence, ***GCHQ, Intelligence and Security Committee,*** *Foreign Involvement in the Critical National Infrastructure, 24 January, 2008*

[104] Keoni Everington, "After report on Huawei's Trojan Horse, Taiwan retains ban on China-made gear", *Taiwan News*, 10 December, 2018, available at: https://www.taiwannews.com.tw/en/news/3593407 (last visited 25 April, 2019).

[105] "Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board: Annual Report 2019," *HCSEC Oversight Board*, March 2019, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf (last visited 20 April, 2019).



Furthermore, there are issues around the hosting of its servers in China, allowing for near-time monitoring of data by Chinese intelligence officials *with or without* Huawei's knowledge. This of course has political impact, but it also could have economic risks. Would Chinese companies be able to outbid their British competitors, privy to internal discussions, budgets, or manufacturing capabilities? Would law firms that deal in mergers and acquisitions find themselves unable to stop data leakage? Huawei has sought to reassure Western publics that they would never spy on behalf of China, but there are a unusually high number of allegations[106] against them in the media and the US Department of Justice has cited a number of issues in its January 2019 indictment[107], including allegations that Huawei offered bonuses to employees who stole intellectual property.

Infrastructure and the Internet of Things (IoT): 5G's much broader data flow, low latency and speed, will allow a host of new uses in manufacturing, self-driving cars, telemedicine, and doubtless many other as-of-yet-unknown sectors[108]. Recent estimates indicate that Huawei and ZTE hold a combined 41% of overall market share for network infrastructure, followed by Ericsson at 27% and Nokia with 23%[109]. UK Government minister cite the need to ensure a multitude of tech providers. It is becoming clear in reality that Huawei is building a dominant global position.

This raises a number of potential risk areas; around which we do not yet have full understanding. If the IoT involves the connecting of critical national infrastructure (CNI), controlling electricity, water, and other essentials, how much of a vulnerability is it to have our network built by a state with whom the UK is sometimes at odds? The Chinese state is increasingly confident about using geo-economic tools to coerce states into submitting to its policy preferences. Strategic plans such as Made in China: 2025 assert China's vision to become a global leader in the production and export of high-tech industries[110]. To that end, establishing a global competitive supply chain for the communications infrastructure aligns both China's state-sponsored industrial policy and its geopolitical goals. Some of these goals are hegemonic

In 2016, the MSS is said to have hacked into the US Office of Personnel Management (OPM), stealing more than 22 million records of US government officials

[106] See Appendix 1 for an index of accusations of espionage made against Huawei in various media outlets.

[107] "Chinese Telecommunications Device Manufacturer and its US Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction of Justice", *US Department of Justice Website*, 28 January, 2019, available at: https://www.justice.gov/opa/pr/chinese-telecommunications-device-manufacturer-and-its-us-affiliate-indicted-theft-trade (last visited 6 May, 2019).

[108] Ian Levy, "Security, Complexity and Huawei; Protecting the UK's telecom's networks", *NCSC Website Blog Post*, 22 February, 2019, available at: https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks (last visited 25 April, 2019).

[109] Stephane Teral, Mobile Infrastructure Market Tracker, *IHS Markit*, April 9, 2019, available at: https://technology.ihs.com/597910/mobile-infrastructure-market-tracker-q4-2018 (last visited 1 May, 2019).

[110] "Made in China 2025", *MERICS Paper on China*, December 8, 2016, available at: https://www.merics.org/en/papers-on-china/made-china-2025 (last visited 1 May, 2019).

and destabilising and to submit to them would be in itself dangerous; for example, during his New Year's Address, PRC President Xi Jinping insisted that China and Taiwan would ultimately be reunified – by force, if necessary[111]. The United States, obliged to defend Taiwan, is also moving toward a strategic competition with the PRC, and the two states are developing a relationship fundamentally different from that which has existed for the past thirty years. It might not be a "new Cold War", but it is certainly an age of increased geopolitical competition, one in which the UK's place as a traditional American ally, and defender of the rules-based international system, will put London increasingly at odds with Chinese geostrategic ambitions. The possibility of Beijing weaponising its operational control of the UK's national infrastructure in pursuit of its national goals in a form of state blackmail on a strategic and global scale cannot and should not be discounted.

Influence and the IoT: In 2018, Huawei unveiled a digital platform for smart cities at the Smart City Expo World Congress in Barcelona. In the UK, it is trialling smart city programmes, with the Chinese company going so far as to commission a Smart Cities Index to helpfully assess the current state of smart city development[112]. While such future technologies have much to offer the UK's economic development, there are questions about the societal impact that they will have. Already, it is clear that China's Ministry of State Security (MSS) is interested in large data sets of Western government officials to facilitate recruitment and espionage. In 2016, the MSS is said to have hacked into the US Office of Personnel Management (OPM), stealing more than 22 million records of US government officials[113]. The use of AI and big data sets is increasingly the purview of intelligence agencies as well as tech firms, and China has begun to develop smart city technologies to track and shape the political behaviour of its population. This Orwellian high-tech system has allowed Chinese security forces to monitor in real time millions of individuals in the Uyghur autonomous region[114], and to develop metrics by which political behaviour might be graded[115]. This issue – that of the risk to liberal societies – is one that remains murky even to engineers and ICT professionals currently working on 5G. We do not yet know what vulnerabilities will open up when we go from having 10,000 devices per square mile to 3 million per square mile.

> *"5G gives you much more access to the population, in terms of having more ways to surveil and influence people…in the past, we talked of states hacking computers. I worry about authoritarian states using new tech, big data and AI, to 'hack' people."*
>
> ***Dr Robert Spalding,*** *Fellow, Hudson Institute24 January, 2008*

While it's true that social media companies in the West have also been accused of

[111] Xi Jinping says Taiwan 'must and will be' reunited with China", *BBC News*, 2 January, 2019, available at: https://www.bbc.co.uk/news/world-asia-china-46733174 (last visited 1 May, 2019).

[112] Eric Woods, et al, "UK Smart Cities Index 2017, Huawei / Navigant, 23 October, 2017, available at: https://e.huawei.com/uk/marketing-material/onLineView?MaterialID={A81CFA81-C7A8-4E8F-A088-963C7E73F3CC} (last visited 20 April, 2019).

[113] Aruna Viswanatha, Dustin Volz, "China's Spying Poses Rising Threat to US", *Wall Street Journal*, April 28, 2019, available at: https://www.wsj.com/articles/chinas-spying-poses-rising-threat-to-u-s-11556359201 (last visited 1 May, 2019).

[114] Lily Kuo, "Chinese surveillance company tracking 2.5m Xinjiang residents", *The Guardian*, 18 February, 2019, available at: https://www.theguardian.com/world/2019/feb/18/chinese-surveillance-company-tracking-25m-xinjiang-residents (last visited 1 May, 2019).

[115] Bernard Marr, "Chinese social credit score: utopian big data bliss or Black Mirror on steroids?" *Forbes*, 21 January, 2019, available at: https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/#183beac348b8 (last visited 1 May, 2019).

misusing big data[116], most of their founders and employees have grown up immersed in liberal traditions. Would this be the same with a 5G built with Huawei expertise and engineering? Or would it allow for a new level of Chinese influence campaigns upon Western foreign policy elites? Would the location of serving members of secret agencies or the Armed Forces, politicians or those in sensitive business be vulnerable to real-time monitoring in Beijing? After all, UK political leaders and civil servants still use commercial networks when going about their private lives. If their behaviour and habits are tracked and analysed using big data, are we likely to see subtler influence campaigns? Robert Spalding, until recently Senior Director for Strategy in the US National Security Council, and a contributor to this report, has argued that many of the vulnerabilities of 5G are as-of-yet unknown, "5G gives you much more access to the population, in terms of having more ways to surveil and influence people…in the past, we talked of states hacking computers. I worry about authoritarian states using new tech, big data and AI, to 'hack' people.[117]" While it might sound outlandish, the PRC has already shown itself adept at persuading Western officials to work on its behalf[118]. Rather than adopting a passive approach, the UK Government and its allies should identify clear goals in research and development, which allow for Western leadership in the emerging technical standards, norms, and governance models.

Analysing Risk

In analysing risk, one must understand how risk is inserted into a network. A Trojan Horse in computing is a malicious computer programme that misleads users concerning its true intent. In information and communications technology (ICT), however, it is not just the 'system' but also the sub-systems that matter. For example, the 5G network relies upon a complicated series of active advanced antennae, that control the radiation pattern, gain, bandwidth, polarisation, and frequency range and power across the network. The key to multiple input, multiple output (MIMO), and the ability to control multiple data streams using the same time and frequency resource is the 'antenna'. Hence, whoever controls the antenna controls the network. For the sake of argument, Huawei could insert a backdoor within the antenna to sit dormant until it required it and there is no way that either NCSC or GCHQ would be able to find it. There is also a serious difference from 4G, which weakens UK claims that its risk mitigation procedures are sufficient. As one senior US official told the *Financial Times*, "One analogy that we can often use is, one minute you're holding a 5G coffee cup that is transmitting back telemetric data on what the temperature is inside. And then the next moment that object can turn into something radically different"[119]. The primary weakness in the NCSC approach toward security, the official continued, was that it was a purely technical mandate, looking at the code or equipment, and not the wider issue of trust in the vendor.

[116] Hilary Osborne, Hannah Jane Parkinson, "Cambridge Analytica Scandal: The Biggest Revelations So Far", T*he Guardian*, 22 March, 2018, available at: https://www.theguardian.com/uk-news/2018/mar/22/cambridge-analytica-scandal-the-biggest-revelations-so-far (last visited 20 April, 2019).

[117] Interview with author, 15 March, 2019.

[118] Nick McKenzie, "Liberal Andrew Robb took $880k China job as soon as he left parliament", *Sydney Morning Herald*, June 6, 2017, available at: https://www.smh.com.au/national/liberal-andrew-robb-took-880k-china-job-as-soon-as-he-left-parliament-20170602-gwje3e.html (last visited 1 May, 2019).

[119] Kiran Stacey, David Bond, "Trump officials warn that UK's 5G approach imperils security", *Financial Times*, 19 March, 2019, available at: https://www.ft.com/content/12e42a00-499b-11e9-8b7f-d49067e0f50d (last visited 29 April, 2019).

Findings:

Looking at the issue of risk, it is clear that despite recent Government assurances that the UK has a wealth of understanding and know-how about Huawei, a number of key issues remain of serious concern.

1. The most recent Oversight Board report (March 2019) makes clear that despite claims that the UK has a system for overseeing Huawei's place inside the UK network, that procedure can offer only limited assurance that the long-term security risks can be managed in the Huawei equipment deployed in the UK.
2. Not only has Huawei done little to assuage the Oversight Board's concerns, but promises to remedy vulnerabilities have also done little to reassure the Oversight Board.
3. The UK's allies – Australia and the United States – do not agree that the UK's approach toward 4G is applicable toward 5G. Specifically, in opposition to the UK position, they believe:
    a. that the differences between core and periphery will not remain as sharply delineated in 5G as they are in 4G;
    b. that network equipment – such as antennas – can simply be re-purposed by a manufacturer once it has been tested and installed;
    c. that one cannot use 5G network equipment without strong trust that there are safeguards from the company in question and the state behind it[120];
4. Risks to the network might entail:
    a. systems control;
    b. data breach;
    c. infrastructure and the IoT;
    d. influence and the IoT.

[120] Dan Sabbagh, "Huawei tech would put UK-US intelligence ties at risk, official says", The Guardian, 29 April, 2019, available at: https://www.theguardian.com/technology/2019/apr/29/drop-huawaei-or-we-could-cut-intelligence-ties-us-warns-uk (last visited 1 May, 2019).

"A 4G antenna works by transmitting and receiving microwave radiation in a pre-shaped fixed sector. The separation of users is by selecting a narrow frequency within a band. The 5G antenna actively focusses the extremely narrow beam towards the handset which means the range is longer, and if the beams do not overlap the same specific frequency can be used for more than one handset.

