OXFORD INFORMATION LABS

Networks and Geopolitics: How great power rivalries infected 5G

Stacie Hoffmann, Samantha Bradshaw and Emily Taylor

Oxford Information Labs

Oxford Information Labs

Centre for International Governance Innovation

The geopolitical power struggles, protectionist policies and national security concerns fuelling the race to 5G.

This is an unedited version of a forthcoming chapter in a book on diplomacy, edited by Chester A. Crocker, Fen Osler Hampson, and Pamela Aall, to be published in 2020.

Table of Contents

1Introduction

Michael Kovrig, a former Canadian diplomat, has found himself at the center of a geopolitical firestorm. Kovrig was arrested in Beijing in December 2018 by Chinese authorities for activities that "endanger national security". Interrogated throughout the day, without access to legal advice, held in isolation and barred from taking exercise outdoors, Kovrig's[1] arbitrary detention has caused deep concerns among Canadian officials (Vanderklippe, 2019). His arrest came days after Canadian officials detained Meng Wanzhou, the Chief Financial Officer of the Chinese telecom giant Huawei, for extradition to the United States (US) on charges of conspiracy to violate American sanctions on Iran and theft of a competitor's intellectual property: 'Tappy' the robot, developed by TalkTalk. Analysts have suggested that Kovrig's detention was a tit-for-tat retaliation for the arrest of Ms. Meng, but China has denied this. Huawei and Ms. Meng deny the charges, and a senior spokesperson called the indictments "unfair and immoral", urging the US to stop the "unreasonable suppression" of the telecommunications company (Swaine & McCurry, 2019).

Since then, the cadence of strike and counterstrike between China and the US has not abated. In March 2019, Huawei issued proceedings against the United States, seeking a declaration that US import laws are unconstitutional. In May, President Trump declared a national security state of emergency, and added the company to a US Entity List barring the supply of US-origin technology to Huawei. What had been a public dispute intersecting with key moments in complex trade negotiations between the two nations rapidly spread through international supply chains. Intended or not, the US government was imposing its will on the rest of the world by means of alarmist rhetoric and long arm regulatory measures.

The diplomatic fireworks underscore long-standing tensions about trade, intellectual property, international competition, and national security. But they also highlight great power rivalries that are currently being fought in cyberspace. The fight threatens to undermine the evolving global dialogue on legitimate national security concerns related to the deployment of 5G networks and the critical services they will support. Enveloping 5G in the wider power struggle risks drowning out significant and documented concerns of particular companies' security practices and accountability structures—most notably Huawei and ZTE.

The US strategy in this diplomatic chess match is unclear. Thus far the white noise from trade negotiations, IP theft, detainments and sanctions have prevented the US from articulating a convincing "clear and present danger" regarding 5G technologies. This impairs the country's ability to make the case for an American-led international order as it did in the Cold War (Trubowitz & Harris, 2019). The US has also failed to recognize that for other countries, the reality of an outright Huawei ban may not be practical, or even possible, due to existing networks and nations' bilateral trade and diplomatic relationships. As a result, the US is impairing wider, internationally-coordinated engagement on the issue.

- Thus far the white noise from trade negotiations, IP theft, detainments and sanctions… is impairing wider, internationally coordinated engagement on legitimate national security concerns.

The US administration's erratic interventions have impoverished an important public debate, have placed stress on long-standing alliances such as the Five Eyes, and risk alienating a cross section of nations sympathetic to western values and approaches to Internet governance. As a result, the US is missing an opportunity to highlight benefits

[1] Kovrig was a prominent political commentator with a focus on Chinese military strategy.

of western-built (and largely non-American) communications networks while advising on risks associated with particular vendors or approaches to 5G. Instead, by drowning out allies' evidence-based inputs, the US is isolating itself and preventing other like-minded nations from joining in the discussion constructively. A worst-case scenario could ultimately be a fractured Internet based on the 5G technology nations choose to adopt at the application and bespoke network layers.

As states struggle for power in cyberspace, many of the traditional structures and norms that have shaped the Internet thus far are under pressure (O'Hara & Hall, 2018). Although there has been progress in establishing high-level principles, most states have yet to turn these commitments into national practices and recent global efforts have highlighted more differences than common approaches (Hitchens & Gallagher, 2019)[2]. 5G—its physical equipment, software, technical standards, and the business models that underpin its global roll-out—has become a lightning rod for these international power struggles.

The way in which 5G is developed and implemented could have significant implications for the future of the open Internet, the norms and rules that govern it, and the ideological assumptions hidden deep within the technical infrastructure. At the national level, a delay in the adoption of new 5G technologies may also result in reduced economic development at home, harm to local industries' ambitions in international markets, and delayed economic and social benefits. The case of 5G also surfaces longstanding international tensions surrounding US dominance of key Internet systems and conflicting visions for the future of Internet governance: whether that be an open, multistakeholder approach, or a closed, top-down approach led by government. Taking a play from the US's playbook of global tech monopolies, China is attempting to shift this balance in its favor by creating a vertically integrated 5G monopoly.

This chapter will look at three facets of these geopolitical struggles. The first section of the chapter presents 5G technology, how it is being developed, what makes it different from existing network technologies, how this could impact Internet governance, and existing relationships and roles of stakeholders. The second section considers national security issues related to 5G through two lenses: cyber security and local/global markets. The third section contrasts Chinese and western approaches to technology and 5G development, elucidating the wider geopolitical landscape of the current dispute.

- The resulting techno cold war could hinder local development and adoption of 5G, create new fracture points for the Internet, and weaken the security of networks and services it enables.

The battle over 5G development is being played out as a zero-sum game, particularly by the US and China. The resulting techno cold war could hinder local development and adoption of 5G, create new fracture points for the Internet, and weaken the security of networks and services it enables ("Best of Today - Today," 2019).

[2] There have been several attempts at establishing norms for responsible state behavior in cyberspace, principally through the United Nations Group of Governmental Experts (UNGGE) and the Organization for Security and Cooperation in Europe (OSCE). Although the GGE established joint commitments in 2010, 2013, and 2015, the 2017 negotiations fell apart, reflecting growing divisions among states surrounding how global cybersecurity should be governed.

2 Internet Governance and the Politics of 5G

2.1 Internet Governance, Standards, and 5G

The Internet is not a single homogenous network, but is an ecosystem comprising technology, software, hardware, content, and institutions—an ecosystem which 5G is set to disrupt. The design and implementation of these infrastructures—from the undersea fiberoptic cables to critical Internet protocols and identifiers—are not neutral, but instead reflect particular economic interests or social values held by the engineers who design them (Bradshaw & DeNardis, 2018; Lessig, 2006; Winner, 1980; Zittrain, 2008).

For most of the Internet's existence, its values were shaped by engineers, educational consortiums, government institutions, and commercial forces located in western democracies. There have been longstanding concerns over US[3] dominance of the Internet, its legal environment, support for multistakeholder governance and values such as privacy and freedom of speech (Abbate, 1999; Goldsmith & Wu, 2006). One example was the perceived influence of the US government over ICANN prior to the IANA transition. Frustrated by the decentralized and multistakeholder approach to Internet governance, some governments—including authoritarian regimes—have been advocating for state-led multilateral approaches through the United Nations (UN) and its specialized agency, the International Telecommunications Union (ITU).

In essence, it is not uncommon to debate the influence that a technology's "home" environment and legal structure have on an organization and its impact on trust (Marks, 2019). With a new, Chinese, leader in 5G, Chinese vendors are now being placed under similar scrutiny from government and industry as American technologies and industry have previously experienced, particularly in a post-Snowden era. Western commentators are skeptical of the accountability and transparency of companies with opaque legal structures, operating within a single-party authoritarian state, shielded from western free market dynamics. With 5G promising to connect more people, things, and services than ever, it would only make sense that technologies being developed by Chinese companies reflect a Chinese approach to technology, including reinforced government control over the Internet, data, information, and even users. The example of the Chinese Social Credit System enabled by the digital economy illustrates that there will be no guarantee that Chinese-origin technologies embody western values (Liang, Das, Kostyuk, & Hussain, 2018).

- It would only make sense that technologies being developed by Chinese companies reflect a Chinese approach to technology, including reinforced government control over the Internet, data, information, and even users.

[3] From the Internet's early origins as a US Cold War military experiment (Naughton, 2016), to the International Corporation for Assigned Names and Numbers (ICANN)—the California-based non-profit organization responsible for coordinating global policy for the Domain Name System—to global commercial forces such as Google, Apple, and Facebook, the Internet has been strongly influenced by American perspectives.

Figure 1 - 4G City

Shorthand for "fifth generation" mobile networks, 5G is the baseline standard that will revolutionize mobile networking technologies. Like previous 4G and 3G technologies, 5G is a technical standard that connects devices to a network. But whereas previous technologies supported handset-to-handset voice and data communication (see Figure 1), 5G is being designed to handle the connection of billions of devices and data transfer at much faster and more reliable rates. In practical terms, this will mean a proliferation of masts, aerials and connected devices from CCTV, to drones, wearables, connected cars, refrigerators, game consoles, and robots (Figure 2). 5G will become the technical foundation upon which we carry out our daily lives, not just as technology users, but as citizens and participants in society.

Figure 2 - 5G City

5G also represents the evolution of telecommunications architecture from static networks of wires and switches to responsive, high-powered computers and networks managed by software. Ultimately 5G is resulting in a consolidation of the Internet's

layers, bringing physical, logical and, in some cases, application layers closer in proximity. The ways in which the Internet's layers are re-aligned will largely be impacted by a particular deployment of 5G. Figure 3 shows consolidation of the logical and physical layers likely to occur in most instances.

- 5G also represents the evolution of telecommunications architecture from static networks of wires and switches to responsive, high-powered computers and networks managed by software.