The more beams, the more users, and the greater the capacity.

These smart 5G base station antennas use from 64 to 128 small antennas such that the beam[s] can be steered electronically by changing the phase of the signal across the elements. This fixed time delay for each squint of the beam results in beam steering, creating a phased array antenna.

Each user is allocated a set of antenna elements at the base station where different delays or phase changes steer the beams electronically.

This technique has been used with radar; e.g. the Samson radar on the Royal Navy Type 45 Destroyer, and sonar systems for many years. However, the base stations are expensive because the beams must be maintained with a narrow shape and they must be kept perfectly aligned with the receiver.

The entire system is software driven, and whoever writes the software will control the antennas. Software is regularly updated so perhaps what worked today might not work in the same direction tomorrow. Physical areas of coverage could be deliberately blanked out by steering nulls in a specific direction."

Professor Peter Varnish, Visiting Cyber Professor, Coventry University

Chapter 5
HUAWEI, THE US, AND 5G

"In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place, oblige it to control itself."

Alexander Hamilton

Robert Spalding, Fellow, Hudson Institute

In the United States, 5G became a national security topic in January 2018 after the leak of a White House report[121], following the completion of the National Security Strategy (NSS). A draft of the report envisioned a complete redesign of the internet, focused on better securing data on a new, superfast wireless network. The redesign concept involved engineers from the major telecom equipment manufacturers responsible for building US carrier networks, who helped policymakers to re-imagine a safer and better-structured network[122]. This study, and the subsequent policy debate it spawned, drew on the premise that China was surpassing the US in the latest wireless technology, 5G. This was itself, the product of a report[123] published earlier that year by Analysys Mason, a telecom consultancy. In that study, it was revealed that China had deployed 350,000 5G-operable base stations, nearly ten times that deployed within the US, and had designated three 200 MHz blocks of spectrum from the mid-band and is conserving reallocating 500 MHz of C-band spectrum[124]. It is investing £139 billion in capital expenditure for its 5G deployment through its three largest telecommunications companies, China Mobile, China Unicom, and China Telecom.

2 US Carriers with Nationwide Spectrum for 5G

1. **Verizon** – High Band (28GHz at 800 MHz spectrum block)
2. **Sprint** – Mid Band (2.5 GHz at 100 MHz spectrum block)

While the US was in 2018 said to be behind China, it still had significant capabilities, with a number of domestic carriers developing and deploying 5G, including Verizon, AT&T, Sprint, and T-Mobile. Of these, only two —Verizon, and Sprint— currently have sufficient nationwide spectrum to build a 5G network and only one is on the mid-band. Verizon had a massive 800 MHz in the high band, but because of the required antenna density, there was no way that spectrum could be deployed quickly to build a nationwide network. Sprint had enough spectrum but was only the fourth largest carrier, and lacked the resources to build a nationwide network. In addition to spectrum issues, it was clear that bureaucratic challenges at the local level were preventing construction of 5G networks. For example, one project in a major metropolitan area was bogged down by requests from more than 40 municipalities, each wanting unique drawings, equipment design and

[121] Disclosure statement: author was Senior Director of Strategy to the President in the White House 5G strategy during this period.

[122] Jonathan Swan, David McCabe, Ina Fried, Kim Hart, "Scoop: Trump teams considers nationalizing 5G network," *Axios*, January 28, 2018, available at: https://www.axios.com/trump-team-debates-nationalizing-5g-network-f1e92a49-60f2-4e3e-acd4-f3eb03d910ff.html (last visited 29 April, 2019).

[123] David Abecassis, Chris Nickerson, Janette Stewart, "Global Race to 5G – Spectrum and Infrastructure Plans and Priorities," Analysys Mason, April 2018, available at: https://api.ctia.org/wp-content/uploads/2018/04/Analysys-Mason-Global-Race-To-5G_2018.pdf (last visited 29 April, 2019).

[124] Milo Medin, Gilman Louie, "The 5G Ecosystem: Risks & Opportunities for DOD," Defence Innovation Board, April 2019, available at: https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF (last visited 29 April, 2019).

fees for deployment. Additionally, the individual owners of fiber-optic cables were not playing well together as they fought to keep their backhaul monopoly intact[125].

Implications for Security

It was apparent to US policymakers involved in the debate that the building of a secure nationwide 5G network in the United States would require new rules, new regulations and strong government leadership in order to make it a priority. In addition to the regulatory hurdles, security was a challenge. A lack of a manufacturing bases in the United States complicated the need for homebuilt hardware. The lack of a trusted manufacturing base for telecom equipment also made securing the supply-chain problematic. Additionally, manufacturers indicated there was not enough demand to justify re-establishing manufacturing capacity in the West.

Questions around security initially became a major issue with the introduction of the Internet of Things (IoT)[126], but inevitably the focus became the nature of 5G technology itself. In January 2018, after the White House memo on nationwide 5G was leaked to Axios, a political debate erupted inside the Trump Administration. The article branded the report as an attempt by the government to "nationalize" 5G, and raised the fact that the recommendations for a strong Government-led process had caused staunch opposition from the telecommunications industry[127]. Immediately after this story broke in January 2018, the Trump administration took a more cautious approach, with some arguing that the US was not losing in 5G, but winning[128]. The narrative became that the surest way to lose in 5G was to have government involvement.

Yet some in government continued to fight for a nationwide secure network as outlined in the National Security Strategy[129]. The deployment of 5G revolved around convincing the Department of Defense to share spectrum with the private sector to accelerate deployment of a secure nationwide 5G network. This idea launched the concept of a single physical network. According to the outcome of these internal discussions, the best nationwide network lay in devoting as much spectrum as possible to one physical network, and then allowing retail telco operators to become virtual network operators[130]. Not only would this provide the best peak speeds, but overall investment and operating expense would be a fraction of what would be required if all carriers were to build their own networks. However, telco business model prerogatives and tradition ensured that telcos would not cooperate in such a convention. Chinese equipment manufacturers like Huawei and ZTE became more attractive since capital expenditures could be subsidised by the Chinese government. This in itself was an unexpected risk, as it saw US carriers beginning to lobby the Administration on behalf of Huawei.

---

[125] Jonathan Swan, David McCabe, Ina Fried, Kim Hart, "Scoop: Trump teams considers nationalizing 5G network," *Axios*, January 28, 2018, available at: https://www.axios.com/trump-team-debates-nationalizing-5g-network-f1e92a49-60f2-4e3e-acd4-f3eb03d910ff.html (last visited 29 April, 2019).

[126] Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, David Eyers, Twenty Security Considerations for Cloud-Supported Internet of Things, in *IEEE Internet of Things Journal*, Volume 3, Issue 3, (June 2016), pp.269 – 284.

[127] Mike Snider, David Jackson, "Trump administration's idea for government-built 5G network met with loud resistance from US telecoms," *USA Today*, 29 January, 2018, available at: https://eu.usatoday.com/story/tech/news/2018/01/29/trump-administration-considering-government-takeover-5-g-network-report-says/1074159001/ (last visited 29 April, 2019).

[128] "Never mind Huawei: US is already winning the 5G race, Cisco report claims," *South China Morning Post*, 20 February, 2019, available at: https://www.scmp.com/news/world/united-states-canada/article/2186876/never-mind-huawei-us-already-winning-5g-race-cisco (last visited 30 April, 2019).

[129] National Security Strategy of the United States of America, *White House*, December 2017 available at: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (last visited 29 April, 2019).

[130] Jonathan Swan, David McCabe, Ina Fried, Kim Hart, "Scoop: Trump teams considers nationalizing 5G network," *Axios*, January 28, 2018, available at: https://www.axios.com/trump-team-debates-nationalizing-5g-network-f1e92a49-60f2-4e3e-acd4-f3eb03d910ff.html (last visited 29 April, 2019).

Reconfiguring the National Debate on 5G

By July 2018, less than six months after the January 2018 leak, trade tensions with China had increased dramatically. In addition, a number of key reports[131] of Chinese cyber security incidents, along with growing dominance of Chinese telecoms in 5G, raised the alarm once again among administration officials. As a result of the idea that the US is losing in "the race" for 5G, there has been a surge in congressional interest. It is in fact a bipartisan issue that all sides agree needs to be addressed. Nevertheless, the telco industry has continued to press for its own policy preferences, and indeed, the most recent expression of policy was President Trump's speech on 12 April, 2019, in which he outlined a number of key policy prescriptions – such as high band spectrum with fiscal allocations for fiber deployment in rural areas.[132] Previously the Federal Communications Commission (FCC) had announced policy measures to speed up deployment of the high-band networks.[133] These policy announcements were not well received by local communities however, as they minimised what communities could charge the companies.[134]

To date the Department of Defense continues to balk at using its spectrum, as it has been burned many times before.[135] Spectrum in the mid-band has still not been made available beyond what Sprint already has, but the FCC promises it will be forthcoming.[136]

Could Huawei's Inclusion in National 5G Plans Affect the Five-Eyes Intelligence-Sharing Alliance?

Throughout the past few years of debate inside the United States, Chinese equipment manufacturers have continued to make gains; this is despite the fact that US diplomats have travelled extensively, attempting to convince allies and partners not to use Huawei in their networks. Secretary of State Mike Pompeo publicly urged NATO allies in Europe to exclude the Chinese company, saying it might limit its military presence in countries that did not do so[137]. More recently, in the wake of the leaked decision by the UK's National Security Council to only ban Huawei from the "core" of its 5G network, the US has made a number of statements which might affect the US' willingness to share real-time intelligence with the UK. Going forward future military cooperation with allies will be challenged if secure communications cannot be maintained.

[131] See for example, Chris Strohm, "China, Russia, Iran top cyber threats, US intelligence finds," *Bloomberg*, 26 July, 2018, available at: https://www.bloomberg.com/news/articles/2018-07-26/china-russia-iran-top-u-s-cyber-threats-u-s-intelligence (last visited 29 April, 2019); "China hackers steal data from US Navy contractor," *BBC* website, 9 June 2018, available at: https://www.bbc.co.uk/news/world-us-canada-44421785 (last visited 28 April, 2019).

[132] Remarks by President Trump on United States 5G Deployment, The White House, April 12, 2019, available at: https://www.whitehouse.gov/briefings-statements/remarks-president-trump-united-states-5g-deployment/ (last visited 29 April, 2019).

[133] "FCC's 5G FAST Plan," *Federal Communications Commission* website, available at: https://www.fcc.gov/5G (last visited 29 April, 2019).

[134] Rob Pegoraro, "Why 5G Internet is a Policy Minefield for Cities", *City Lab*, October 2, 2018, available at: https://www.citylab.com/life/2018/10/fcc-5g-wireless-broadband-regulations-city-government/571921/ (last visited 30 April, 2019).

[135] Marguerite Reardon, "FCC rakes in $45 billion from wireless spectrum auction," *Cnet website*, January 29, 2015, available at: https://www.cnet.com/news/fcc-rakes-in-45-billion-from-wireless-spectrum-auction/ (last visited 29 April, 2019).

[136] Sacha Segan, "FCC Commissioner demands more mid-Band 5G spectrum," *PC Mag* Website, available at: https://www.pcmag.com/news/368002/fcc-commissioner-demands-more-mid-band-5g-spectrum (last visited 29 April, 2019).

[137] Don Lee, David Cloud, "Allies balk at Trump administration bid to block Chinese firm from cutting-edge telecoms markets," *Los Angeles Times*, Feb 21, 2019, available at: https://www.latimes.com/nation/la-na-huawei-trump-20190221-story.html (last visited 29 April, 2019).

Still unresolved is the security challenge. There has been no effort to bring back microelectronic manufacturing. It is also not clear what, if anything, the Government will require in terms of security for 5G. Because of the wide range of interconnectivity and broad range of applications in a 5G network, there are still dangers about which we do not fully understand. There is, for example, a spectrum of dangers in the malicious compromising of 5G-networked applications in the real world, such as self-driving cars, health equipment, parts of the critical national infrastructure, and other devices integrated into society. At the time of writing, it is unclear whether the Five Eyes intelligence agencies have realised just how much of a challenge it will be, nor what their role should be in mitigating the potential hazards.[138]

[131] C. Todd Lopez, "Pentagon Official: US, partners must lead in 5G technology development", *US Department of Defense*, March 26, 2019, available at: https://dod.defense.gov/News/Article/Article/1796437/pentagon-official-us-partners-must-lead-in-5g-technology-development/ (last visited 30 April, 2019).

Chapter 6
AUSTRALIA, HUAWEI AND TELECOMMUNICATIONS

"It is important to remember that a threat is the combination of capability and intent. Capability can take years, decades to develop. And in many cases won't be attainable at all. But intent can change in a heartbeat".

***Malcolm Turnbull,** former PM, Australia*

Danielle Cave, Tom Uren, Australian Strategic Policy Institute (ASPI)

In 2010 the Australian Government began to roll out the country's largest ever infrastructure project, a high-speed internet network. Involving a combination of thousands of wireless towers and thousands of kilometres of fibre, the project was known as the National Broadband Network (NBN)[139]. Chinese telecommunications company Huawei - hoping to secure up to AUD$1 billion in contracts, was fighting an uphill battle to overcome perceived links to the Chinese state's sweeping cyber espionage efforts[140] and close linkages to the Chinese state[141], including particularly the People's Liberation Army.

In a first for the company, Huawei launched a bold new 'localisation strategy' in 2011— the telecommunications giant appointed three independent directors to an Australian Huawei board with strong political, government and military links[142]: Alexander Downer, a former foreign minister from the Liberal party; John Brumby, a former state premier from the Labor Party; and John Lord, a retired rear admiral. In the same media release the company committed research funding for RMIT university in Melbourne that included a commitment to train 1,000 Australian students via a new 'Next Generation Technology Training Centre[143]. This new localisation strategy, while quite creative and replicated in other countries around the world,[144] didn't work.

By March 2012, and, based on concerns raised by Australia's domestic intelligence agency— the Australian Security Intelligence Organisation[145]—Huawei had been banned from tendering for the NBN. Nicola Roxon, from the office of Australia's Attorney-General at the time put out a statement that saying that the NBN "..will become the backbone of Australia's information infrastructure" and that the Government has "a responsibility to do our utmost to protect its integrity and that of the information carried on it."[146]

[139] Emma Rodgers, "Big gig: NBN to be 10 times faster", *ABC News*, 12 August, 2010, available at: https://www.abc.net.au/news/2010-08-12/big-gig-nbn-to-be-10-times-faster/941408

[140] Council of Foreign Relations, Cyber Operations Tracker (search Victim: Australia and State Sponsor: China) https://www.cfr.org/interactive/cyber-operations (last visited 2 May, 2019)

[141] ASPI International Cyber Policy Centre, Mapping China's Technology Giants, Huawei (see 'Communist Party activities') https://chinatechmap.aspi.org.au/#/company/huawei

[142] Huawei press release, "John Brumby, Alexander Downer, John Lord join Huawei Australia Board of Directors: Creation of Australian Board marks a world-first for Huawei", 6 June 2011 https://web.archive.org/web/20190206112735/https://www.huawei.com/au/press-events/news/au/2011/hw-u_151021 (last visited 2 May, 2019)

[143] Mahesh Sharma, "Huawei, RMIT to build networking training centre: About 1,000 students to benefit", *itnews*, 7 July 2010, available at: https://www.itnews.com.au/news/huawei-rmit-to-build-network-training-centre-219129 (last visited 2 May, 2019)

[144] Huawei press release, "Huawei strengthens its UK Board with appointment of three Non-Executive Directors", 4 March 2015, available at: https://web.archive.org/web/20190428131434/https://www.huawei.com/en/press-events/news/2015/03/hw_415000 (last visited 2 May, 2019)

[145] Peter Hartcher, "Why ASIO won't get online with Huawei", *The Sydney Morning Herald*, 10 April 2012, available at: https://www.smh.com.au/politics/federal/why-asio-wont-get-online-with-huawei-20120409-1wl2y.html (last visited 2 May, 2019).

[146] Harrison Polites, "Government bans Huawei from NBN tenders," *The Australian*, 26 March, 2012: https://www.theaustralian.com.au/business/business-spectator/news-story/government-bans-huawei-from-nbn-tenders/84dcd69855af473f4f0d1f32ecb420cf (last visited 1 May, 2019).

Despite promising rhetoric from the then-opposition Liberal Party, the ban on Huawei remained intact once they were elected to office in 2013. The new Attorney-General George Brandis—now Australia's High Commissioner to the UK—cited advice from national security agencies and declined to alter the policy: "The decision of the previous government not to permit Huawei to tender for the NBN was made on advice from the national security agencies. That decision was supported by the then opposition after we received our own briefings from those agencies."[147]

The Huawei debate faded from the front pages, and although it was locked out of the NBN the company continued a high-profile charm offensive. Within a week of the initial NBN ban, the company announced sponsorship of the Canberra Raiders, the Australian capital's rugby league team[148]. The company also funded politicians' travel to its headquarters in Shenzhen. In fact, the company was the largest corporate sponsor of Australian parliamentarians' overseas travel between 2010 and 2018[149]. It was only in 2018, when the Australian Government began to turn its mind to the next major critical telecommunications infrastructure investment—5G—that security concerns surrounding Huawei's participation in critical national infrastructure found its way into the media again. Across the year a dynamic and in-depth public debate played out that focused on Huawei's participation in Australia's 5G network[150] and a 'whole-of government' effort went into advising then Prime Minister Turnbull and his Cabinet on the potential policy options. While the decision was complicated by protracted and increasingly typical tensions in the Australia-China bilateral relationship, it wasn't an especially difficult policy decision.

In fact, the company was the largest corporate sponsor of Australian parliamentarians' overseas travel between 2010 and 2018

There were a range of considerations:

First, concerns about Chinese state espionage had not diminished, they had in fact increased. Despite a 2017 agreement to not "conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information with the intent of obtaining competitive advantage"[151], Chinese state cyber espionage remained widespread[152]. This was highlighted by a Chinese state-based hack into one of Australia's premier universities — the Australian National University in Canberra — which had not only gained access but had also maintained an ongoing presence in the university's IT systems for "several months"[153].

A particularly concerning example of alleged Chinese espionage overseas was the hack of the African Union (AU) headquarters, as reported by Le Monde and the Financial Times, where Huawei was the key ICT provider[154]. The Le Monde report alleges that from

[150] "Huawei and Australia's 5G Network", *ASPI's International Cyber Policy Centre*, 10 October 2018, available at: https://www.aspi.org.au/report/huawei-and-australias-5g-network (last visited 2 May, 2019)

[151] Jamie Smyth, "Australia and China in pact against cyber theft", *Financial Times*, 24 April, 2017, available at: https://www.ft.com/content/9df81164-28b5-11e7-9ec8-168383da43b7 (last visited 1 May, 2019).

[152] Dr Adam Segal, Dr Samantha Hoffman, Fergus Hanson & Tom Uren, "Hacking for cash: Is China still stealing Western IP?", *APSI*, 25 September 2018, available at: https://www.aspi.org.au/report/hacking-cash (last visited 2 May, 2019)

[153] Stephanie Borys, "Chinese hackers infiltrate systems at Australian National University," *ABC News*, 8 July, 2018, available at: https://www.abc.net.au/news/2018-07-06/chinese-hackers-infilitrate-anu-it-systems/9951210 (last visited 1 May, 2019).

[154] Danielle Cave, "The African Union headquarters hack and Australia's 5G network", *ASPI Strategist*, 13 July 2018 online at https://www.aspistrategist.org.au/the-african-union-headquarters-hack-and-australias-5g-network/ (last visited 2 May, 2019)

January 2012 to January 2017 servers based inside the AU's headquarters in Addis Ababa were transferring data between midnight and 2 am —every single night — to unknown servers hosted more than 8,000 kilometres away in Shanghai[155]. Following the discovery of what media referred to as 'data theft', Le Monde also reported that microphones hidden in desks and walls were detected and removed during a sweep for bugs.

"The stakes could not be higher. This is about more than just protecting the confidentiality of our information—it is also about integrity and availability of the data and systems on which we depend."

Second, a 5G network is not just about telephones, it is critical national infrastructure. Mike Burgess, Director-General of the Australian Signals Directorate (ASD), Australia's signals intelligence and cybersecurity agency, stressed that the "stakes could not be higher. This is about more than just protecting the confidentiality of our information—it is also about integrity and availability of the data and systems on which we depend"[156] and that "the next generation of telecommunications networks will be at the top of every country's list of critical national infrastructure."[157] This is an important point which has not received enough public attention. While understandable, the public commentary has focused on espionage and finding a 'smoking gun'. But this decision is not just about what has already happened – it is about planning for what *could* happen in the future – something telecommunications companies don't have to worry about, but governments must. The potential for espionage, while concerning, is not as concerning as possessing the ability to disrupt or event shut down all connected national, commercial and personal infrastructure. Hence, ensuring integrity and availability of your data and systems – and trusting that the vendors you work with will always safeguard the integrity and availability of your data and systems - must be front and centre for policymakers.

Third, the Chinese Communist Party's grip on notionally private companies had also grown rather than receded. In a rare moment of uncensored candour, the CEO of Sogou, a Chinese search engine company stated: "We're entering an era in which we'll be fused together. It might be that there will be a request to establish a Party committee within your company, or that you should let state investors take a stake … as a form of mixed ownership. If you think clearly about this, you really can resonate together with the state. You can receive massive support. But if it's your nature to go your own way, to think that your interests differ from what the state is advocating, then you'll probably find that things are painful, more painful than in the past."[158]

Huawei's links to and work with the Chinese Communist Party are clearly articulated online for anyone who can read Mandarin.[159] For example, Chinese media reported that by 2007 Huawei had established more than 300 Chinese Communist Party branches within

[155] Joan Tilouine, Ghalia Kadiri, "A Addis-Abeba, le siege de l'Union africaine espionne par Pekin, *Le Monde Afrique*, 26 Janvier, 2018, available at: https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html (last visited 18 April, 2019).

[156] Mike Burgess, Director General of Australian Signals Directorate (ASD) – Offensive Cyber", *Lowy Institute*, 27 March 2018, available at: https://www.lowyinstitute.org/news-and-media/multimedia/video/mike-burgess-director-general-australian-signals-directorate-asd (last visited 1 May, 2019).

[157] Ibid.,

[158] Elsa Kania, "Much ado about Huawei", *The Strategist*, ASPI, 28 March, 2018, available at: https://www.aspistrategist.org.au/much-ado-huawei-part-2/ (last visited 26 March, 2019).

[159] Please see ASPI International Cyber Policy Centre, Mapping China's Technology Giants, Huawei (see 'Communist Party activities') for detailed information https://chinatechmap.aspi.org.au/#/company/huawei

the company. A report from a Huawei publication states that on 1 September 2000 the company's party committee organised a self-criticism and reflection meeting for research and development (R&D) personnel, which was attended by more than 6,000 employees. At the time, Huawei had more than 1,800 party members and 38 branches. Then party secretary, Chen Zhufang, told the audience, "Under the leadership of the party and the government, and through ten years of arduous and outstanding entrepreneurship, Huawei has continually maintained fast growth and momentum, attaining a series of achievements. But the better our position, the more we need to maintain level headedness." CEO Ren Zhengfei also spoke at the meeting.

But beyond these clear and compulsory links to the CCP, another sticking point is the Chinese state's ability to compel organisations and individuals to participate in intelligence collection.[160] This is clearly articulated in Article 7 of China's 2017 National Intelligence Law, which states:

> 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. The state shall protect individuals and organisations that support, cooperate with, and collaborate in national intelligence work.[161]

This law crystallised concerns that the Chinese state had the capability to compel Huawei to assist with state espionage or sabotage efforts.