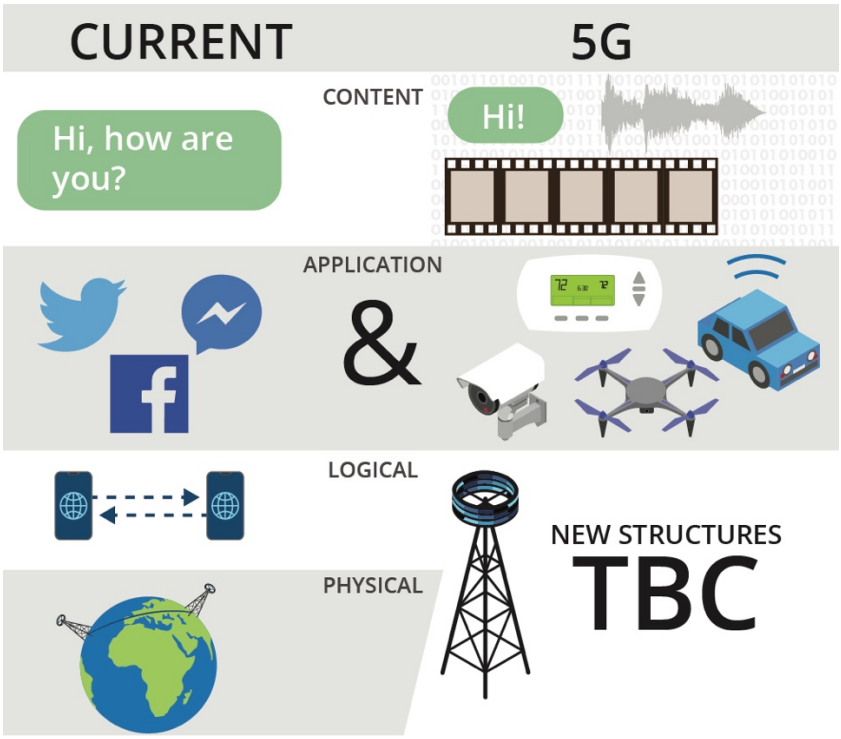

Figure 3 - Internet Layers

The development and testing of 5G is carried out by a constellation of actors including operators, equipment and parts providers, governments and other interested stakeholders[4]. China's Huawei alone invested CNY 89,690 million (USD 13.4 m) in research and development in 2017 ("Research & Development - About Huawei," 2017). The company is one of the leaders in 5G technology, aiming to have standalone 5G deployment by 2020, five years ahead of the rest of the world (Eurasia Group, 2018). Western telecommunication equipment manufacturers—such as Ericsson, Nokia and Qualcomm—had been leading the way, thus far, on developing patents, but Huawei has recently strode head (Pohlmann, 2018).

These actors come together across numerous standard development organizations (SDOs) and industry bodies to define the technical specifications of 5G. Some important SDOs in this space include the 3rd Generation Partnership Project (3GPP) and the European Telecommunications Standards Institute (ETSI), as well as industry bodies such as GSMA[5]. The Radiocommunication Sector of the ITU (ITU-R) is where technical specifications and radio spectrum allocation for 5G are being negotiated by governments. ITU-R has launched a project on next generation network technology called International Mobile Telecommunication (IMT)-2020, and 3GPP is contributing the technical specifications it develops to this project in the ITU-R.

[4] Government-led efforts have been complemented by big operators and other players in the East such as Samsung, KT, SK Telecom (Korea) and Huawei, ZTE, China Mobile, China Unicom and China Telcom (China). In the West network operators like AT&T, Verizon, Vodafone, Telefonica, Telenor and Deutsche Telekom have been testing 5G technologies for deployment.

[5] The Internet Engineering Task Force (IETF), a key multistakeholder Internet standards body, is currently developing the next generation of Internet protocols which deserve their own review through the lens of geopolitical issues. Although these protocols will be used in 5G, the IETF is not working on 5G-specific standards.

Yet even these seemingly technical and mundane forums quickly become politicized. Work in the ITU related to its IMT-2020 project but outside the ITU-R sector, such as edge computing and network management, are primarily steered by just China and Korea. This is providing China the opportunity to legitimize and promote their own flavor of 5G (Lazanski, 2019). Additionally, China has created its own "IMT-2020 Promotion Group" outside the ITU for "research and international exchange", in which Huawei plays a key role (Huawei, 2018).

The choice of standards bodies in which to engage reflects stakeholders' and states' ideology. Concentrating on work in SDOs like 3GPP and GSMA reflects a preference for industry-led and a multistakeholder approach to standards-setting (a western preference), while working in bodies like the ITU reflects a preference for a government-led and multilateral approach (the favored approach of those looking for greater control over the Internet) (Lazanski, forthcoming). A summary of these initiatives and their key 5G work is summarized in Table 1.

- The choice of standards bodies in which to engage reflects stakeholders' and states' ideology.

Body	5G-related work
3GPP	Developing technical specifications for 5G (so-called "non-standalone" and "standalone" specifications[6]).
ITU-R	Negotiating technical specifications and international regulations for harmonized radio spectrum use for 5G.
ETSI	Developing standards for technologies that will enable and optimize 5G, such as network function virtualization (NFV), multi-access edge computing (MEC), next generation protocols (NGP), and millimeter wave transmission (mWT)[7].
GSMA	Developing frameworks, guidance, and best practices through industry collaboration on key 5G topics, such as migration to virtual networks[8], security[9] and spectrum policy[10].

Table 1 - Where are 5G Standards Being Developed?

2.2 The Politics of 5G

This section highlights five ways in which 5G is susceptible to politics: the impact of standards, the adaptive nature of the network, net neutrality, competition policy, and intellectual property[11]. Each element is discussed in turn.

First, we look at the manner in which 5G technologies are elaborated through standards and developed and deployed as hardware, software, and services, embeds

[6] Non-standalone 5G specifications are designed to use existing 4G LTE infrastructure for 5G mobile communications, whereas standalone specifications support 5G independent of existing 4G technology and are due for release in early 2020.
[7] See https://www.etsi.org/technologies/5g
[8] See GSMA's reference document on Migration from Physical to Virtual Network Functions: Best Practices and Lessons Learned available here: https://www.gsma.com/futurenetworks/5g/migration-from-physical-to-virtual-network-functions-best-practices-and-lessons-learned/
[9] See GSMA's Working Group on fraud and security here: https://www.gsma.com/aboutus/workinggroups/working-groups/fraud-security-group.
[10] See the GSMA 5G spectrum public policy position available here: https://www.gsma.com/spectrum/resources/5g-spectrum-positions/
[11] There are additional concerns such as Internet consolidation ("Future Thinking," 2019) and human rights (Freedom House, 2018) which are not fully explored here but which are equally important and deserving of detailed analysis.

a range of public interest issues, including convergence of technologies, intellectual property, Internet neutrality, competition policy, and security. With an untold number of devices and types of data connected by 5G, supporting a wide variety of services, there are increased risks of data theft, espionage, or compromise with real-world physical effects. Accordingly, the politics of 5G security are not only about confidentiality, integrity, and availability of information and resiliency of networks, but protection of the underlying services that 5G enables. 5G is built on physical and virtual layers of the Internet stack—physical network components, Internet protocols and cloud/virtual technologies. Thus, 5G is not only susceptible to the same variety of threats as any system connected to the Internet, but, given its low position in the stack embodied by the points above, 5G introduces a greater and broader range of security threats than traditional communications networks.

- 5G is not only susceptible to the same variety of threats as any system connected to the Internet, but … represents a greater and broader range of security threats than traditional communications networks.

Second, 5G converges computing and communications, pushing network intelligence closer to the "edge" of the core network (i.e. closer to the application layer)[12]. Intelligence in the core[13] of the network, supported by massive data centers, will manage and configure the network in real time to optimize efficiency—making it responsive instead of static. As a result, there are greater opportunities for censorship and control over specific segments of the network: rather than cutting access to the entire Internet, specific neighborhoods, government offices, or businesses could be isolated or targeted.

Third, 5G manifests the most recent reincarnation of contentions surrounding net neutrality (Crawford, 2018). 5G fundamentally changes business models in the mobile and Internet sectors (Obiodu & Giles, 2017). For example, the mobile operators' business models are shifting towards that of a connectivity and cloud service provider as networks move from physical infrastructure of switches and relays to high-powered computers connected by radio waves and fiber cables. The 5G network will be run and managed by software (a software defined network (SDN)) and hosted by large data processing centers (e.g. Amazon Web Services). Operators were previously owners of the Internet's "dumb pipes" but 5G increases their control over intelligent networks and services. Connectivity, platforms or other services will be leased out to or resold by third parties—like a smart city, healthcare services, or content providers such as Netflix. Another key difference is the focus not on individual consumers, but on new business-to-business (B2B) service models. As B2B agreements are negotiated, 5G infrastructure providers could prioritize certain companies' speeds and service access unfairly over others, distorting the marketplace for consumers.

Fourth, 5G technology embeds issues related to competition policy. The shift from network provider to service provider creates an attractive vertically integrated business model, where an operator becomes the middleman between hardware, software, network management and services. Tech companies with a diversified portfolio, like Huawei, are in good standing to provide a full end-to-end solution for business and consumer alike, including designing the devices and services that connect to the network. This could result in the rise of a vertically integrated, global 5G tech monopoly or the further entrenchment of existing dominant market positions. Operators will have powerful incentives to create market distortions by prioritizing certain services and actors (including themselves) over others.

Fifth, although 5G's initial technical specifications are open and freely available, intellectual property[14] for hardware and software still plays a key role. This potentially

[12] This is where the term "edge computing" comes into play in 5G networks.
[13] The network "core" is responsible for operations and critical security functions such as network management and device authentication.
[14] Intellectual property rights are protected under international trade law. For example, by the World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).

impairs traditional Internet values around permissionless innovation, leading to disputes over intellectual property rights and access to information. Firms are rushing to register patents which can generate future revenue streams, help secure a dominant position in 5G markets and generate ongoing revenue from infrastructure maintenance and support.

Although 5G equipment procurement and standards development might appear to be neutral, 5G represents a fundamental evolution in the underlying architecture of the Internet, with new technology, physical infrastructure, use cases and changes in business models. Importantly, its rollout is tightly coupled with questions surrounding the ideological dominance and governance structures of an Internet that will support future connectivity and critical services, which many in the West have taken for granted to date. This evolution also creates new stress points, for example at the network edge and spectrum use, that could fracture the current global Internet ecosystem. The stakes are high for both states and domestic industry, such as first mover advantage, economic growth, intellectual property ownership, and resources required to deploy 5G networks.

- This evolution also creates new stress points, for example at the network edge and spectrum use, that could fracture the current global Internet ecosystem.

3 5G and National Security

In western media, much of the political positioning around 5G is framed around fears over political and corporate espionage via backdoors and the threat of withholding intelligence from allies (Bryan-Low, Packham, Lague, Stecklow, & Stubbs, 2019; Lecher, 2019). Though these positions are sometimes motivated by genuine security concerns, such concerns are sometimes co-opted to cloak protectionist measures in response to international economic power struggles (Steinbock, 2017). Unfortunately, stress is being placed on existing alliances, disengaging and alienating much of the world from the discussion. As nations become reliant on digital technologies to run their cities, enable digital economies, and measure development, technologies like 5G will be integral to national wellbeing and security.

The following section explores national security concerns into two buckets: cyber security[15]; and economic concerns—primarily local industry and access to foreign markets. The aim is to understand where risk really lies in the 5G ecosystem, not only those fears expressed in the media. Admittedly, China is one of many possible threat actors in such scenarios, but there are particular factors that highlight the potential negative impact on national security of a global Chinese leader in 5G.

3.1 Cyber Security and 5G

3GPP and its international membership of industry and national partners (including the US and China) has adopted a "security by design"[16] approach to the development of 5G technical specifications—the specifics of which we will not address here. This means security tools are being built into the technology—something that wasn't done

[15] For the purpose of this chapter, we take a general approach to cyber security and the reduction of risk of cyber attacks. Considerations include the protection of networks and systems (including hardware and software), services, and data from threats. Threats manifest through a variety of means, including but not limited to unauthorized access (e.g. hacking), malware (e.g. WannaCry virus) or DDoS attacks (e.g. the Dyn Attack).