And therein lies the crux of the matter—an issue which many governments around the world are currently grappling with—the Chinese Government had a demonstrated intent to conduct wide-ranging cyber espionage and IP theft coupled with the capability to use Huawei, or any company for that matter, to assist in compelled intelligence collection. And when we are dealing with critical national infrastructure, these realities can't be ignored or compromised away.[162]

Without mentioning any company by name ASD Director-General Mike Burgess described high-risk vendors as "vendors that have headquarters in countries where those countries have capability, form, intent and coercive laws that compel their companies to co-operate on matters of national intelligence."[163]

"The ASD assesses that the distinction between core and edge collapses in 5G networks. That means that a potential threat anywhere in the network will be a threat to the whole network."

[160] Elsa Kania and Dr Samantha Hoffman, Huawei and the ambiguity of China's intelligence and counter-espionage laws, ASPI Strategist, online at https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/

[161] National Intelligence Law of PRC (2017), on China Law Translate website, available at: https://www.chinalawtranslate.com/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E5%9B%BD%E5%AE%B6%E6%83%85%E6%8A%A5%E6%B3%95/?lang=en (last visited 28 May, 2019).

[162] Danielle Cave, "Huawei highlights China's expansion dilemma: espionage or profit?", ASPI Strategist, 15 June 2018, available at: https://www.aspistrategist.org.au/huawei-highlights-chinas-expansion-dilemma-espionage-or-profit/ (last visited 1 May, 2019).

[163] Jamie Smyth, "Australia banned Huawei over risks to key infrastructure," Financial Times, 27 March, 2019, available at: https://app.ft.com/content/543621ce-504f-11e9-b401-8d9ef1626294?sectionid=home (last visited 1 May, 2019).

[164] Mike Burgess, Director-General Australian Signals Directorate, speech to ASPI National Security Dinner 2018, online at https://asd.gov.au/speeches/20181029-aspi-national-security-dinner.htm (last visited 1 May, 2019).activities') for detailed information https://chinatechmap.aspi.org.au/#/company/huawei

Having identified a heightened risk in particular vendors—based on Chinese state capability and intent—the question becomes how to mitigate this risk. The traditional approach has been to confine high-risk vendors to the edge of the network, but ASD assesses that "the distinction between core and edge collapses in 5G networks. That means that a potential threat anywhere in the network will be a threat to the whole network."[164]

Regardless of disagreements about whether the core and edge of 5G networks will become separated as the technology matures, the UK's experience of attempting to mitigate the risk of Huawei involvement in critical national infrastructure through security evaluation has not been a positive one. Oversight Board reports have become increasingly pessimistic; the last one is damning: "the Oversight Board can only provide *limited assurance* that all risks to UK national security from Huawei's involvement in the UK's critical networks can be sufficiently mitigated long-term."[165] The long-term financial costs involved in these mitigation efforts can also not be ignored.

In summary…

It would be a triumph of lobbying over experience to think that creating an Australian version of a Huawei cyber security evaluation centre would somehow produce a satisfactory outcome despite eight years of UK experience to the contrary. And while such an evaluation centre may have a role to play in technical security risk evaluation—which is of course incredibly important—it is unable to assess or mitigate other political and security risks that accompany cooperation with companies that are subject to extra-judicial direction from foreign states.

The Australian Government has clearly laid out a position on 'high risk vendors' such as Huawei that is based on national interest and national security.[166] This decision didn't just assess company equipment and software, importantly it took into account the fact that Chinese state behaviour demonstrates both intent and capability that indicates a heightened level of threat, particularly to connected critical infrastructure. Informed not just by the technical, but also by political and broader security assessments, it focused on the steps that were necessary to ensure the ongoing safety and security of Australia's 5G networks.

Could Huawei's Inclusion in National 5G Plans Affect the Five-Eyes Intelligence-Sharing Alliance?

Speaking from a narrow intelligence collection and sharing point of view, no, probably not. Intelligence organisations have robust, extensive and expensive protections for their communications, and these communications mechanisms won't be affected by 5G vendors. They also have strong reasons for collaboration; reasons that have endured over the 60-plus years of the UKUSA agreement.

But the Five-Eyes relationship has now extended far beyond intelligence sharing. There are, broader levels of sharing—and political realities—at play. The United States' chief cyber diplomat Ambassador Robert L Strayer[167] has explicitly warned about information-

[165] "Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board: Annual Report 2019," *HCSEC Oversight Board*, March 2019, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf (last visited 20 April, 2019).

[166] Australian Government media release, "Government provides 5G security guidance to Australian carriers", 23 August 2018, found at https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers (last visited 1 May, 2019).

[167] "US will rethink cooperation with allies who use Huawei: official", *Reuters*, 25 March, 2019, available at: https://www.reuters.com/article/us-usa-huawei-tech/u-s-will-rethink-cooperation-with-allies-who-use-huawei-official-idUSKCN1S517H (last visited 1 May, 2019).

sharing, saying, “If other countries insert and allow untrusted vendors to build out and become the vendors for their 5G networks we will have to reassess the ability for us to share information and be connected with them in the ways that we are today.”

Probably the more pressing concern is: how will the broader Five-Eyes alliance be impacted if some partners compromise long-term security for potential short-term commercial and political gain? And how will these divisions affect trust, and shape the various relationships within the alliance, going forward?

Chapter 7
THE IMPLICATIONS OF 5G AND HUAWEI FOR CANADIAN SECURITY

"Both the human and technical reach of Chinese companies now give the intelligence services opportunities to gain direct access to many governments within the developing world as well as many Allied and European countries with inroads into other societies".

Canadian Security and Intelligence Service, *"China and the Age of Strategic Rivalry"*

J. Berkshire Miller, Asia-Pacific Foundation of Canada

The advent of 5G technology, along with its promise and challenges, has led to a major debate in Canada – as it has among many of Ottawa's international partners and allies. Ensuring proper management of the security risks associated with 5G technology will be one of the most critical challenges for the Canadian federal government, in close coordination with private-sector stakeholders and international allies, especially its Five Eyes partners. Canada is currently undergoing a comprehensive security review on 5G and the risks of allowing Huawei to take part in the development of such technology in the country.

Canada's Minister of Public Safety Ralph Goodale has indicated that a decision on the review will be made before the next federal election in Canada this October. Goodale also stressed that Canada would take into consideration its consultation with Five Eyes partners, in addition to the G7. Goodale noted on April 30, "We want to make sure Canadians have access to the best and most beneficial 5G technology, and at the same time we want to make sure they are safe and that their systems are not compromised."[168]

This debate has prompted a range of important questions. How can we expect Canada to assess the risk of 5G, and what are the main principle and actors that engage on matter? On the issue of risk assessment – it is informative to look at the relatively new Canadian Centre for Cyber Security (CCCS) which was established in October 2018, after an extensive round of cyber consultations – led by Public Safety Canada. The CCCS, which is tasked with assessing such risk in the cyber realm and defending specialized cyber technologies, is housed within Canada' Communications Security Establishment (CSE). CSE, as the primary signals intelligence agency in Canada, works closely with the CCCS on assessing the risk and providing intelligence forward for the security review[169].

The Major Actors in the Canadian Debate

While CSE, which reports to the Minister of National Defence, plays a key role in the risk assessment process, there are other important players as well. Public Safety Canada – which houses the Canadian Security Intelligence Service – also participates actively in providing input to the assessment. Other government stakeholders are also involved, including Innovation, Science and Economic Development and the Canadian Security Telecommunications Advisory Committee. Additionally, telecommunications service providers (TSPs) and equipment vendors also are consulted to ensure the integrity of Canada's critical telecommunications infrastructure[170].

[168] Steven Chase, "Goodale Say Decision on Huawei to Come Before the Election," *Globe and Mail*, May 1, 2019 available at: https://www.theglobeandmail.com/politics/article-goodale-says-decision-on-huawei-to-come-before-election/ (last visited 9 May, 2019).

[169] Canadian Centre for Cyber Security, "Backgrounder," Government of Canada, 1 October, 2018, available at:https://cse-cst.gc.ca/en/backgrounder-fiche-information (last visited 9 May, 2019).

[170] Canadian Centre for Cyber Security, "CSE's Security Review Program for 3G/4G/LTE in Canadian Telecommunications Networks." *CCCS*, 2 November, 2018, available at: https://www.cyber.gc.ca/en/news/cses-security-review-program-3g4glte-canadian-telecommunications-networks (last visited 9 May, 2019).

The critical principles to the security review programme remain focussed on protecting the integrity of the networks. While the guiding principles for the current 5G review are confidential, it is instructive to look at the security review program – in place since 2013 – that was focussed on 3G/4G/LTE. This review aims: to exclude designated equipment in sensitive areas of Canadian networks; to enact mandatory assurance testing in independent third-party laboratories for designated equipment before use in less sensitive areas of Canadian networks; to restrict outsourced managed services across government networks and other Canadian critical networks[171].

Through a risk assessment process, the CSE and the CCCS continue to work with relevant TSPs, vendors, service providers, laboratories and also key allies – such as Five Eyes – to ensure that Canadians have secure networks that are both protected and resilient. Others are also contributing to this review, especially as it pertains to the potential for dual-use of 5G network for nefarious means – such as state-sponsored espionage (be it economic or militarily focused). Canadian Security Intelligence Service Director David Vigneault highlighted this in a speech last December noting that "advanced technologies are dual-use in nature in that they could advance a country's economic, security or military interests. In particular, CSIS has seen a trend of state-sponsored espionage in fields that are crucial to Canada's ability to build and sustain a prosperous, knowledge-based economy."[172]

This leads to the most critical matter: the implications to Canada's looming decision on the 5G security review and Huawei. On the strategic political level, the current Liberal Government under Prime Minister Justin Trudeau is under significant pressure at home owing to mounting domestic scandals as well as a rapidly deteriorating bilateral relationship with China (as a result of Beijing's arbitrary detention of two Canadian citizens shortly after arrest – on the request of the US for extradition - of Huawei chief financial officer Meng Wanzhou). But while the issue of Meng is a political challenge for Canada, the 5G review is a separate matter.

If Canada's 5G review decides to ban Huawei architecture in its 5G networks, there will positive reactions – although muted – both internally from the security and intelligence communities in Canada and also from Canada's Five Eyes security partners. The risks of such a decision would be twofold: some TSPs in Canada that have already invested deeply in Huawei equipment for their networks would suffer a significant economic hit; the second risk of course would be a pernicious reaction from Beijing which would no doubt escalate its pressure on Canada (as evidence by its recent restrictions on Canadian exports of canola to China).

Different Positions Among the Five-Eyes Affect Intelligence Sharing or Risk the Alliance Relationship

A decision that allows Huawei architecture in Canadian 5G networks could – depending on the nature of the permission – cause significant and perhaps irreparable damage to our Five Eyes relationship and our longstanding security-intelligence sharing relationship with the United States. The potential fallout of such a decision would be particularly damaging to the latter, with Washington consistently warning on the need for the Five Eyes to have a united approach to Huawei and 5G.

[171] Ibid.

[172] David Vigneault, "Remarks at the Economic Club of Canada," December 4, 2018, available at:https://www.canada.ca/en/security-intelligence-service/news/2018/12/remarks-by-director-david-vigneault-at-the-economic-club-of-canada.html (last visited 9 May, 2019).

Chapter 8
CONCLUSION AND RECOMMENDATIONS

"The personal connections of Huawei's senior executives with China's security apparatuses are highly significant when it comes to understanding the company's emergence as a 'national champion' supported by the party-state, and its pursuit of national strategic goals along with profitability."[173]

Rick Umback, *former ASPI*

This report has sought from the outset to understand Chinese Party / State influence over corporate entities, how China uses those companies to expand its global power and influence, and the technical vulnerabilities posed by 5G software-driven networks. From the outset, it has been clear that different communities disagree on a number of key axes. For example,

- there is little agreement on whether Huawei is a private company or a state-controlled entity;
- there is little agreement on whether it has close relations with intelligence and military agencies of the PRC or not;
- there is little agreement on whether the HCSEC and NCSC can successfully mitigate any risks inherent in Huawei's inclusion in the UK's 5G network;
- there is little agreement over the probable nature of 5G as the network matures, particularly over core / periphery distinctions;
- there is little agreement over whether or not the Five Eyes relationship will be adversely affected by Huawei's inclusion into the UK's 5G network.