[16] *Security by design* is a process by which security concerns are taken into account from the outset of conception and design, resulting in security tools and risk mitigation being built into the end product instead of added on after development.

for earlier mobile technologies. However, security-by-design alone will not resolve the security conundrum in the multipolar 5G environment. Standards can still contain in-built security flaws or unexpected side effects and will not address all future threats. Additionally, some governments and other actors deliberately interfere with both standard setting processes and networks to advance their interests (Parton, 2019). It is not a matter of if, but when, how and by whom networks will be exploited.

Governments are considering the long-term impacts of today's decisions. 5G will support critical infrastructure and services in an increasingly unknown environment due to bespoke deployments and responsive networks. Therefore, procurement choices for 5G infrastructure need to take into account both immediate concerns such as social and economic development and long-term issues like commercial relationships with third parties. A key difference between building communications networks and other physical infrastructure (e.g. roads) is the required, constant and highly specialized maintenance and support. In addition to supply chain concerns—in which China plays a key role—security complexities are augmented by 5G. These include unique and widespread deployments of high-capacity computers, the software-based core network's susceptibility to cyberattacks (e.g. malware), the reduced effectiveness of traditional risk mitigation techniques (e.g. product and systems testing), and an increased attack surface[17].

- Procurement choices for 5G infrastructure need to take into account both immediate concerns such as social and economic development and long-term issues like commercial relationships with third parties.

Unlike previous networks that relied heavily on hardware, 5G will be primarily software-based, run and managed in a cloud environment. This opens the entire network to a new source of cyberattacks[18]. Recent years have seen a ramping up in the severity of cyberattacks, including NotPetya, Wannacry and the Mirai attacks, which have led to the disruption of websites and services. However, an attack on 5G could lead to physical harms, and disrupt a wider range of critical services, such as the network management servers, a dedicated factory network, or a city's transportation system.

Due to the nature of 5G, the attack surface is significantly greater than previous networked technologies[19]. It is projected that there will be 20 times more radio antennae to relay information, each representing a potential vulnerability (Crawford, 2018). This will increase the threat from devices connected to and data on the network, putting the services and systems the network enables at risk. For example, a compromised smart water supply system could result in contaminated water, public health issues, or even the spread of water-borne diseases such as cholera.

- It is projected that there will be 20 times more radio antennae to relay information, each representing a potential vulnerability.

Securing 5G systems will require specialized tech firms to have ongoing access to networks, software and data processing centers—bringing with it opportunities for bad actors to exploit those networks for strategic gain (Hemmings, 2018). Governments are questioning the degree to which a single provider should be entrenched in networks that form part of critical national infrastructure. Lack of component diversity will increase the risk of a single point of failure in the network. Network equipment can be a backdoor in itself, potentially providing vendors access to all of the data, information, services, and systems communicated or provisioned over the network (Cerulus, 2017). Additionally, 5G could allow for more targeted manipulation of that network. While it will be difficult to build a 5G network without Huawei, the principle of purchasing parts from rival suppliers supports resiliency and protects against a single point of failure ("Huawei is at the centre of political controversy," 2019).

[17] An *attack surface* is the sum of the vulnerabilities, or points susceptible to attack, in, for example, devices, software, hardware or systems.
[18] These include malware, hacking, man-in-the-middle and distributed denial of service (DDoS) attacks.
[19] This is due to an increased amount and variety of physical network equipment like cell towers and connected "things", as well as vulnerabilities related to computer software, cloud computing and data.

Every system will have bugs and vulnerabilities which can be exploited by adversaries ("Huawei is at the centre of political controversy," 2019). Edward Snowden revealed that the US hacked Chinese telecommunications firms and the network backbone of Tsinghua University (Lam & Chen, 2013). China is alleged to have siphoned off data from the African Union's networks to China for years—networks built, paid for and managed by Chinese companies including Huawei (Fidler, 2018). There is debate as to whether or not this was intentional. If not, the fact it took so long to identify the security flaw calls into question the quality of Huawei's security practices.

Mitigating risks will be more difficult with 5G. Testing and monitoring is a common risk mitigation technique for systems and equipment. The UK's Huawei Cyber Security Evaluation Centre (HCSEC) was built for this purpose. Although there are different views on the HCSEC's effectiveness, it provides an evidence-based, technical assessment of networks and components ("FCC Proposes to Protect National Security Through FCC Programs," 2018; Intelligence and Security Committee, Intelligence and Security Committee, Great Britain, & Parliament, 2013). Testing and evaluation also adds a degree of protection from supply chain exploitation, an increasingly complex threat to global equipment and software markets from which no country is immune or excluded from taking advantage of opportunities (Schneier, 2018).

However, existing testing and monitoring programs will not be as effective for 5G (Donaldson, 2018). Firstly, there is the challenge of inspecting an enormous volume of code for vulnerabilities or defects—which in itself could take years to analyze. Even if it is possible, due to "developer's advantage" it will be more difficult for customers (i.e. governments and operators) to analyze the code. Testing reviews a system at a particular point in time and 5G networks are not static. They will be constantly adapting, possibly in real time, and seemingly mundane maintenance such as software updates can cause unforeseen issues or be used for malicious purposes (Lin, 2019). Security evaluations also fail to address deployment diversity—a key aspect of 5G—which can affect the behavior of a device or system (Donaldson, 2018; Rogers & Ruppersberger, 2012).

- 5G networks will be constantly adapting, possibly in real time, and seemingly mundane maintenance such as software updates can cause unforeseen issues or be used for malicious purposes.

In any industry there is a difference in quality and company culture between vendors, both of which have a direct impact on product resilience and incident response. Company culture is reflected in how we, as citizens and operators, can expect a network provider to respond in the face of an incidents. Although Chinese officials try to downplay the issue, there is plenty of evidence related to Huawei's sub-standard security and support practices (Lin, 2019). The UK's HSEC and Australian government have executed technical reviews of Huawei equipment and voiced concern over the company's products and processes (Huawei Cyber Security Oversight Board, 2019; Fifield & Morrison, 2018). NCSC's technical director, Dr. Ian Levy, called Huawei equipment "shoddy" and its engineering outdated, both of which impacts the resiliency of the network (Hancock, 2019). Instead of highlighting security concerns substantiated by testing and experience, the media has focused on economic power struggles, claims of sanctions violations, and corporate espionage. In contrast, the US's approach of scaremongering and threatening allies without highlighting hard evidence has been unhelpful. Ultimately the global dialogue on 5G cyber security has been undermined by making the debate irrelevant to the vast majority of countries around the world—and is partially due to a lack of coherent strategy and evidence by the loudest voice, the US government.

3.2 Markets, Standards, and 5G

China is poised to assume first-mover advantage in 5G technology. This is buoyed by the fact that Chinese companies have the resources—including a favorable regulatory structure and financial capital—to run large 5G testbeds, tightly control supply chains, develop vertical markets, and access a wide variety of global markets. In technology markets, first-mover advantage generally leads to a winner-takes-all scenario, due to economies of scale, network effects, and switching costs—these factors help to explain why the race to 5G has become a zero-sum game (Barwise, Featured, 2018, Truth, Trust, & Comments, 2018). 5G will bring decades of vendor lock-in for critical infrastructure providers. It could also result in walled gardens of devices and services, capture of markets, further reduction in market competition and the emergence of a vertical, Chinese, 5G tech monopoly.

The emerging 5G ecosystem is already hardening preferred business models. Chinese content platforms like Alibaba are heavily investing in 5G via mobile operators (e.g. China Unicom), likely in a bid to alter the business relationship between Internet layers and influence business models (Triolo & Allison, 2018). Huawei, with its ability to bundle 5G-enabled services and network solutions, is an even more attractive prospect—creating a more concentrated 5G technology marketplace. Paired with vendor lock-in, a generation would be enough time for tech companies like Huawei to effectively quash foreign competition—particularly if markets are not carefully protected from distortion, and local research and development (R&D) is not sufficiently supported.

- Paired with vendor lock-in, a generation would be enough time for tech companies like Huawei to effectively quash foreign competition.

Some experts wonder if western companies should adopt a riskier strategy such as leapfrogging to 6G innovation. 6G, the name given to the next-but-one technology, will further develop 5G software and services while using 5G infrastructure. There are no American network providers like Ericsson (Sweden), Nokia (Finland), Samsung (Korea) or Huawei, but American companies are well positioned to develop the revolutionary software and services layer of 6G (Triolo & Allison, 2018). However, this risky strategy could result in western companies losing existing market shares in Internet infrastructure. Additionally, the West would still need to engage in and devote resources to technology development and standardization to protect national interests, such as spectrum allocation and future market share.

Critical 5G spectrum allocation negotiations at the ITU's World Radio Congress (WRC) in November 2019 will highlight points of contention in 5G standards development. In 5G different spectrum ranges can be given priority for core communications or supplemental use cases. The choices will impact the technical requirements for network equipment and devices connecting to the network, which could be another fragmentation point (Obiodu & Giles, 2017). Unsurprisingly the US, China, and others are at loggerheads on the exact ranges to allocate[20].

While a fracture point in spectrum allocation increases the threat of a splinternet, more likely is a geopolitical division in markets for the hardware and software of Internet infrastructure. This would result in reduced access to some markets for western equipment providers, especially in the developing world. It would also

[20] The US prefers high frequency for core communications while China in particular prefers low frequency. Within regions there is also a lack of alignment over the exact bands to be released (e.g. Europe), and sometimes even national players differ in opinion (e.g. Japan) (Mavrakis, 2018; Triolo & Allison, 2018). Africa's position is unique as it has yet to complete digital migration of TV which would release critical bands for 5G (Reed, 2018).

relegate China's market access to developing countries and states that prefer Internet governance to be done along the lines of the ITU's "UN bloc politics", opposed to the open, industry-led, multistakeholder approach supported by western countries and the 5G models they promote (Nye, Jr., 2014, p. 7).

Competing visions of the Internet are echoed in the standards development process and reflected by the SDOs or technical groups specifically chosen by different parties. There are long-standing concerns related to SDOs being used as a political tool to build in vulnerabilities, sabotage standards, or make design decisions to benefit specific stakeholders (Forrell & Solaner, 1986; Wessel, 2019). More recently, it has emerged that China is increasing participation in and acquisition of key roles in intergovernmental and standards bodies such as the UN, ITU, IETF and 3GPP in order to fast-track their own "flavor" of Internet technology, legitimize the corresponding standards, and sell it to the world (Lazanski, 2019; Okano-Heijmans, van der Putten, & van Schaik, 2018).

Such an alternative Internet governance model would give certain governments and industry players greater control over citizens' data, impair access to information, and have a chilling effect on expression. Chinese approaches to Internet technology include centralized and indiscriminate data aggregation (usually with the government or one of its many entities, augmenting the potential for surveillance), increased control over aspects such as user profiles or information flows, and social engineering tools such as China's highly criticized Social Credit System and surveillance technology used to monitor minorities (Byler, 2019; Lazanski, 2019). These attributes are particularly attractive to authoritarian governments (for example in the Gulf) who have long been fighting for greater control over the Internet and access to user data and profiles—effectively reinforcing digital divides between Internet users based on access to information or services and human rights protections.

- Chinese approaches to Internet technology include centralized and indiscriminate data aggregation, increased control over aspects such as user profiles or information flows, and social engineering tools and surveillance technology.

Western governments have an interest in protecting market access and local industry to avoid a 5G marketplace dominated by Chinese-origin technology. China has proved successful at building globally competitive indigenous companies. Part of this is thanks to a decline in western equipment and network technology providers[21]—which many attribute at least in part to Huawei's growth in global market share. As a knock-on effect of smaller market shares and revenues, western companies are unable to allocate sufficient resources on R&D to maintain their competitiveness with Chinese actors. Chinese companies also have an uncanny ability to undercut the competition by offering network equipment at half the price of its competitors such as Ericsson or Nokia. Critics claim this amounts to predation, enabled by China's "illegal government subsidies" and stolen intellectual property (Tong, 2019).

Predatory market practices do not fully account for Huawei's competitive edge. China's foreign development Belt and Road Initiative also assists, for example, through easier access to markets and bundling networks with other Belt and Road initiatives. China, through a patient, long-term strategy, is creating an asymmetric market environment by using its power to bind nations to its financial and technological solutions (Manuel, 2017). The Belt and Road Initiative has built networks across Africa, South America, and Asia. Sometimes this is paired with anticompetitive lending practices backed by Chinese state-owned banks. For example, in Mexico a 1% interest loan with the Bank of China was offered if 80% of the funding was spent with Huawei when building a 4G network (Johnson, February 6, & Headquarters, 2019). In Brazil, Huawei bid on a radio network project and provided the broadband network, service, and support at no extra charge—effectively locking in a generation of Brazil's internet

- China, through a patient, long-term strategy, is creating an asymmetric market environment by using its power to bind nations to its financial and technological solutions.

[21] Companies such as Alcatel, Lucient and Marconi closed down or were absorbed by remaining competitors like Nokia.

technology (Johnson et al., 2019).

While contracts with Chinese companies may not require substantial investment at the outset, the potential long-term effect paints a different picture. China has been called out for its predatory loan practices that undermine sustainable financing and often result in China's acquisition of valuable national resources (Hurley, 2018). For instance, China has assumed shares of a Sri Lankan port in return for USD 584 million in debt forgiveness (Sirilal, 2018). This could foreshadow further absorption of key national resources by Chinese entities which may be used to float its own complex economy if and when other at-risk countries[22] fall short on debt repayment.

- This could foreshadow further absorption of key national resources by Chinese entities which may be used to float its own complex economy if and when other at-risk countries fall short on debt repayment.

The evidence suggests that China is pursuing a multi-pronged strategy whose medium-term objective is to lock out foreign industry from competing in 5G deployment internationally. Key levers include generous ICT infrastructure projects, and the bait-and-switch lending practices described above. The strategy is further enabled by the dwindling number of international competitors in network equipment markets[23]. Knock-on effects include the widespread uptake of technologies that reflect Chinese approaches to Internet governance and disregard for international human rights frameworks. This could result in the fracturing of Internet technologies at the spectrum and services layers, while a global monopoly tolls the bell for non-Chinese competitors.

4 National Strategies and 5G

5G will support the digital economy and economic growth, determine our access to public utilities and other goods and services, and enable even more invasive and pervasive surveillance by corporations and governments. Economic stability and national security are increasingly linked by governments, with technology billed as a key supporting factor ("Geoeconomics," 2018a; "Geoeconomics," 2018b). In the case of China, a long-view foreign policy is intertwined with national policy, using foreign markets and assets to build local economic stability and increase global power. This is in contrast to the US where national policy informs foreign policy but is largely reflective of—and changes with—the party politics of the President. As the world becomes ubiquitously connected, the ability to disentangle the technical from the political is increasingly difficult. With international economic rivalries manifesting in 5G, governments are tasked with making decisions—and alliances—that will impact local industry, critical infrastructure and citizens for years to come.

4.1 Chinese Approaches

Historically, China is known as a major manufacturer and exporter of goods, but also for corporate espionage, protectionist policies, government influence in private industry, and its Great Firewall[24]. Over the past 20 years, China has adopted a strategic focus on diversifying its economy to include digital technology innovation

[22] Eight of the most vulnerable countries include Djibouti, the Maldives, Laos, Mongolia, Tajikistan, Kyrgyzstan, and Pakistan (Hurley, 2018).
[23] Simplistically, this includes a small mix of American, European, Japanese, Korean, and Chinese vendors.
[24] The Great Firewall creates a national intranet only connected to the global network through a limited number of highly monitored gateways, creating a connected environment (including data, information, and users) which is easier to monitor, manage, and track.

and exporting[25]. Development targets include plans to be 70% self-sufficient and hold a dominant position in global trade—highlighting the entanglement between national and foreign strategies (McBride & Chatzky, 2019).

Supporting China's ambitions is a complex weave of public-private relationships, national policies, and foreign development enacted through various forms of soft and hard power. These policies have a direct impact on the development of 5G and related markets through intellectual property, technical standards and competition policy. Although western countries also take measures to support local industries, they are more transparent and within the bounds of internationally-agreed norms (e.g. WTO trade rules). A closer look at China's strategy uncovers a more complex and multi-layered approach in an attempt to skirt those same norms while maintaining the façade of complying with international rules-based systems (McBride & Chatzky, 2019). It is not difficult to imagine the successful implementation China's strategies resulting in a vertically integrated global tech monopoly—echoing the emergence of American tech monopolies and their role in shaping today's Internet. China does not intend to relinquish its current level of control over the Internet with the adoption of 5G, and Chinese-origin technologies should be considered within this light.

- It is not difficult to imagine the successful implementation China's strategies resulting in a vertically integrated global tech monopoly – echoing the emergence of American tech monopolies and their role in shaping today's Internet.

4.1.1 Opaque Public-Private Relationships

Deliberate actions taken by the Chinese government to support technology innovation, manage local markets, and skew foreign markets have been described as "political engineering" (Rosen & Kennedy, 2019). Strong government influence is also reflected in China's authoritarian approach to Internet governance, characterized by pervasive surveillance and promotion of "government micromanagement of the internet" (O'Hara & Hall, 2018, p. 8). Close coordination between industry and government, including civil-military integration, remains opaque (Cheung, 2018, p. 321). Huawei is a key market actor in this arena, focusing on Chinese approaches to data, infrastructure and cloud security. It is one of 10 firms that account for 40% of the national cyber security market (Cheung, 2018). Chinese companies that do not follow the appropriate line in international forums risk difficulties back home. In 2016, Lenovo initially voted for a US-origin (Qualcomm) technology being developed for 5G by 3GPP; but this vote was switched in the final round after public, and likely government, pressure to support Huawei's standard (Hersey, 2018). The private-public relationship is worsening the business climate in China for foreign firms, and the country's relationship with other nations (McBride & Chatzky, 2019; Zarroli, 2019).

Additional insight into the blurring boundaries between public and private in China can be gained from examining the flow of financial capital through government subsidies, as well as diversified funding streams including venture capital, private equity investors, and stock markets (Kennedy, 2017, p. 18)[26]. These financial links can be exploited to exercise soft power on private industry (Intelligence and Security Committee et al., 2013; Rogers & Ruppersberger, 2012). Huawei usually counters claims of government ties with carefully-worded statements about employee ownership and the absence of government on its board (Huawei, 2019). However, during an investigation of Huawei by the US government in 2012, internal company

[25] From 1997 to 2017 China's high-technology exports increased from approximately USD 20.5 billion to USD 504.4 billion (World Bank, n.d.).
[26] In 2016 a USD 46 million "cybersecurity investment fund" was established by the China Internet Development Foundation, which has links to the Cyberspace Administration of China (Cheung, 2018, p. 322). In the context of Chinese companies' foreign investments, a Chinese state-owned investment company (CITIC) was effectively handed a financial stake in the Czech Republic after assuming the assets of a Chinese conglomerate (CEFC) (Muller, 2018).

documentation was deemed "state secret" and Huawei reported a Chinese Communist Party Committee within the company—a common occurrence in China (Johnson et al., 2019; Rogers & Ruppersberger, 2012). More recently, in June 2019 China requested a stop to a WTO review of its market economy status—a battle China was losing—brought forward by the US and European Union (Miles, 2019c). Overall, the secrecy around Huawei's business practices have made it difficult to determine the relationship between state and firm. This heightens western distrust of claimed separation between public and private entities, particularly in light of recent changes to national security policies.

4.1.2 National Policies, Strategies, and the Tech Industry

Over the past two decades a raft of national policies and strategies have been put into place to proactively foster, promote and protect the tech sector. These well-documented protectionist policies effectively promote local providers, disadvantaging foreign investors, and have implications for privacy and access to data (Hoffman & Kania, 2018; Sacks, 2018). Policies support key emerging technologies including 5G, Artificial Intelligence, Internet of Things and facial recognition. On the international stage, this national strategy has resulted in increased involvement of Chinese tech players in international SDOs, and the holding of strategic positions within those organizations. Strategies include:

- These well-documented protectionist policies effectively promote local providers, disadvantaging foreign investors, and have implications for privacy and access to data.

- Intellectual property ownership through research and development, mergers and acquisitions, joint partnerships, or technical standardization;
- Support for strategic industries including funding, market restructuring and manipulation;
- Use of competition policy and national security[27] rhetoric to promote local companies and constrain foreign competition (Kennedy, 2017); and,
- Building Internet infrastructure (e.g. as part of the Belt and Road initiative) globally.

China's recently enacted Cybersecurity Law (2017), requires data localization, restricts cross-border data flows, and requires "hardware and software reviews for information technology firms" (Cheung, 2018, p. 322). To comply, foreign companies need to partner with local data storage providers or build their own local resources. Both require the handing over of proprietary information (e.g. data, hardware and software) for review, risking the potential loss of privacy and intellectual property. An additional impact is the loss of business for entities located outside of China, such as those providing data analysis or cloud services, thus constricting the global marketplace.

- Indigenous intellectual property paired with the technical standards would enable the mass exporting of a Chinese approach to Internet technologies.

The drive to develop indigenous intellectual property is a common thread in China's recent policies[28]. Paired with the technical standards, this would enable the mass exporting of a Chinese approach to Internet technologies. Combined, Chinese entities currently own 10% of new 5G IP[29], compared with only 7% in total for the predecessor 4G technology (Scott, 2018). The Chinese share of 5G IP is likely to grow when standalone specifications are released in 2020. This could result in even cheaper Chinese products, reduced reliance on imported IP resulting in lower costs

[27] For instance, the National Intelligence Law, Counter Espionage Law, and State Security Law. It is also worth noting that the Xi Jinping government takes a broad interpretation of "national security" including 11 areas: political, territorial, military, economic, cultural, social, economic, science and technology, information, nuclear, and natural resources (Wong, 2017).

[28] Some motivation behind the drive to build China's high-tech industry and for self-sufficiency was highlighted by President Trump's now repealed ban on semiconductor sales to ZTE which would have resulted in the company's demise ("Geoeconomics," 2018a).