Addressing these issues one-by-one, we have been able to add clarity on some, but not others. If we look at these five questions a bit more closely, we can see that they boil down to three major questions:

1. Is Huawei influenced or likely to be influenced by the Chinese state?
2. Can the UK Government mitigate the risks of including an actor controlled by the Chinese state in its 5G network?
3. How will this affect the Five Eyes Alliance?

Is Huawei under the influence of the Chinese state?

Yes. We believe it is subject to influence by the Chinese state. Perhaps it is not directly managed, but in all the ways that are important, it is responsive to strategic direction, financing, and to its ownership by a trade union committee. A number of additional arguments follow: First, it built the PLA's national network in the 1990s and has a privileged position in procurement – something that few private companies in China have. Second, it has borrowed significant sums from Chinese state banks to "go out" and operate in line with China's foreign policy objectives in the Belt and Road Initiative

[173] Rick Umback, "Huawei and Telefunken: Communications Enterprises and Rising Power Strategies,", ASPI, Strategic Insights, 17 April, 2019, available at: https://www.aspi.org.au/report/huawei-and-telefunken-communications-enterprises-and-rising-power-strategies (last visited 6 May, 2019).

and Digital Silk Road. Third, it has a credit line of £77 billion, which allows it to undercut private telecommunications firms in the West and establish market dominance in a sector of great importance to the Chinese leadership. Fourth, the Chinese Government's Civil-Military Fusion Doctrine of pushing its tech firms to collaborate closely with the military; its concentration on systems warfare, AI, and quantum computing; and Huawei's own research focus, mean that its relationship with the Chinese Party State's military will become closer, not more distant, over time. Fifth, China's 2017 National Intelligence Law gives China's intelligence agencies the power to compel Huawei – and any other tech firm – to cooperate with them in China or abroad. Sixth and finally, Huawei's ownership structure – while unique – is not that of a private company. Its trade union committee ownership makes to all intents and purposes state-owned and operated. Trade unions are paid according to government pay scales, from the state treasury, and are under Party discipline. The 2001 amendments to China's Trade Union Law only strengthened party hierarchy.

Can the UK Mitigate the Risks?

It is unclear. While the Oversight Board to HCSEC, responsible for overseeing Huawei's operations in the UK, has been deeply critical of the company's practices, they have not identified any intentional backdoors or attempts to hack into UK data. Problematically, the UK Government has not been unanimous however and there have been mixed signals from the NCSC and the HCSEC Oversight Board on whether the risks presented by Huawei's poor coding and engineering practices can be successfully mitigated. Ultimately the NSC has ruled on the side of the NCSC, which states categorically that it can mitigate the risks by adapting a number of principles in the building and maintaining of Britain's networks. These principles consist of defence-in-depth, diversity of telecoms providers, and the restriction of Huawei's components to the periphery or "dumb" part of the network, such as antennas. While convincingly-stated, these arguments have failed to convince the NCSC's peers in Australia and the United States for the following reasons: First, the restriction of Huawei to antenna overlooks the fact that edge computing is upon us and network components are increasingly software-driven, meaning that antenna can be repurposed through the use of patches and updates by their manufacturers at-will and from a distance. According to our own expert analysis, such patches are impossible to discover until they are activated. Today's antennas might serve a different purpose tomorrow, which presents high-risks in a 5G scenario with self-driving roadways and other complex systems. Second, the distinction between core and periphery is destined to break down as the development of 5G continues and edge computing technology matures. This was reflected in a number of interviews conducted for this project and reflects a major discrepancy between the UK Government and its Five Eyes allies.

How will this affect the Five Eyes Alliance?

It's unclear. While we can categorically say that there is likely to be political damage to the alliance and to the UK's credibility, it is still unclear whether or not there will be "technical damage" to the integrity of the Five Eyes intelligence-sharing network or networks. While little is publicly known about this network, it is likely to be separated completely from the civilian network, and the UK Government has stated that no Huawei components will ever be used in any part of this network, which raises the question of why we should use Huawei components in other parts of the network. While the Government might believe that an unquantifiable but potentially significant amount of political and security damage is worth the exchange for the promise of economic and investment gains, there are two flaws with this argument.

First, it does not really weigh in the wider geopolitical trend that sees the US and China moving toward greater strategic and economic competition. It pretending a blindness – frankly – to the historic trends that see greater geostrategic rivalry between the two, year after year. Because of this is undervalues the weight that Washington puts on this issue, we risk a serious degrading of the Special Relationship for short-term economic gains. No one has suggested that the UK would be kicked out the Five Eyes, but it might find itself losing influence at an ever-increasing rate with a country that – while imperfect – remains a democracy with similar values and norms to the UK.

Second, it identifies technical risk in the narrowest of ways – looking for backdoors and cyber-attacks – and completely misses the emergence of two worrying trends: First, the development of social media, big data, and artificial intelligence being used to harvest immense amounts of data on societies. Second, the interest and growing expertise of authoritarian powers in the application of these technologies in controlling and influencing populations. The narrow band of risk assessment and mitigation that only considers about data breaches or system failure but ignores the slow build-up of data about the UK's military leaders, its political leaders, and its media influencers and owners, betrays an unsophisticated understanding of technological risk. It is to all intentions and purposes – risk so narrowly defined as to be useless.

RECOMMENDATIONS

We recommend the following:

In the short-term

1. The Government should block high-risk vendors such as Huawei from participation in the 5G network, unless they can prove a very high degree of insulation from the parent company.
2. Work with other Western allies to provide alternatives to Chinese tech firms in the 5G space.
3. To create a new risk assessment system, such as that laid out in the Prague Proposals, specifically, which:
    a. **Take into account the overall risk of influence** on a supplier by a third country, notably in relation to its model of governance, the absence of cooperation agreements on security, or similar arrangements, such as adequacy decisions, as regards data protection, or whether this country is a party to multilateral, international or bilateral agreements on cybersecurity, the fight against cybercrime, or data protection. In the case of Chinese tech firms, their data protection arrangements inside the PRC, should be seen as a sign of risk.
    b. **Take into account the legal environment** and other aspects of a supplier's ecosystem. In the case of Chinese tech firms, their submission to the Party State, to its financing, and its 2017 National Intelligence Law, should be seen as signs of risk.
    c. **Take into account the transparency**, ownership, partnerships, and corporate governance of service providers. There is no point arguing for diversity of providers, while purchasing services from state-owned enterprises who are not playing on a level playing field and who are driven by both economic and geostrategic factors.

4. To introduce a clear definition of "high-risk vendors" for the UK ICT market, that is shared by our closest allies and intelligence-sharing partners.

5. To quickly expedite into legislation, the 2018 BEIS White Paper on National Security and Investment, which is urgently needed to guide trade-oriented civil servants and the security services on issues that broach both security and trade.

6. To create a whole-of-government policy approach toward China and Chinese state entities that operate in the UK.

In the long-term

7. To create a Five Eyes risk assessment system that not only considers technical risks, but also considers societal and interference risks.

8. To create a Five Eyes risk assessment system that defines providers by their ownership, legal environment, and transparency as low-risk, medium-risk, or high-risk.

9. To support open-architecture approaches toward 5G network-building, such as the O-RAN Alliance.

10. To support global norms that foster provider interoperability rather than aide providers who adapt a "lock-in" approach toward network-building.

The UK's allies – Australia and the United States – do not agree that the UK's approach toward 4G is applicable toward 5G. Specifically, in opposition to the UK position, they believe:

11. The differences between core and periphery will not remain as sharply delineated in 5G as they are in 4G.

12. That significant equipment – such as antenna – can simply be re-purposed once it has already been tested and installed.

13. That one cannot use 5G manufactured goods without strong trust that there are safeguards in the company in question.

While we do not believe that these recommendations are beyond the art-of-the-possible. Indeed, while some are clearly long-term projects – such as creating a Five Eyes standard of risk – there is inherent value in the process as much as there is in the conclusion. Protecting our shared values and national interests will only strengthen the alliance at a time of ever-increasing authoritarian challenge to the rules-based system.

Appendix 1
TECHNICAL DESCRIPTION OF ANTENNA VULNERABILITIES:

- A 5G millimetre wave [mmw] network promises to ease the burden on the current infrastructure by offering significantly higher data rates through increased channel bandwidth.
- The 5G Digital cellular network is divided into a mosaic of small geographical areas called cells which communicate using microwaves via a local antenna array and a low power transceiver mounted at the antenna.
- Because 5G uses mmw the maximum range between the antenna and receiver is short and the cells are limited in size, and therefore multiple antennas are required to cover any one cell.
- Each cell requires multiple antennas so that when a user crosses from one cell to another the mobile device automatically hands over seamlessly from one antenna to another in the new cell.
- The local antennas are connected to the network per se using a high bandwidth optical fibre.
- However the mobile environment at these mmw bands is far more complex than at 4G as the propagation losses vary greatly depending on the environment and therefore the antenna design must be 'smarter'. That is in the form of an array.
- The description 'array' is significant because the antenna is not a simple whip or dipole but it is deployed in the shape of crosses, rectangles, circles or hexagons.
- All signals radiating from the antenna share the same basic characteristics. Multipath, fading and delay spread will reduce the capacity of a cellular network, and congestion of the channels and co-channel interference will reduce the capacity further.
- An active phased array antenna will help to mitigate these interference problems by adapting the beam shape, polarisation etc.
- Hence, beam forming antenna arrays are essential in the 5G network as the large number of antenna elements can create a series of complex beam shapes in order to improve the nontrivial signal to noise ratio [SNR].
- Multiple bitstreams of data are transmitted at any one time requiring smart beam forming at the antennas and therefore the antenna computer will constantly determine which channel is preferred for each device.
- Within the smart antenna is a number of control circuits some possibly manufactured from application specific integrated circuits or ASICs. It is impossible both to 'open up' an ASIC to examine all its functions or indeed to reverse engineer them.
- Hence the client will be unsure exactly what is in the driver circuits which will be controlled by software loaded either during manufacture, or potentially loaded externally.

- Clearly this is not a dumb antenna but a device which is key to the operation of not only the specific cell and network but also each platform within it.
- Interfere with the antenna design, or build, and steer the beam away from one or all the devices and the communication will be shut down.
- The smarter the antenna the more vulnerable it may become.

Appendix 2
PRAGUE PROPOSALS[174]:

The Chairman Statement on cyber security of communication networks in a globally digitalized world Prague 5G Security Conference Prague, 3 May 2019

PREAMBLE: COMMUNICATION NETWORKS IN GLOBALLY DIGITALIZED WORLD

Communication is the cornerstone of our societies. It defines almost every aspect of our lives. Yet the rapid development and scale on which we use communication technologies increases our dependency and vulnerabilities.

5G networks and future communication technologies will transform the way we communicate and the way we live substantially. Transportation, energy, agriculture, manufacturing, health, defense and other sectors will be significantly enhanced and altered through these next generation networks. High-speed low-latency technology is expected to allow for a true digital evolution, stimulating growth, innovation and well-being. Automatization of everyday activities and the use of the internet of things in its full potential will be made possible.

These developments, however, invoke major risks to important public interests and have national security implications. Today, malicious actors operate in cyber space, with the intention to undermine cohesion of our societies and paralyze the proper functioning of states or businesses. This includes attempts to control or disrupt our communication channels and the information transmitted. In digitalized societies, this can have serious consequences.

Security of communication channels has therefore become vital. Disruption of the integrity, confidentiality or availability of transmitted information or even the disruption of the service itself can seriously hamper everyday life, societal functions, economy and national security. Communication infrastructures are the cornerstone of our societies, with 5G networks to become the building blocks of a new digital environment.