[29] Industry leader Qualcomm reportedly owned 15%, followed by Nokia with 11% at the end of 2017.

through reduced royalty payments, increased inward flow of capital by foreign adoption of Chinese IP, and reduced reliance on global supply chains susceptible to geopolitics (Cheung, 2018, p. 311). These market advantages will be mirrored by increased costs to foreign competitors of integrating a *de facto* standard based on Chinese IP, and governments like the US having one fewer bargaining chip with China.

Western countries have reacted to the Chinese strategies by blocking certain acquisitions. The United States blocked the acquisition of Qualcomm by a Singaporean firm for fear it would move a key tech industry away from the US, and closer to Beijing (Rushe, 2018). Germany also blocked the Chinese acquisition of a machine tool manufacturer noting concern over strategic foreign takeovers pursuant to the Made in China 2025 program (Delfs, 2018).

4.1.3 The Case of Huawei

- Companies like Huawei are a perfect example of the successful execution of China's various national and foreign strategies.

Companies like Huawei are a perfect example of the successful execution of China's various national and foreign strategies. Taking into account the variety and potential severity of security concerns related to 5G, the US and Australia have tightened existing policies regarding the presence of Chinese companies in networks. Huawei has not hidden its frustration at its curtailed access to foreign markets and claims a lack of publicized "intentional security vulnerabilities" (Ghosh, 2019; Huawei, 2019). It is also calling upon strategic friends to support its position. The ITU Secretary General, Houlin Zhao (originally an ICT engineer from China), departed from the ITU's position of technological neutrality to make targeted statements against the "unfair" blacklisting of Huawei—showing a disregard for the interests and experiences of the ITU's other industry, academic, and governmental members (Miles, 2019a).

However, a variety of concerns regarding Huawei's business and its equipment have been made public, and they are not new. In 2012 Australia requested that Huawei not bid on their national broadband network, effectively banning the company from the project (Chirgwin, 2012). Then in 2013, following a government review, the US banned Huawei and ZTE from participating in national 4G rollout (Muncaster, 2013). Both cited national security concerns—not an uncommon move for governments[30].

- Historically, there have been a number of reports of basic security flaws in devices and poor security management by Huawei, which seem to have been lost in the media storm, despite being the hardest evidence of cybersecurity risks inherent in choosing Huawei as a supplier.

The UK's 2019 HCSEC report which reviews current equipment in UK networks is among the most critical public statements regarding the technical quality and security of Huawei's network equipment (Huawei Cyber Security Oversight Board, 2019)[31]. The analysis highlights Huawei's lack of good security practices and capabilities, calling out "serious and systematic defects in Huawei's software engineering and cyber security competence" (Huawei Cyber Security Oversight Board, 2019, para 3.16). Australia's technical security simulation on the company's 5G equipment resulted in a ban on Huawei products in its networks (Bryan-Low, Packham, Stecklow, & Stubbs, n.d.).

The 2018 and 2019 HCSEC report and Australian simulation were not the first inklings of the company's technical shortcomings. Historically, there have been a number of reports of basic security flaws in devices and poor security management by Huawei, which seem to have been lost in the media storm, despite being the hardest evidence of cybersecurity risks inherent in choosing Huawei as a supplier (Corfield, 2019). In 5G the risk is heightened from a flaw in a home router to a more serious flaw in the

[30] For example Lenovo has had restrictions placed on it in Australia, the UK, Canada, New Zealand, and the US (Robertson, 2013). Products from Russia's Kaspersky Labs have also experienced restrictions (Schneier, 2018).

[31] The 2019 report, building on security concerns first expressed in 2018, flagged difficulties related to risk mitigation and "defects in Huawei's software engineering and cyber security processes"(Huawei Cyber Security Oversight Board, 2019, p. 4).

network itself (Corfield, 2019). Huawei's carefully-worded indictment of the US focuses on "intention", not the existence of vulnerabilities. Intention is difficult to prove, made even more difficult by millions of lines of code and moving parts (Science and Technology Committee, 2019). The US might have evidence of collusion between China and Huawei, but that evidence is classified. The upcoming court case may result in the US government revealing more information on vulnerabilities or other risks associated with Huawei, which would likely benefit the ongoing international dialogue on the topic and bring a much-needed evidence base to other countries poised to invest in 5G infrastructure. Until then, there are a variety of concerns that, if exploited, could result in serious harms to people and society.

4.2 Western Approaches

The presence of Chinese components in western Internet and telecommunications infrastructure is not new—a point the US seems to be overlooking. Unfortunately, the complexity of the issue is lost in the Twitter diplomacy and ongoing trade negotiations between the US and China. Key events in the US-China trade negotiations and the developing Huawei story intertwine as 2019 progresses (see Table 2). This reinforces the view that the US is using Huawei as a pawn in the diplomatic chess game, but revelations during the period from other countries also show real security concerns relating to the Chinese company.

Date	Event
2018[32]	Early stages of trade war: Escalating tensions between US and China, imposition of tariffs; US DoC bans companies from dealing with ZTE, later reaches deal with ZTE[33].
13/08/2018	US Congress approves the National Defense Authorization Act, banning government and its contractors from using Huawei and ZTE equipment or services[34].
23/08/2018	Australia announces Telecommunications Sector Security Reforms effectively banning Chinese companies from 5G rollout[35].
8/11/2018	UK announces Telecoms Supply Chain Review focusing on supplier and procurement aspects related to network security[36].
09/11/2018	US and China resume trade talks[37].
19/11/2018	US releases proposed export controls on emerging tech[38].
28/11/2019	New Zealand blocks operator's 5G contract with Huawei[39].
01/12/2018	Meng Wanzhou arrested in Vancouver[40].
02/12/2018	US and China agree to temporary 90-day truce[41].

[32] Events in the US China trade negotiations are colored blue. The authors acknowledge the chronology of the US China trade war produced by China Briefing (Denzan Shira & Associates) in the preparation of this table https://www.china-briefing.com/news/the-us-china-trade-war-a-timeline/.
[33] https://www.commerce.gov/news/press-releases/2018/06/secretary-ross-announces-14-billion-zte-settlement-zte-board-management.
[34] https://www.congress.gov/bill/115th-congress/house-bill/5515/text.
[35] https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers.
[36] https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference.
[37] https://www.wsj.com/articles/u-s-china-resume-talks-to-cool-trade-tensions-1542064355.
[38] https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies; https://www.washingtonpost.com/?utm_term=.cbc7faab74a0
[39] https://www.theguardian.com/business/2018/nov/28/new-zealand-blocks-huawei-5g-equipment-on-security-concerns.
[40] https://edition.cnn.com/2018/12/05/tech/huawei-cfo-arrested-canada/index.html.
[41] https://www.whitehouse.gov/briefings-statements/statement-press-secretary-regarding-presidents-working-dinner-china/.

07/12/2018	Huawei pledges $2bn on improving software quality (UK)[42].
12/12/2018	Michael Kovrig and Michael Spavor reported arrested[43].
27/12/2018	Canadian man to appear in Chinese court on drug smuggling charges[44].
28/12/2018	Sarah McIvor (Canadian teacher) released; others still detained[45].
07/01/2019	US and China engage in three-day trade talks in Beijing[46].
13/01/2019	Huawei employee arrested in Poland on espionage charges[47].
28/01/2019	US DoJ unseals charges against Meng Wanzhou[48].
30/01/2019	US and China hold two-day trade talks in Washington DC[49].
05/02/2019	Norway intelligence service issues Huawei warning[50].
06/02/2019	Huawei security issues will take five years to fix, firm tells Commons[51].
11/02/2019	US-China trade talks in Beijing[52].
20/02/2019	Huawei founder says he would defy Chinese law on intelligence gathering[53].
20/02/2019	UK cyber security chief says Huawei risk can be managed[54].
21/02/2019	US and China hold trade talks in Washington; Trump extends tariff deadline[55].
22/02/2019	US government threatens to end intelligence-sharing with allies that buy Huawei[56].
07/03/2019	Huawei sues US government over product ban[57].
12/03/2019	US tells Germany to drop Huawei or it will intelligence sharing[58].
25/03/2019	Italy extends "special powers" over 5G noting national security[59].
26/03/2019	European Commission recommends common EU approach to 5G security, stating countries have the "right to exclude companies from their markets for national security reasons"[60].
28/03/2019	UK HCSEC report published[61].
28/03/2019	US and China hold trade talks in Beijing[62].
03/04/2019	US and China hold trade talks in Washington[63].

[42] https://www.theguardian.com/technology/2018/dec/07/huawei-pledges-2bn-in-effort-to-allay-uk-security-concerns.
[43] https://www.theguardian.com/world/2018/dec/11/michael-kovrig-detained-china-former-canadian-diplomat.
[44] https://www.theguardian.com/world/2018/dec/27/china-canada-man-drugs-trial-huawei-tensions.
[45] https://www.theguardian.com/world/2018/dec/29/china-releases-canadian-teacher-but-others-still-held-in-huawei-row.
[46] https://ustr.gov/about-us/policy-offices/press-office/press-releases/2019/january/statement-united-states-trade.
[47] https://www.bloomberg.com/news/articles/2019-01-13/huawei-s-poland-crisis-threatens-to-intensify-spying-concerns.
[48] https://www.nytimes.com/2019/01/28/us/politics/meng-wanzhou-huawei-iran.html.
[49] https://www.nytimes.com/2019/01/31/business/trump-china-trade-tariffs.html.
[50] https://www.rappler.com/technology/news/222721-norway-intelligence-service-issues-huawei-warning-february-2019.
[51] https://www.theguardian.com/technology/2019/feb/06/huawei-security-issues-will-take-five-years-to-fix-firm-tells-commons.
[52] http://www.globaltimes.cn/content/1138995.shtml.
[53] https://www.cbsnews.com/news/huawei-president-ren-zhengfei-says-he-would-defy-chinese-law-on-intelligence-gathering/.
[54] https://www.ft.com/content/4c2b6fa0-350d-11e9-bd3a-8b2a211d90d5.
[55] https://www.nytimes.com/2019/02/24/us/politics/us-china-trade-truce.html.
[56] https://www.wired.co.uk/article/wired-awake-220219.
[57] https://www.bbc.co.uk/news/business-47478587.
[58] https://www.wsj.com/articles/drop-huawei-or-see-intelligence-sharing-pared-back-u-s-tells-germany-11552314827.
[59] https://www.lexology.com/library/detail.aspx?g=ef072174-4897-4f52-8506-64fac69187ff.
[60] http://europa.eu/rapid/press-release_IP-19-1832_en.htm.
[61] https://www.bbc.co.uk/news/technology-47830056.
[62] https://www.scmp.com/news/china/diplomacy/article/3003787/pleasure-see-you-again-much-work-do-us-china-trade-talks.
[63] https://www.scmp.com/news/china/diplomacy/article/3003787/pleasure-see-you-again-much-work-do-us-china-trade-talks.