ON THE IMPORTANCE OF SECURITY OF 5G NETWORKS

Considering that security of 5G networks is crucial for national security, economic security and other national interests and global stability, the chair believes that the architecture and functions of 5G networks must be underpinned by an appropriate level of security.

EU Member States underline their own ongoing process aimed at defining a common EU approach on the issue of cybersecurity of 5G networks as initiated by the European Commission with the publication of its Recommendation published on 26 March 2019.

With the intention to support ongoing discussions how to decrease the security risks associated with developing, deploying, operating, and maintaining complex communication infrastructures such as 5G networks, the chair recognizes existence of the following perspectives:

[174] The Prague Proposals: The Chairman Statement on cyber security of communication networks in a globally digitalized world, Prague 5G Security Conference,

Cyber security not only a technical issue

Cyber security cannot be regarded as a purely technical issue. A safe, secure and resilient infrastructure requires adequate national strategies, sound policies, a comprehensive legal framework and dedicated personnel, who is trained and educated appropriately. Strong cyber security supports the protection of civil liberties and privacy.

Both technical and non-technical nature of cyber threats

When dealing with cyber security threats, not only their technical nature, but also specific political, economic or other behaviour of malicious actors which seek to exploit our dependency on communication technologies should be taken into account.

Possible serious effects of 5G networks disruption

Due to the wide application of 5G based networks, unauthorized access to communications systems could expose unprecedented amounts of information or even disrupt entire societal processes.

Nation-wide approach

Policies and actions taken to ensure a high level of cyber security should not be aimed and carried out only by primary stakeholders (i.e. operators and technology suppliers), but should also be reflected by all relevant stakeholders in other areas and sectors which significantly influence the general level of security, e.g. education, diplomacy, research and development, etc. Safeguarding cyber security of communication infrastructure is not solely an economic or commercial issue.

Proper risk assessment essential

Systematic and diligent risk assessment, covering both technical and non-technical aspects of cyber security, is essential to create and maintain a truly resilient infrastructure. A risk based security frameworks should be developed and deployed, taking into account state of art policies and means to mitigate the security risks.

Broad nature of security measures

Cyber security measures need to be sufficiently broad to include whole range of security risk, i.e. people, processes, physical infrastructure, and tools both on the operational and strategic level.

No universal solutions

The decision on the most optimal path forward when setting the proper measures to increase security should reflect unique social and legal frameworks, economy, privacy, technological self-sufficiency and other relevant factors important for each nation.

Ensuring security while supporting innovation

Innovation is the main driver of development and economic growth in modern societies. It also fosters new security solutions. Policies, laws, and norms, should allow security measures to be flexible to manage the interface between security and specific national conditions. Through this flexibility, creativity and innovation should be encouraged.

Security costs money

Achieving a proper level of security sometimes does require higher costs. Increased costs should be tolerated if security necessitates it. At the same time, security does not necessarily imply higher costs.

Supply chain security

Shared responsibility of all stakeholders should drive supply chain security. Operators of communication infrastructure often depend on technology from other suppliers. Major security risks emanate from the cross-border complexities of an increasingly global supply chain which provides ICT equipment. These risks should be considered as part of the risk assessment based on relevant information and should seek to prevent proliferation of compromised devices and the use of malicious code and functions.

Bearing in mind these perspectives, the chair calls upon a responsible development, deployment, and maintenance of 5G networks and future communication technologies, considering the following proposals and best practices.

PRAGUE PROPOSALS

The Chairman suggests following proposals in four distinct categories in preparation for the roll out of 5G and future networks.

A. Policy

a. Communication networks and services should be designed with resilience and security in mind. They should be built and maintained using international, open, consensusbased standards and risk-informed cybersecurity best practices. Clear globally interoperable cyber security guidance that would support cyber security products and services in increasing resilience of all stakeholders should be promoted.

b. Every country is free, in accordance with international law, to set its own national security and law enforcement requirements, which should respect privacy and adhere to laws protecting information from improper collection and misuse.

c. Laws and policies governing networks and connectivity services should be guided by the principles of transparency and equitability, taking into account the global economy and interoperable rules, with sufficient oversight and respect for the rule of law.

d. The overall risk of influence on a supplier by a third country should be taken into account, notably in relation to its model of governance, the absence of cooperation agreements on security, or similar arrangements, such as adequacy decisions, as regards data protection, or whether this country is a party to multilateral, international or bilateral agreements on cybersecurity, the fight against cybercrime, or data protection.

B. Technology

a. Stakeholders should regularly conduct vulnerability assessments and risk mitigation within all components and network systems, prior to product release and during system operation, and promote a culture of find/fix/patch to mitigate identified vulnerabilities and rapidly deploy fixes or patches.

b. Risk assessments of supplier's products should take into account all relevant factors, including applicable legal environment and other aspects of supplier's ecosystem, as these factors may be relevant to stakeholders' efforts to maintain the highest possible level of cyber security.

c. When building up resilience and security, it should be taken into consideration that malicious cyber activities do not always require the exploitation of a technical vulnerability, e.g. in the event of insider attack.

d. In order to increase the benefits of global communication, States should adopt policies to enable efficient and secure network data flows.

e. Stakeholders should take into consideration technological changes accompanying 5G networks roll out, e.g. use of edge computing and software defined network/network function virtualization, and its impact on overall security of communication channels

f. Customer – whether the government, operator, or manufacturer -- must be able to be informed about the origin and pedigree of components and software that affect the security level of the product or service, according to state of art and relevant commercial and technical practices, including transparency of maintenance, updates, and remediation of the products and services.

C. Economy

a. A diverse and vibrant communications equipment market and supply chain are essential for security and economic resilience.

b. Robust investment in research and development benefits the global economy and technological advancement and is a way to potentially increase diversity of technological solutions with positive effects on security of communication networks

c. Communication networks and network services should be financed openly and transparently using standard best practices in procurement, investment, and contracting.

d. State-sponsored incentives, subsidies, or financing of 5G communication networks and service providers should respect principles of fairness, be commercially reasonable, conducted openly and transparently, based on open market competitive principles, while taking into account trade obligations.

e. Effective oversight on key financial and investment instruments influencing telecommunication network development is critical.

f. Communication networks and network service providers should have transparent ownership, partnerships, and corporate governance structures.

D. Security, Privacy, and Resilience

a. All stakeholders including industry should work together to promote security and resilience of national critical infrastructure networks, systems, and connected devices.

b. Sharing experience and best practices, including assistance, as appropriate, with mitigation, investigation, response, and recovery from network attacks, compromises, or disruptions should be promoted.

c. Security and risk assessments of vendors and network technologies should take into account rule of law, security environment, vendor malfeasance, and compliance with open, interoperable, secure standards, and industry best practices to promote a vibrant and robust cyber security supply of products and services to deal with the rising challenges.

d. Risk management framework in a manner that respects data protection principles to ensure privacy of citizens using network equipment and services should be implemented.

Appendix 3
ARTICLES ABOUT HUAWEI CONCERNED ABOUT CYBER SECURITY ISSUES

10 April 2019

"US firm wins Oz-backed bid to block Huawei from subsea Pacific cables" The Register https://www.theregister.co.uk/2019/04/10/subcom_solomon_cable/

- "An American company is to build a series of undersea cables linking Australia to China after the Aussie government put its foot down and kicked Huawei off the contract."
- "The often-cited justification by western countries for banning Huawei is that the Chinese company's employees can be legally compelled to help Chinese state spies carry out their nefarious doings. This conveniently ignores the fact that all of the western "Five Eyes" nations have identical laws, such as Britain's Snoopers' Charter."

28 March 2019

"Long-term security risks from Huawei" BBC https://www.bbc.co.uk/news/technology-47732139

- "The Chinese company Huawei has been strongly criticised in a report by the body overseeing the security of its products in UK telecoms. The report, issued by the National Cyber Security Centre, which is part of GCHQ, says it can provide 'only limited assurance that the long-term security risks can be managed in the Huawei equipment currently deployed in the UK'."

28 March 2019

"Huawei's equipment poses 'significant' security risks, UK says" CNBC News https://www.cnbc.com/2019/03/28/huawei-equipment-poses-significant-security-risks-uk-says.html

- "The new U.K. government said it 'does not believe that the defects identified are a result of Chinese state interference.' Instead, it blamed 'poor software engineering' and a lack of 'cybersecurity hygiene.' In other words, Huawei's networks could be exploited by a 'range of actors,' not just the Chinese government."

7 March 2019

"Huawei: US Congress acted as 'judge, juror and executioner' with ban on our products", CNN https://edition.cnn.com/2019/03/06/tech/huawei-suing-united-states/index.html

- Huawei, the world's biggest maker of telecommunications equipment, said Thursday that it has filed a lawsuit in Texas challenging a recent US law that bans federal agencies from buying its products. "This ban not only is unlawful, but also restricts Huawei from engaging in fair competition, ultimately harming US consumers," Huawei Deputy Chairman Guo Ping said"
- "The US Congress has repeatedly failed to produce any evidence to support its restrictions on Huawei products"

25 February 2019

"GCHQ chief warns on Huawei security threat", Financial Times
https://www.ft.com/content/90c07bbe-38ce-11e9-b856-5404d3811663

- "The head of GCHQ, the UK's signals intelligence agency, has become the latest British spy chief to voice concerns over the threat posed by Chinese technology."

20 February 2019

"Britain managing Huawei risks, has no evidence of spying: official" Reuters
https://uk.reuters.com/article/us-huawei-europe-britain/britain-managing-huawei-risks-has-no-evidence-of-spying-official-idUKKCN1Q91PM

- "Vodafone, the world's second-largest mobile operator, said last month it was "pausing" deployment of Huawei equipment in core networks until Western governments give full security clearance."

20 February 2019

"Britain is vulnerable to 'ruthless' Chinese interference campaign and must block Huawei, report claims" Roland Oliphant, Telegraph
https://www.telegraph.co.uk/news/2019/02/20/britain-vulnerable-ruthless-chinese-interference-campaign-must/

- "The Royal United Services Institute (Rusi) said it would be "naive" and "irresponsible" to allow Chinese tech giant Huawei to access the UK's telecommunications system and called on the government to pass legislation as a matter of urgency introducing tougher restrictions on investments in critical infrastructure."
- "Charles Parton, the Mandarin-speaking former British diplomat who wrote the report"...said..."Britain is an important member of Five Eyes and that underpins our global status and importance. If the US, Australia and New Zealand won't let Huawei in, they may conclude that our own systems are not secure and we risk losing that."

6 February 2019

"Huawei says it needs up to 5 years to satisfy UK demands", Financial Times,
https://www.ft.com/content/d112d2b4-2a0c-11e9-88a4-c32129756dd8

- "He said Huawei has sold equipment to 1,500 telecoms companies in more than 170 countries over the past 30 years, but that no "serious" security incidents have happened."

28 January 2019

"Chinese Telecom Conglomerate Charged with Multiple Crimes" FBI News
https://www.fbi.gov/news/stories/chinese-telecom-firm-huawei-indicted-012819

- "conspiracy to defraud the United States, Bank Fraud, and Theft of Trade Secrets Among Nearly Two Dozen Charges Against Huawei"
- "both sets of charges expose Huawei's brazen and persistent actions to exploit American companies and financial institutions and to threaten the free and fair global marketplace"

29 January 2019

"Justice Dept. charges Huawei with fraud, ratcheting up U.S.-China tensions" The Washington Post
https://www.washingtonpost.com/world/national-security/justice-dept-charges-huawei-with-fraud-ratcheting-up-us-china-tensions/2019/01/28/70a7f550-2320-11e9-81fd-b7b05d5bed90_story.html?utm_term=.2c2aca730692

- "A 13-count indictment filed in New York City against Huawei, two affiliates and its chief financial officer, Meng Wanzhou, details allegations of bank and wire fraud. The company also is charged with violating U.S. sanctions on Iran and conspiring to obstruct justice related to the investigation."
- "The criminal activity in this indictment goes back at least 10 years and goes all the way to the top of the company"
- "In a statement in Beijing, a Foreign Ministry spokesman decried the charges. "For some time, the U.S. has used its government power to discredit and crack down on specific Chinese companies in an attempt to stifle their legitimate operations," Geng Shuang said. "We strongly urge the U.S. to stop the unreasonable suppression of Chinese companies, including Huawei, and treat Chinese companies objectively and fairly."