08/04/2019	Huawei wi-fi modules were pulled from Pakistan CCTV system[64].
15/04/2019	Dutch government sets up a task force to review security risks in 5G[65].
24/04/2019	Five Eyes will not use Huawei in sensitive networks: senior US official[66].
26/04/2019	Huawei row: top civil servant demands leak inquiry cooperation[67].
30/04/2019	US and China hold trade talks in Beijing[68].
03/05/2019	Czech Republic holds a meeting with like-minded EU and NATO nations on 5G security best practices[69].
10/05/2019	US increases tariff on $200bn of Chinese goods to 25%[70].
13/05/2019	China increases tariffs on $60bn of US goods[71].
16/05/2019	Trump Executive Order declares national emergency over IT threats; enters Huawei on Entity List[72].
20/05/2019	Huawei's use of Android restricted by Google[73].
22/05/2019	ARM cuts ties with Huawei, threatening future chip designs[74].
22/05/2019	US DoC creates 90-day temporary general license, delaying impact of Executive Order[75].
23/05/2019	Markets slide as Panasonic joins list of firms walking away from Huawei[76].
28/05/2019	Huawei seeks summary judgment in case against US[77].
01/06/2019	IEEE temporarily bars Huawei from reviewing papers[78].
04/06/2019	Britain has not made a decision on Huawei in 5G: security minister[79].
04 & 05/06/2019	Chinese government convened US, UK, and South Korean tech companies to warn against complying with the US Entity List[80].
10/06/2019	Huawei denies links to Chinese government[81].
15/06/2019	China halts market economy dispute at WTO after series of unfavorable decisions[82].
01/07/2019	Dutch task force concludes, ensuring "extra high standards" for 5G equipment suppliers[83].

[64] https://www.bbc.co.uk/news/technology-47856098.
[65] https://www.reuters.com/article/us-huawei-europe-netherlands/the-netherlands-forms-task-force-to-assess-5g-security-risks-idUSKCN1RR0RU.
[66] https://www.reuters.com/article/us-britain-huawei-ncsc-usa/five-eyes-will-not-use-huawei-in-sensitive-networks-senior-u-s-official-idUSKCN1S01CZ.
[67] https://www.bbc.co.uk/news/uk-politics-48061793.
[68] https://www.cbc.ca/news/business/u-s-china-productive-trade-talks-beijing-1.5118278.
[69] https://www.reuters.com/article/us-telecoms-5g-security/western-allies-agree-5g-security-guidelines-warn-of-outside-influence-idUSKCN1S91D2.
[70] https://csms.cbp.gov/viewmssg.asp?Recid=24227&page=&srch_argv=301&srchtype=&btype=&sortby=&sby=.
[71]https://www.uschina.org/sites/default/files/tariff_commission_notice_2019_no._2.pdf?utm_campaign=Marketing_Cloud&utm_medium=email&utm_source=Standalone+-+China+announces+tariff+retaliation+and+exclusion+process+-+May+13&%20utm_content=https%3a%2f%2fwww.uschina.org%2fsites%2fdefault%2ffiles%2ftariff_commission_notice_2019_no._2.pdf.
[72] https://www.bbc.co.uk/news/world-us-canada-48289550.
[73] https://www.bbc.co.uk/news/world-us-canada-48289550.
[74] https://www.theverge.com/2019/5/22/18635326/huawei-arm-chip-designs-business-suspension.
[75] https://www.federalregister.gov/documents/2019/05/22/2019-10829/temporary-general-license.
[76] https://www.theguardian.com/technology/2019/may/23/huawei-markets-slide-as-panasonic-joins-list-of-firms-cut-ties.
[77] https://www.cnbc.com/2019/05/29/huawei-files-motion-for-summary-judgement-in-lawsuit-against-us.html.
[78] https://www.engadget.com/2019/06/01/ieee-bans-huawei-from-reviewing-papers/?guccounter=1&guce_referrer=aHR0cHM6Ly9kdWNrZHVja2dvLmNvbS8&guce_referrer_sig=AQAAACM3sxpzjP-L2aaHUzFZBZsqWaMam8DDoXHkfSYPh2wadsa5EpL5NY-3mOFiPf74sXhX0k8WNh47q5wBhLgXHxr-_Jz-sExguYAydqzZCRRAqb-gxm1mo1XCbycRGP8Q6AuBqGXH-RPEbHyMx8ySEyvZcbII48MymuMpeWGh3_QU.
[79] https://uk.reuters.com/article/uk-huawei-tech-usa-britain/britain-has-not-made-a-decision-on-huawei-in-5g-security-minister-idUKKCN1T50ON.
[80] https://www.nytimes.com/2019/06/08/business/economy/china-huawei-trump.html.
[81] https://www.bbc.co.uk/news/business-48588661.
[82] https://www.reuters.com/article/us-usa-china-wto-eu/china-pulls-wto-suit-over-claim-to-be-a-market-economy-idUSKCN1TI10A.
[83] https://uk.reuters.com/article/us-netherlands-telecoms/no-huawei-ban-in-dutch-5g-rollout-government-idUKKCN1TW2V8.

03/07/2019	French task force proposes a bill with increased government oversight of 5G network rollout including "defense and national security parameters"[84].

Table 2 - Chronology of US-China trade talks and Huawei events 2018-2019

Amid the sound and fury of US rhetoric, hard evidence and technical reports like those by the UK and Australia have been overshadowed in the media. The US has also failed both to recognize the different environments in which other countries must operate and to create an inclusive dialogue on the issues.

There is vocal concern from some governments *vis-à-vis* risks of further embedding Chinese firms into critical national infrastructures. Governments must weigh up the costs and benefits of their positions. Geopolitics, trade relationships and diplomatic ties play a role in positions, as does the potential damage to public services and the economy of a significantly delayed national 5G rollout. Governments must also consider the risks of being drawn into China's Internet policies promoting government control, human rights infringement, anti-competitive behavior, and the threat of helping to create a vertically integrated Chinese 5G monopoly.

Emerging positions reflect assessment of the *extent* to which Chinese providers such as Huawei might be incorporated in 5G rollout in order to benefit from early adoption. This includes drawing lines between edge equipment and the core network's hardware and software. Nations may not need or want to take the US's strong-armed approach, emphasizing the need for a clear story on 5G security matters. Conflating too many tangential issues specific to the US-China context—such as corporate espionage and sanctions violations—without clear positioning within the wider landscape risks diluting essential dialogue around national security and other issues such as net neutrality and human rights which are relevant the world over.

- Emerging positions reflect assessment of the extent to which Chinese providers such as Huawei might be incorporated in 5G rollout in order to benefit from early adoption. This includes drawing lines between edge equipment and the core network's hardware and software.

In response to China's strategic moves, western countries are displaying a wariness towards Chinese firms. Table 3 provides an overview of the reported positions and actions taken by some western countries with regard to Chinese technology companies[85]. A common approach by governments is to undertake a technology review, with simulations and an evaluation of supply chain risks. Some countries are considering or have implemented protectionist policies, reminiscent of those already established in China, albeit lighter touch (e.g. equipment testing and contracting requirements), sometimes under the pretext of national security.

[84] https://uk.reuters.com/article/us-france-telecoms-5g/french-parliament-taskforce-agrees-on-controls-for-5g-roll-out-idUKKCN1TY2QG.
[85] Information as of June 2019. Some non-western countries are taking action to restrict Chinese companies' access to 5G markets. For example, Japan has blocked Chinese equipment, Taiwan renewed an existing ban on Huawei and ZTE equipment (Morris, 2018), and Israel has legal restrictions on Chinese equipment (Triolo & Allison, 2018).

Country	Ongoing review(s)	Completed review	Announced/ official position	Policy/ procurement changes	Warning on Chinese firm(s)	Ban on Chinese firm(s)	No action
US		X	X			X	
Canada	X						
Australia		X	X			X	
New Zealand	X					(Blocked Huawei contract)	
France	X			Likely	X		
UK	X			Likely	X		
Italy	X			X			
Germany		X	X				X
Norway		X		X			
Netherlands		X		Likely			
Czech Republic	X				X		
Poland	X						
Belgium		X					X
EU			X			(national decision[86])	
NATO	X						

Table 3 - National inquiries into network security and Huawei

The national responses reveal a range of soft and hard power strategies. Cautious steps call for official multilateral positions (e.g. Poland's call for an EU-NATO position (Reuters, 2019)) or internal security reviews (e.g. Canada). At the time of writing, Germany and Belgium are the only countries not to proactively restrict Chinese companies' access to national 5G deployment, following a security review.

The hardline responses to date are blanket bans at national (Australia) and/or targeted corporate (US) levels—an unsurprising outcome from countries that since the early 2010s have publicly voiced concerns about Chinese telecoms companies' involvement in national networks (Lu-YueYang, 2012; Rogers & Ruppersberger, 2012). The US's tough policies are paired with bilateral diplomacy approaches, aimed at engendering a global shift in national 5G strategies to exclude Chinese firms (Johnson, 2019; Table 2).

- Although the Entity List is an American policy, it, like Chinese policies, has extraterritorial impact and is also likely to damage the US's relationship with foreign governments and industry.

However, failure of the US's closest allies to rally to their cause threatens to destabilize long-standing alliances such as the Five Eyes. First, the US threatened to reduce intelligence sharing with allies who allowed Huawei into local networks (see Table 2). Then, Huawei was added to a US Entity List, barring companies around the world from trading with or supplying American-origin goods or services to Huawei.

[86] The European Union has not issued a ban on Chinese firms, but instead left the decision to governments. Reports highlight that some security officials feel the broad range of risks "posed by Chinese technology in general" are not addressed by the banning of a single supplier (Bryan-Low, Packham, Lague, Stecklow, & Stubbs, 2019).

This blunt tool had huge ripple effects outside of the 5G arena and American borders. Google quickly revoked Huawei's access to licensed material including software updates; the UK's ARM and Japan's Panasonic halted trade or initiated reviews of their relationship with the Chinese company; and the Institute of Electrical and Electronic Standards (IEEE), an SDO, placed a temporary hold on Huawei's participation in standards reviews to assess compliance with the US's Entity List (see Table 2). Although the Entity List is an American policy it, like Chinese policies, has extraterritorial impact. Unfortunately, and also in parallel with China, this is likely to damage the US's relationship with foreign governments and industry.

Evidence-based, moderate policy approaches aimed at procurement and contracting processes are emerging, namely in Norway, the UK, and Italy[87]. These approaches are relatable and attainable for most governments and could develop a best practice approach for others to follow. This could also lead to a re-alignment of like-minded nations working together to address a collective resource issue—cyberthreats in an increasingly connected world.

- This could also lead to a re-alignment of like-minded nations working together to address a collective resource issue – cyberthreats in an increasingly connected world.

4.2.1 Markets and Trade Relations

It is not surprising that each country has taken a slightly different approach to the threat of a China-dominated 5G market. Ongoing diplomatic and trade relations between countries play a key role. For instance, in addition to the tensions caused by detentions of Canadian citizens and Meng Wanzhou, a 2012 Canada-China agreement[88] allows Huawei to bring claims against the Canadian government in response to restrictive regulatory action (McGregor & February 17, 2019). In the meantime, as Canada executes its security review, China has blocked key Canadian exports such as canola oil and pork (Blatchford, 2019; Patton & Nickel, 2019). In other parts of the world, disruption to travel and ongoing trade negotiations between New Zealand and China have been linked to the banning of Huawei from a local operator's 5G rollout (Withers, 2019). Italy was the first of the G7 to sign a Belt and Road deal with China, yet telecoms was reportedly purposefully left out of the deal (Fonte & Piscioneri, 2019).

Procurement, contracting and policy approaches such as those being put forward by the UK, Italy and Norway offer important flexibility for governments in treading around such politicized and complex issues by setting minimum, universally applicable requirements. First, they may reduce some vendors' access to contract competitions through legitimate and transparent means. Secondly, security becomes a primary purchasing point—something that was not done for previous networks (Intelligence and Security Committee et al., 2013). And third, such approaches can provide a way forward for governments who wish to have a degree of control over which technology is used in 5G networks, but which may not be able to enact a ban for political or practical reasons. Such an approach could fairly and efficiently deliver the quiet exclusion of Chinese firms like Huawei, at least from critical parts of a network.

- Procurement, contracting and policy approaches could fairly and efficiently deliver the quiet exclusion of Chinese firms like Huawei, at least from critical parts of a network.

The UK's National Cyber Security Centre (NCSC) has published advice on adopting good cybersecurity practices. For example, NCSC has called for the use of vendors with a track record of minimizing vulnerabilities, impact, and harm (Levy, 2019). One

[87] Norway implemented changes to its laws and regulations, including the Security Act and sectoral laws, to give heavier weight to security assessments (Wijnen, 2019). Similarly, the UK initiated a Telecoms Supply Chain Review (due spring 2019) looking at market incentives and security risks (Department for Digital, Culture, Media & Sport, 2018), while Italy's government passed a law listing 5G network technology among the nation's "Strategic Assets for national security", requiring notification of intent to use foreign telecoms equipment and includes veto power (Giarda, Lattanzio, & Liotta, n.d.).

[88] Agreement for the Promotion and Reciprocal Protection of Investments.

way for industry to operationalize this advice is to work with vendors which follow best practice in security by design, have good transparency practices and vulnerability reporting initiatives, such as Microsoft's Government Security Program (Microsoft, 2003). To further address concerns, the UK is also stressing the need to manage risk and increase vendor diversity in the ecosystem in order to prevent a single point of failure (Donaldson, 2018; Levy, 2019). Governments and operators adopting such an approach will take into consideration the extent to which Chinese equipment providers are already integrated into local infrastructure (Morris, 2018).

Reducing Huawei's 5G network presence will be more difficult for small community network operators or countries with less capital to invest. Western companies (e.g. Qualcomm, Nokia, Ericsson) should consider how to make their 5G technology accessible and affordable in developing markets, for example, through joint ventures to deliver a more competitively priced product. Additionally, governments could help subsidize rollout, offer tax relief, or loosen policies on network deployment in order to increase purchasing power and make a wider range of 5G technology providers accessible to a greater number of market actors. Combined, these actions could help to re-balance the developing asymmetric and complex global 5G marketplace.

5 Conclusion

5G will transform current business models and financial flows around Internet infrastructure and network provision. This transformation engenders concerns over security and surveillance, intellectual property rights, net neutrality, and Internet censorship. There is a shifting landscape of threats and risks related to mobile communications, such as the growing complexity and size of a network's attack surface and the potential for a single incident to result in physical damage—all of which impact 5G's ability to support critical infrastructure. The interconnected and global nature of the Internet means that it could become the next tragedy of the commons if not governed appropriately. A likely fracture point is at the system and services layer which will re-concentrate power into the hands of the infrastructure providers. As such, there should be a wider discussion of the threats and benefits of 5G that go outside bilateral trade negotiations and economic power struggles.

- China is hoping that first mover advantage will result in an indigenous global monopoly that shapes the next generation of Internet technologies, business models, and our daily lives – much the way American tech companies have shaped the current Internet.

In the first half of 2019 there was a flurry of governmental statements, actions, and finger-pointing as China and the US brought the 5G race up to the brink of an all-out techno cold war. East and West seem to be adopting earlier moves from each other's playbooks—not many would have foreseen China levelling five complaints in a year at the US[89] and threatening Australia via the WTO a few years ago (Miles, 2019b; World Trade Organization, n.d.). China is hoping that first-mover advantage will result in an indigenous global monopoly that shapes the next generation of Internet technologies, business models, and our daily lives—much the way American tech companies have shaped the current Internet. The US is using opaque claims of national security, reminiscent of a Chinese approach, to advance its protectionist position. Other western nations are implementing protectionist policies that impede China's access to local markets, yet these approaches better reflect cyber security best practices and buoy an admittedly small, but strategically important, marketplace. Ironically, the fall-out from the Trump Executive Order is likely to motivate Chinese tech companies to create an entirely indigenous supply-chain,

[89] Up from an average of about one per year from 2002 to 2016.

further impacting global supply chains. Differences in the US and Chinese approaches come down to perceptions of openness, transparency, quality, and the degree of separation between public and private entities, including legal and national security frameworks.

How we resolve geopolitical tensions regarding 5G will impact the future of cyber security and national economies. Companies play a "fundamental role in shaping" technology as well as the norms and rules of the Internet (Hurel & Lobato, 2018, p. 66). As a result, the state-firm diplomacy that has evolved over the past three decades is now taking center stage in geopolitics as the US government and Huawei go head to head (Strange, 1992). An example of effective state-firm diplomacy is the UK's Huawei Cyber Security Evaluation Centre, paid for by Huawei and overseen by the NCSC. Although not without its critics, the mutual benefit of such a solution (e.g. market access and oversight of critical infrastructure) speaks to the ability of actors to find common ground on specific aspects of contested issues (Katwala, 2019). Good practices such the HCSEC can be replicated elsewhere and evolve with technology. The benefit of centers like HCSEC goes beyond finding vulnerabilities to building assurance and understanding of a system (Science and Technology Committee, 2019). However, the limitations of such a testing and review center should be acknowledged.

At the national level, hard-line responses such as naming and shaming, the addition of tariffs, or other trade-related actions that potentially breach international norms such as WTO trade rules, risk stifling innovation and the opportunities offered by 5G. A likely outcome of the national and regional inquiries currently being undertaken (Table 3) is stricter requirements on procurements and contracting that adhere to the WTO's most favored nation principle and national security exemptions, and which support recommended norms (Global Commission on Internet Governance, 2016; World Trade Organization, n.d.-b). Policy updates could include requirements for compliance with principles such as security-by-design (Day, 2018), the ability to provide evidence on risk mitigation techniques, vulnerability disclosure and transparency reports (Global Forum on Cyber Expertise, 2018; IoT Security Foundation, 2017), or the use of conformance, testing or certification requirements for market entry (Johnson et al., 2019).

- Japan, Israel, Taiwan, the UK, Canada, Norway, Czech Republic, New Zealand and others have voiced similar concerns, but these voices have been lost in the media noise.

Governments can also form new strategic partnerships to promote a more moderate, evidence-based policy dialogue around 5G, promote best practices in cyber security, and increase overall awareness of the national security and other concerns (e.g. human rights) encapsulated in 5G. Japan, Israel, Taiwan, the UK, Canada, Norway, the Czech Republic, New Zealand and others have voiced similar concerns, but these voices have been lost in the media noise. These countries could work together to deliver a broadly accessible line of reasoning that is reflective of the varied risks associated with companies like Huawei. It may also result in new international alliances for the 5G era. The May 2019 summit in the Czech Republic is a good first step in this direction (see Table 2), but measured and practical actions like this lack the Twitter-friendly media frenzy of US-China relations.

- In essence, the public conversation needs to change – moving away from bilateral trade wars towards arguments which are relatable to governments and people the world over.

In essence, the public conversation needs to change—moving away from bilateral trade wars towards arguments which are relatable to governments and people the world over. This includes the increased ability for targeted communications interception or network shutdowns, the collective commons issue of cyber security, the need to adopt best practices, and improving network resilience through principles such as supplier diversity, discouraging the adoption of sub-standard practices, and raising awareness about the policy context in which Chinese companies operate. A more constructive approach should also address the

"elephant in the room" of market protectionism by the West and market manipulation by Chinese firms. However, possibly the most hard-hitting approach would be the de-classification of information regarding additional security threats that have until now been discussed behind closed doors.

Norms development in this space will necessarily be an iterative process due to the ongoing evolution of technology and risk management, but not least the sensitivity of the topic to national security. Finding solutions to these issues does not necessarily need to be state-led. Stakeholders should also redouble efforts across relevant standards bodies and expert groups, particularly those that are multistakeholder, open and transparent such as the IETF, ETSI, and industry forums such as GSMA and the Global Networking Initiative.

The UN is making a concerted effort to find its place in Internet governance, and 5G is no exception. In Internet governance, this would place the open, multistakeholder approach at risk and does not engage the large body of actors that are key to the internet. The recent UN High Level Panel on Digital Cooperation (HLPDC) focused heavily on a UN flavor of coordinated cooperation (United Nations, 2019). With the upcoming UN Group of Government Experts (GGE) and Open-ended Working Group (OEWG) there will be even more governments involved in processes at the UN level. However, these groups, and most likely initiatives to arise from the HLDC, remain government-led and closed in terms of participation and agreed outputs. The arenas in which China is pushing its 5G standards, such as the ITU, lack the remit and expertise to work on human rights issues such as privacy. Yet recent high-level conferences show the drive by some nations to dangerously expand the ITU's remit to work on legally and culturally sensitive issues, embedding particular approaches to these topics into technology, away from public oversight (Article 19, 2017). Centralizing efforts in a closed, intergovernmental environment under increasing influence by those that do not share western approaches to Internet governance does not bode well for western values or vision of the Internet. It minimizes the role of, and to an extent excludes, industry and technologists who innovate, build and run technologies and services that underpin daily lives. Academia and civil society provide important sources of research, information sharing and watchdog roles which are curtailed in closed, intergovernmental forums. Their participation is reliant on the benevolence, and perspective, of those governments shaping the discussion.

Both governments and users should be wary of a Chinese 5G Internet. Countries like China that champion government control of the Internet, information, data and users will not relinquish that control with future technologies. The realist in this situation would expect Chinese-origin technology to instead design and develop new technologies to better fit China's needs and end-goals. A technology's home environment including legal and policy landscape also enables particular behaviors. Heretofore, public disagreements between tech giants and governments have often focused on access to user accounts and devices, as seen between the US government and Apple in 2016 (Khamooshi, 2016). However, with 5G the use of national law like China's National Intelligence Law could grant the government access to an entire cloud service running a network—and all the data on that network, not just a user's device.

- Each country will need to navigate different waters including diplomatic relationships, market interest, existing equipment in and resiliency of their networks, and short and long-term benefits of 5G rollout.