8 January 2019

"Exclusive: New documents link Huawei to suspected front companies in Iran, Syria" Reuters
https://uk.reuters.com/article/uk-huawei-iran-exclusive/exclusive-new-documents-link-huawei-to-suspected-front-companies-in-iran-syria-idUKKCN1P21ME

- "U.S. authorities allege CFO Meng Wanzhou deceived international banks into clearing transactions with Iran by claiming the two companies were independent of Huawei, when in fact Huawei controlled them. Huawei has maintained the two are independent: equipment seller Skycom Tech Co Ltd and shell company Canicula Holdings Ltd."

26 December 2018

UK Defense Secretary "Gavin Williamson has 'grave' concerns over Chinese telecom giant Huawei providing UK 5G network" Telegraph
https://www.telegraph.co.uk/politics/2018/12/26/gavin-williamson-has-grave-concerns-overchinese-telecom-giant/

- Williamson's "comments follow a warning this month from Alex Younger, the MI6 chief, who said Britain needed to decide how comfortable it was using Chinese-owned technologies within its communications infrastructure"
- "BT has said it will not use Huawei's equipment within the heart of its 5G mobile network when it is rolled out in the UK...[and] that it was stripping out Huawei's equipment from the core of its existing 3G and 4G networks"
- "A US-commissioned report recently warned that Beijing could force Huawei and other Chinese 5G equipment makers to 'modify products to perform below expectations or fail, facilitate state or corporate espionage, or otherwise compromise the confidentiality, integrity, or availability' of networks"

- "Earlier this month, New Zealand became the latest country to bar a local network from using Huawei's 5G gear"
- "Ren Zhengfei, [Huawei's] founder, was a former engineer in the country's army and joined the Communist Party in 1978. There are questions about how independent any large Chinese company can be."

14 December 2018

"How a National Security Investigation of Huawei Set Off an International Incident" New York Times
https://www.nytimes.com/2018/12/14/business/huawei-meng-hsbc-canada.html

- "From 2009 to 2014, HSBC helped the Chinese telecommunications giant Huawei move money in Iran, in breach of United States sanctions. This time, the bank said, it had a good excuse: Huawei, and one of its top executives, tricked HSBC into handling the business."

6 December 2018

"Huawei Q&A: what you need to know about the Chinese phone maker" The Guardian
https://www.theguardian.com/technology/2018/dec/06/huawei-qa-what-you-need-to-know-about-the-chinese-phone-maker

- Huawei "In the second quarter of 2017 the Chinese company sold 54.2m phones, making up 15% of the share of the market."

5 December 2018

"BT bars Huawei's 5G kit from core of network" BBC
https://www.bbc.co.uk/news/technology-46453425

- "The British firm, however, still plans to use the Chinese company's phone mast antennas and other products deemed not to be at the "core" of the service."

28 November 2018

"Huawei: NZ bars Chinese firm on national security fears" BBC News
https://www.bbc.co.uk/news/business-46368001

- "New Zealand has become the latest country to block a proposal to use telecoms equipment made by China's Huawei because of national security concerns"
- "Telecoms firm Spark New Zealand planned to use equipment from the Chinese firm in its 5G network."
- "The head of NZ's Government Communications Security Bureau (GCSB) told Spark the proposal "would, if implemented, raise significant national security risks", the company said."

26 October 2018

"How the world is grappling with China's rising power" BBC News
https://www.bbc.co.uk/news/business-45948692

- "Australia's parliament this year passed new laws to prevent foreign interference in the country, which was widely seen as targeting China."
- "The Australian government banned Huawei and ZTE from providing 5G technology for the country's wireless networks"
- "Steve Tsang, director of SOAS China Institute in London" said "I think there is genuine reason to be concerned because of the lack of transparency about Huawei's relationship with the Chinese government and the Communist Party"
- "Germany's government earlier this year also vetoed the takeover of an engineering company by a Chinese firm on the ground of national security"

23 August 2018

"Huawei and ZTE handed 5G network ban in Australia" BBC News
https://www.bbc.co.uk/news/technology-45281495

- "On Thursday, the Australian government said national security regulations that were typically applied to telecoms firms would be extended to equipment suppliers"
- "Huawei is the world's biggest producer of telecoms equipment. It also ranks second in global smartphone sales, behind Samsung and ahead of Apple."
- "Under Chinese law, companies must co-operate with the intelligence services. Analysts therefore warn that equipment produced by firms such as Huawei and ZTE could be compromised."
- "The United States has previously banned Huawei from bidding for government contracts because of fears over espionage"
- "How has China responded?" "It called on Australia to 'abandon ideological prejudices and provide a fair and competitive environment for Chinese companies'."

1 August 2018

"Chinese takeover of German firm Leifeld collapses" BBC News
https://www.bbc.co.uk/news/world-europe-45030537

- "The German government has vetoed the takeover of an engineering company by a Chinese firm on the grounds of national security."
- "Leifeld speicalises in manufacturing for Germany's aerospace and nuclear industries"

1 August 2018

"Huawei beats Apple to become second-largest smartphone maker" The Guardian
https://www.theguardian.com/technology/2018/aug/01/huawei-beats-apple-smartphone-manufacturer-samsung-iphone

- "Huawei has denied it facilitates spying and has said it is a private company and not under Chinese government control and not subject to Chinese security laws overseas."

19 July 2018

"UK criticizes security of Huawei products" BBC News
https://www.bbc.co.uk/news/technology-44891913

- "A UK government report in Huawei's broadband and mobile infrastructure equipment has concluded that it has 'only limited assurance' that the kit poses no threat to national security"
- "In response, Huawei acknowledged there were 'some areas for improvement'."
- "Huawei is the world's biggest producer of telecoms equipment and is a major supplier of broadband and mobile network gear in Britain"

29 January 2018

"AU spying report absurd: China" ENCA
https://www.enca.com/africa/au-spying-report-absurd-china

- "China ambassador to the African Union on Monday denounced as 'absurd'"
- "China is deeply investing in Africa, regularly offering low-interest loans and gifts to individual nations and doing $149.2 billion (R1,7 trillion) in trade with the continent in 2016"

7 August 2016

"The Chinese firm taking threats to UK national security very seriously" The Guardian
https://www.theguardian.com/technology/2016/aug/07/china-huwaei-cell-uk-national-security-cyber-surveillance-hacking

- Huawei "The company makes everything from the routers and switches that steer traffic across the internet, to BT's green street cabinets, to the transmission equipment used in mobile phone masts."

9 September 2015

"Spy Software Found Preinstalled on Lenovo, Huawei, and Xiaomi Smartphones" The Epoch Times
https://www.theepochtimes.com/spy-software-found-pre-installed-on-lenovo-huawei-and-xiaomi-smartphones_1748900.html

- "the findings points to poor security standards for Chinese smartphones"
- "it cannot be removed…if anyone finds the malware on their phone, their only option is to buy a new one"
- Shows intention "the group or individual behind the spy software would need to unlock each phone, install the malware, then lock each phone up again"
- "state spying can't be ruled out either…the Chinese regime as a track record of using similar smartphone malware to spy on people"

2 March 2015

"Huawei's watch is stylish as well as smart" CNN
https://money.cnn.com/2015/03/02/technology/huawei-smartwatch/index.html

- "Huawei is a telecoms company based in China. It's a major player in computer networking, government and mobile communications. Recently, the firm has made a big push into consumer electronics."

19 July 2013

"Ex-CIA chief accuses Huawei of industrial espionage" The Telegraph
https://www.telegraph.co.uk/technology/news/10191154/Ex-CIA-chief-accuses-Huawei-of-industrial-espionage.html

- "God did not make enough briefing slides on Huawei to convince me that having them involved in our critical communications infrastructure was going to be okay" Former head of the CIA & NSA in the US, General Michael Hayden
- "claims that he has seen hard evidence that communications company Huawei has engaged in espionage on behalf of the Chinese government"

10 May 2013

"India joins list of nations vetting Huawei, ZTE" The Register
https://www.theregister.co.uk/2013/05/10/india_to_test_huawei_and_zte_kit/

- "Australia forbade Huawei from supplying the nation's nascent national broadband network, on security grounds. Australia's decision was made just a few weeks after a visit by Barack Obama, who's retinue is believed to have offered Australian authorities a briefing on the risks posed by Huawei."
- "the Hindustan Times now says India has expressed similar concerns. The Delhi-based paper reports India's Department of Telecommunications has responded to a request from the nation's Cabinet and will establish a lab to test for the presence of "Spyware, Malware and bugging software" in telecoms kit."

9 May 2013

"Reclusive Huawei CEO breaks media silence" CNN
https://money.cnn.com/2013/05/09/news/huawei-founder/index.html

- "Huawei made its name selling telecom equipment, and specializes in building the routers and switches needed for national communication systems. Now the industry's second-largest firm, Huawei recently won a contract to build a mobile network in New Zealand. But the Chinese company has been shut out of other markets, including Australia and the United States."

25 October 2012

"Exclusive: Huawei partner offered U.S. tech to Iran" Reuters
https://www.reuters.com/article/us-huawei-iran/exclusive-huawei-partner-offered-u-s-tech-to-iran-idUSBRE89O0E520121025

- "An Iranian partner of Huawei Technologies Co Ltd, a Chinese company that has denied breaking U.S. sanctions, last year tried to sell embargoed American antenna equipment to an Iranian firm, according to documents and interviews."
- "South Africa's MTN Group, which owns 49 percent of MTN Irancell, said the Iranian telecoms firm had requested 36 German-made antennas not subject to sanctions but that "Huawei, through its local partner Soda Gostar, mistakenly provided details of U.S.-manufactured" antennas."
- "Reuters has documented how China has become a backdoor way for Iran to obtain embargoed U.S. computer equipment."

23 October 2012

"China Cyber Threat: Huawei and American Policy Toward Chinese Companies"
Heritage Foundation
https://www.heritage.org/defense/report/china-cyber-threat-huawei-and-american-policy-toward-chinese-companies

- "On October 8, the House Permanent Select Committee on Intelligence released a report, U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE. The report concluded that using telecommunications hardware and infrastructure from these two firms entails a risk to American economic and national security."
- "The report cites several studies that point to the People's Republic of China (PRC) as the greatest source of cyber attacks and intrusions. These incidents are often widespread and coordinated, suggesting state involvement or even leadership."
- "A Disturbing Trend
    - 2001: Two people funded by state-owned Datang Telecom indicted for stealing secrets from Lucent.[1]
    - 2002: Two people funded by Hangzhou city government indicted for stealing secrets from four firms.[2]
    - 2003: PetroChina employee arrested for attempting to steal seismic imaging software from Silicon Valley firm (later pled guilty).[3]
    - 2004: Canada's Nortel discovers that China-based hackers have compromised its entire network.[4]
    - 2005: Chinese national working at U.S. unit of Dutch firm AkzoNobel begins stealing material needed to replicate advanced industrial coating.[5]
    - 2006: Two people indicted for stealing proprietary information from auto parts maker Metaldyne and seeking to pass it to Chinese firms.[6]
    - 2007: Chinese national employed by Dow begins transferring trade secrets to Chinese government-controlled institutes.[7]

- 2008: Former DuPont employee picked by state-owned Pangang to make titanium dioxide, supposedly using DuPont production method (later pled guilty to espionage).[8]
- 2009: Ford Motor employee arrested for stealing trade secrets—later found guilty—supposedly on behalf of Beijing Auto.[9]
- 2010: Dozens of multinationals disclosed as targeted in China-based hacking of Google.[10]
- 2011: American Superconductor sues top Chinese turbine maker Sinovel for stealing software used to drive wind turbines.[11]
- 2012: NSA director acknowledges that China-based hackers compromised a company that provides computer security services to defense firms such as Lockheed Martin.[12]"

30 July 2012

"Expert: Huawei routers are riddled with vulnerabilities" CNET
https://www.cnet.com/news/expert-huawei-routers-are-riddled-with-vulnerabilities/

- "German security researcher says the Chinese government doesn't need to demand back doors on Huawei routers because there are already major holes in their firmware."
- "Huawei routers are mostly used in Asia, Africa and the Middle East. Because they're cheap, though, they're increasingly turning up in other parts of the world"

30 July 2012

"Hackers reveal critical vulnerabilities in Huawei routers at Defcon" Computerworld
https://www.computerworld.com/article/2505191/hackers-reveal-critical-vulnerabilities-in-huawei-routers-at-defcon.html

- "The researcher, who also analyzed the security of Cisco networking equipment in the past, described the security of the Huawei devices he analyzed as "the worst ever" and said that they're bound to contain more vulnerabilities."

9 December 2011

"Huawei pledges not to pursue Iran business" Financial Times
https://www.ft.com/content/d244cf16-2276-11e1-923d-00144feabdc0

- "Huawei Technologies has pledged not to pursue new business in Iran as the world's second-largest telecom infrastructure vendor seeks to contain damage to its reputation in Western markets."
- "The Huawei announcement comes as political pressure is mounting in the US on companies that do business with Iran. Last week the Senate passed a measure by 100-0 which would place sanctions on banks which deal with the Iranian central bank. The Wall Street Journal reported in October that Huawei had signed a deal earlier this year to supply Mobile Communication Co of Iran (MCCI) with products that could help track users' locations. Huawei has denied this."

- "Because Huawei's founder, Ren Zhengfei, once worked for the People's Liberation Army as an officer, Huawei has been unable to shake off suspicions that it might be an arm of the Chinese military and government."
- "In September, the US government barred the company from taking part in the development of a wireless network to be used by police and other emergency services."

27 October 2011

"Chinese Tech Giant Aids Iran" Wall Street Journal
https://www.wsj.com/articles/SB10001424052970204644504576651503577823210

- "Huawei Technologies Co. now dominates Iran's government-controlled mobile-phone industry. In doing so, it plays a role in enabling Iran's state security network."

11 October 2011

"Chinese telecom firm tied to spy ministry" The Washington Times
https://www.washingtontimes.com/news/2011/oct/11/chinese-telecom-firm-tied-to-spy-ministry/

- "A U.S. intelligence report for the first time links China's largest telecommunications company to Beijing's KGB-like intelligence service and says the company recently received nearly a quarter-billion dollars from the Chinese government."
- "Huawei's links to the Chinese military have been disclosed previously. The Open Source Center (OSC) report provides the first details of its links to Chinese intelligence, which U.S. officials have said has been engaged in a massive effort to acquire secrets and economic intelligence from government and private-sector computer networks around the world."

18 January 2011

"Huawei Opens New Headquarters in Canada; Deepens Commitment to North America through Strong Local Presence"
https://www.businesswire.com/news/home/20110118005694/en/Huawei-Opens-New-Headquarters-Canada-Deepens-Commitment

- "Huawei will continue to focus on strategic executive hires both in Canada and more widely across North America. Most recently, the company appointed Sean Yang to the position of President of Huawei Canada. Effective immediately, Yang will play a key role in expanding Huawei's sales/R&D/presence in the growing Canadian market."
- "Huawei will continue to focus on strategic executive hires both in Canada and more widely across North America. Most recently, the company appointed Sean Yang to the position of President of Huawei Canada. Effective immediately, Yang will play a key role in expanding Huawei's sales/R&D/presence in the growing Canadian market."

8 October 2009

"India's telecom agency raises China spy scare" UPI Asia
https://web.archive.org/web/20091009235328/http://www.upiasia.com/Security/2009/10/08/indias_telecom_agency_raises_china_spy_scare/1789/

- "Recently the Intelligence Bureau urged the DoT's Telecom Enforcement Resource and Monitoring cells to conduct surprise checks on the domestic set-ups of Huawei and ZTE Corp., two major Chinese telecom equipment makers."
- "critics say, some of the equipment is not manufactured in compliance with various electrical and telecommunications equipment safety guidelines and may prove to be a health hazard. However, Chinese companies, including Huawei and ZTE, deny such allegations.

29 March 2009

"Spy chiefs fear Chinese cyber attack" Sunday Times
https://www.thetimes.co.uk/article/spy-chiefs-fear-chinese-cyber-attack-3z9vqhslsnt

- "Intelligence chiefs have warned that China may have gained the capability to shut down Britain by crippling its telecoms and utilities. They have told ministers of their fears that equipment installed by Huawei, the Chinese telecoms giant, in BT's new communications network could be used to halt critical services such as power, food and water supplies."

17 December 2008

"Chinese spy fears on broadband frontrunner" The Australian
https://www.theaustralian.com.au/business/latest/chinese-spy-fears-over-broadband/news-story/3977bc5dcd66d95efacbde49e035f952

- "Huawei was the subject of a US congressional investigation on national security grounds this year after legislators expressed concern about its links to the Chinese military and intelligence apparatus. The concerns led Huawei to withdraw from its joint $US2.2billion ($3.3billion) bid to buy a stake in US internet router and networking giant 3Com."
- "Huawei, the shadowy company based in Shenzen and founded by former People's Liberation Army officer and Communist Party member Ren Zhengfei, has triggered debate in the US, Britain and India about whether it is a legitimate international telecom player or a company bent on doing Beijing's bidding."
- "a study by global think tank the Rand Corporation states: "Huawei maintains deep ties with the Chinese military, which serves as a multi-faceted role as an important customer, as well as Huawei's political patron and research and development partner."

15 January 2006

"The Huawei Way" Newsweek
https://www.newsweek.com/huawei-way-108201

- "Huawei, like many fast-growing Chinese companies, is a little too close to the Chinese government, and a little too obsessed with acquiring advanced technology."
- "According to press reports, India's Intelligence Bureau suspects that Huawei has ties to China's intelligence apparatus and military, and even performs the debugging sweeps for the Chinese Embassy in India. (Huawei says that's not true.)"
- "Opaque bookkeeping has also frightened analysts: an August report by the Thailand-based consulting company MWL argues that Huawei may rely on "unsustainably low prices and government export assistance" to make sales. The report adds that some customers "should be wary of making it a primary supplier for now."
- "Huawei has also been dogged by accusations of intellectual-property theft and corporate espionage. In 2003, Cisco sued the company in a U.S. court for copying computer codes used in its routers, machines that connect online networks. According to court documents, Huawei even copied Cisco's model numbers to make it easier for customers to switch to cheaper Huawei versions. Cisco eventually dropped the suit--but only after Huawei pulled the contested products from the market and agreed to alter their design codes. Neither company will reveal other details about the settlement."
- "In 2004, Huawei got a $10 billion credit line from the state-owned China Development Bank and $600 million from the Export-Import Bank of China to fund its global expansion."

5 April 2005

"Huawei wins series of contracts in Africa"
https://www.itweb.co.za/content/mYZRXv9JbZa7OgA8

- "Huawei has won a number of large telecoms contracts in Africa over the past six months amounting close to $500 million, supplying both fixed and mobile telecommunications solutions."
- "Kenya`s biggest mobile operator SAFARICOM has awarded Huawei a $34 million contact to reconstruct and update its Intelligent Network."
- "Huawei has also signed two contracts with Zimbabwe`s state-owned fixed-line operator TEL*ONE and mobile operator NET*ONE, worth $288 million and $40 million respectively."

20 March 2003

"3Com teams up with Huawei" The Register
https://www.theregister.co.uk/2003/03/20/3com_teams_up_with_huawei/

- "Networking suppliers 3Com and Huawei Technologies yesterday announced a joint venture partnership in China to target the country's emerging networking equipment market. The joint venture, called 3Com-Huawei in English and Huawei-3Com in Chinese, will be based in Hong Kong with principal operations in Hangzhou, China. Huawei's contribution to the Huawei-3Com will include 'enterprise networking business assets, including LAN switches, routers, engineering, sales/marketing resources and personnel, and licenses to its related IP'."

12 December 2001

"Chinese firm's dealings: police kept in dark about probe" The Hindu
https://www.thehindu.com/2001/12/12/stories/2001121200721100.htm

- "Huawei India, with two facilities in Bangalore, had 513 employees, of whom 178 were Chinese professionals. They were engaged in developing telecom software at the two R&D centers. ``Huawei Technologies is a private company that provides total telecom solutions to telecom operators across the globe. Our company's global business is in compliance with the U.N. standards and regulations. Huawei India has close cooperation with leading Indian IT companies and has completed several projects in collaboration with them,'' the spokesperson said."

ABOUT THE AUTHORS

Bob Seely MP is Member of Parliament for the Isle of Wight and sits on the House of Commons Foreign Affairs Select Committee. He served in Afghanistan, Iraq, and Iraq as a member of the Armed Services. Seely has written academically on Russian military and strategic doctrine as well as more generally on non-conventional and new forms of conflict.

Dr Peter Varnish OBE is an independent electronics and weapons engineer specializing in defence and security technologies and a visiting professor of cyber security at the University of Coventry. Previously, he had a long career serving in various technical capacities for the UK Ministry of Defence.

Dr John Hemmings is Director of the Asia Studies Centre and Deputy Director of Research at the Henry Jackson Society. He is also an Adjunct Fellow at CSIS and at Pacific Forum. He has held previous positions at RUSI, focusing on security issues pertaining to the Indo-Pacific.

CONTRIBUTING AUTHORS

Dr Robert Spalding is a Senior Fellow at Hudson Institute, where his work focuses on US-China relations, pertaining to economic and national security. Previously, he was Senior Director for Strategy to the President and contributed to the 2017 National Security Strategy. He has served in Iraq and Libya, and is fluent in Mandarin.

Danielle Cave is the Deputy Head of ASPI's International Cyber Policy Centre and has worked across government and non-government since 2006. She is a former analyst and team leader in the Open Source Centre at the Office of National Assessments. Previously, she worked at Lowy Institute.

Tom Uren is a Senior Analyst in ASPI's International Cyber Policy Centre. Prior to this, he worked in Australia's Department of Defence, across a range of cyber and internet security issues.

J. Berkshire Miller is a Distinguished Fellow with the Asia-Pacific Foundation of Canada. He is concurrently a senior fellow with Japan Institute of International Affairs, the Asian Forum Japan (AFJ) and the EastWest Institute.

ACKNOWLEDGMENTS

The authors would like to thank our contributing authors, Dr Robert Spalding from the Hudson Institute, Dr Danielle Cave and Tom Uren, from ASPI, and J. Berkshire Miller from the Asia-Pacific Foundation of Canada & Senior Fellow, Asian Forum Japan. We are also grateful to those who gave technical feedback on aspects of the paper, including Michael Shoebridge from ASPI, Klon Kitchen from Heritage Foundation, Dr Lindsay Gorman from the German Marshall Fund of the United States, and Ian Levy from the National Cyber Security Centre. We're grateful to Jessica Turner for her research assistance. We are also very grateful to Dr Andrew Foxall for reviewing this paper and a number of technical experts who also looked at the paper, but who must remain unnamed. Any mistakes or issues with the paper are ours alone.

Title: "DEFENDING OUR DATA:
HUAWEI, 5G AND THE FIVE EYES"
By Bob Seely, MP; Dr Peter Varnish, OBE
& Dr John Hemmings

The Henry Jackson Society
Millbank Tower, 21-24 Millbank
London SW1P 4QP, UK

www.henryjacksonsociety.org

HJS
Henry
Jackson
Society

ASIA
STUDIES
CENTRE

DEMOCRACY | FREEDOM | HUMAN RIGHTS

May 2019