The US is one of—if not the—strongest powers when it comes to utilizing tools enabled by the Internet. However, the US perceives the possibility of China taking first-mover advantage in 5G as a means to further shift power to the East, solidify its leadership in emerging technologies, and abuse that power. China is a complex business, trading, and diplomatic partner with opaque private-public relationships,

a history of exploiting the Internet's architecture for political and economic gain, a concerning track record of market manipulation and a fundamentally different approach to Internet governance and human rights. To some extent, the race comes down to a question of whom governments prefer to be rooted in their critical infrastructure. Separating parties into camps will include an element of subjectivity. Each country will need to navigate different waters including diplomatic relationships, market interest, existing equipment in and resiliency of their networks, and short and long-term benefits of 5G rollout.

6 Bibliography

Abbate, J. (1999). *Inventing the Internet*. Cambridge: MIT Press.

Article 19. (2017, October 16). Privacy: Yes! But not at the ITU. Retrieved June 12, 2019, from ARTICLE 19 website: https://www.article19.org/resources/privacy-yes-but-not-at-the-itu/

Barwise, P., Featured, 2018, Truth, Trust, & Comments, T. C. (2018, June 14). Why Tech Markets Are Winner-Take-All. Retrieved March 20, 2019, from Media Policy Project website: https://blogs.lse.ac.uk/mediapolicyproject/2018/06/14/why-tech-markets-are-winner-take-all/

Best of Today - Today: The View From Washington - BBC Sounds. (2019, January 31). Retrieved January 31, 2019, from https://www.bbc.co.uk/sounds/play/p06zkjpt

Blatchford, A. (2019, May 30). The Bank of Canada is very worried about the U.S.-China trade war getting worse, Wilkins says | Financial Post. Retrieved June 27, 2019, from Financial Post website: https://business.financialpost.com/news/economy/trade-war-escalation-major-preoccupation-for-bank-of-canada-top-official

Bradshaw, S., & DeNardis, L. (2018). The politicization of the Internet's Domain Name System: Implications for Internet security, universality, and freedom. *New Media & Society*, *20*(1), 332–350.

Bryan-Low, C., Packham, C., Lague, D., Stecklow, S., & Stubbs, J. (2019, May 21). Special Report: Hobbling Huawei - Inside the U.S. war on China's... *Reuters*. Retrieved from https://ca.reuters.com/article/technologyNews/idINKCN1SR1EV

Bryan-Low, C., Packham, C., Stecklow, S., & Stubbs, J. (n.d.). Hobbling Huawei: Inside the U.S. war on China's tech giant. Retrieved June 27, 2019, from Reuters website: https://www.reuters.com/investigates/special-report/huawei-usa-campaign/

Byler, D. (2019, April 11). China's hi-tech war on its Muslim minority. *The Guardian*. Retrieved from https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition

Cerulus, L. (2017, December 11). China's ghost in Europe's telecom machine. Retrieved March 5, 2019, from POLITICO website: https://www.politico.eu/article/huawei-china-ghost-in-europe-telecom-machine/

Cheung, T. M. (2018). The rise of China as a cybersecurity industrial power: balacning national security, geoppolitical, and development priorities. *Journal of Cyber Policy*, *3*(3). https://doi.org/10.1080/23738871.2018.1557234

Chirgwin, R. (2012, March 25). Huawei banned from Australia's NBN: reports. Retrieved June 27, 2019, from https://www.theregister.co.uk/2012/03/25/huawei_nbn_ban/

Corfield, G. (2019, March 28). Huawei's half-arsed router patching left kit open to botnets: Chinese giant was warned years ago – then bungled it. Retrieved May 7, 2019, from https://www.theregister.co.uk/2019/03/28/huawei_mirai_router_vulnerability/

Crawford, S. (2018). *Fiber*. Yale University Press.

Day, J. (2018). *IoTSF Secure Design Best Practice Guide*. 17.

Delfs, A. (2018, August 1). *Germany Toughens Stance and Blocks China Deal*. Retrieved from https://www.bloomberg.com/news/articles/2018-08-01/germany-said-to-block-company-purchase-by-chinese-for-first-time

Department for Digital, Culture, Media & Sport. (2018, November 8). Telecoms Supply Chain Review Terms of Reference. Retrieved March 11, 2019, from GOV.UK website: https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference

Donaldson, K. (2018, December 3). *Spy Boss Says U.K. Must Decide If Huawei Suitable for 5G Network*. Retrieved from https://www.bloomberg.com/news/articles/2018-12-03/spy-boss-says-u-k-must-decide-if-huawei-suitable-for-5g-network

FCC Proposes to Protect National Security Through FCC Programs. (2018, April 18). Retrieved March 20, 2019, from Federal Communications Commission website: https://www.fcc.gov/document/fcc-proposes-protect-national-security-through-fcc-programs-0

Fidler, M. (2018, March 7). African Union Bugged by China: Cyber Espionage as Evidence of Strategic Shifts. Retrieved March 6, 2019, from Council on Foreign Relations website: https://www.cfr.org/blog/african-union-bugged-china-cyber-espionage-evidence-strategic-shifts

Fonte, G., & Piscioneri, F. (2019, March 20). Italy to extend golden share powers to 5G technologies: League party. *Reuters*. Retrieved from https://uk.reuters.com/article/us-china-italy-5g-idUKKCN1R10X8

Forrell, J., & Solaner, G. (1986). *Competition, Compatability and Standards: The Economics of Horses, Penguins and Lemmings*. UC Berkeley.

Freedom House. (2018). *Freedom on the Net 2018*. Retrieved from https://freedomhouse.org/report/freedom-net/freedom-net-2018

Future Thinking: Alissa Cooper on the Technical Impact of Internet Consolidation. (2019, February 12). Retrieved February 13, 2019, from Internet Society website: https://www.internetsociety.org/blog/2019/02/future-thinking-alissa-cooper-technical-impact-internet-consolidation/

Geoeconomics: the Chinese Strategy of Technological Advancement and Cybersecurity. (2018a, December 3). Retrieved March 20, 2019, from Lawfare website: https://www.lawfareblog.com/geoeconomics-chinese-strategy-technological-advancement-and-cybersecurity

Geoeconomics: the U.S. Strategy of Technological Protection and Economic Security. (2018b, December 11). Retrieved March 20, 2019, from Lawfare website: https://www.lawfareblog.com/geoeconomics-us-strategy-technological-protection-and-economic-security

Ghosh, S. (2019, February 26). Huawei says US has “no evidence, nothing” of Chinese spying - Business Insider. Retrieved March 21, 2019, from https://www.businessinsider.com/huawei-says-us-has-no-evidence-nothing-of-chinese-spying-2019-2?r=US&IR=T

Giarda, B. M.-R., Lattanzio, A., & Liotta, J. (n.d.). Italy tightens foreign investment scrutiny over 5G technology | Lexology.

Retrieved June 27, 2019, from Lexology website: https://www.lexology.com/library/detail.aspx?g=ef072174-4897-4f52-8506-64fac69187ff

Global Commission on Internet Governance. (2016, June 21). One Internet | Centre for International Governance Innovation. Retrieved March 29, 2019, from https://www.cigionline.org/publications/one-internet

Global Forum on Cyber Expertise. (2018, September 10). The Cybersecurity Tech Accord supports the GFCE's call for industry-wide adoption of transparent policies for coordinated vulnerability disclosure (CVD). Retrieved March 21, 2019, from Cybersecurity Tech Accord website: https://cybertechaccord.org/supports-gfce-call-for-cvd/

Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet? Illusions of a Boarderless World*. Oxford: Oxford University Press.

Hancock, S. (2019). *Panorama - Can We Trust Huawei?* Retrieved from https://www.bbc.co.uk/iplayer/episode/m0004cgm/panorama-can-we-trust-huawei

Hemmings, J. (2018, December 7). To Ban or to Banbury? Retrieved March 6, 2019, from RUSI website: https://rusi.org/commentary/ban-or-banbury

Hersey, F. (2018, May 16). Lenovo founder in public backlash for 'unpatriotic 5G standards vote' · TechNode. Retrieved June 27, 2019, from TechNode website: https://technode.com/2018/05/16/lenovo-huawei-5g/

Hoffman, S., & Kania, E. (2018, September 13). Huawei and the ambiguity of China's intelligence and counter-espionage laws. Retrieved March 12, 2019, from The Strategist website: https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/

Huawei. (2018, April 12). Huawei First to Complete IMT-2020 (5G) Promotion Group's Core Network Test for 5G Non-Standalone - Huawei Press Center. Retrieved June 27, 2019, from Huawei website: https://www.huawei.com/en/press-events/news/2018/4/IMT-2020-5G-Group-Core-Network-Test

Huawei. *Huawei Technologies USA, Inc. et al v. United States of America, et al :* , (2019).

Huawei Cyber Security Oversight Board. (2019, March 28). Huawei cyber security evaluation centre oversight board: annual report 2019. Retrieved March 29, 2019, from GOV.UK website: https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019

Huawei is at the centre of political controversy. (2019, April 27). *The Economist*. Retrieved from https://www.economist.com/briefing/2019/04/27/huawei-is-at-the-centre-of-political-controversy

Hurel, L. M., & Lobato, L. C. (2018). Unpacking cyber norms: private companies as norm entrepreneurs. *Journal of Cyber Policy*, *3*(1), 61–76. https://doi.org/10.1080/23738871.2018.1467942

Hurley, J. (2018, March). *Examining the Debt Implications of the Belt and Road Initiative from a Policy Perspective*. 39. Retrieved from https://www.cgdev.org/sites/default/files/examining-debt-implications-belt-and-road-initiative-policy-perspective.pdf

Intelligence and Security Committee, Intelligence and Security Committee, Great Britain, & Parliament. (2013). *Foreign involvement in the critical national infrastructure: the implications for national security*. London: Stationery Office.

IoT Security Foundation. (2017, December). Vulnerability Disclosure Best Practice Guidelines. Retrieved July 3, 2019, from https://www.iotsecurityfoundation.org/best-practice-guidelines/

Johnson, C., February 6, & Headquarters, 2019 1:00 pm-2:30 pmCSIS. (2019). *Mitigating Security Risks to Emerging 5G Networks*. Retrieved from https://www.csis.org/events/mitigating-security-risks-emerging-5g-networks

Katwala, A. (2019, February 22). Here's how GCHQ scours Huawei hardware for malicious code. *Wired UK*. Retrieved from https://www.wired.co.uk/article/huawei-gchq-security-evaluation-uk

Kennedy, S. (2017). *The Fat Tech Dragon: Benchmarking China's Innovation Drive*. 52.

Khamooshi, A. (2016, March 3). Breaking Down Apple's iPhone Fight With the U.S. Government. *The New York Times*. Retrieved from https://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html, https://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html

Lam, L., & Chen, S. (2013, June 22). EXCLUSIVE: Snowden reveals more US cyberspying details. Retrieved March 14, 2019, from South China Morning Post website: https://www.scmp.com/news/hong-kong/article/1266777/exclusive-snowden-safe-hong-kong-more-us-cyberspying-details-revealed

Lazanski, D. (forthcoming). Governance in International Technical Standards Making: A Tripartite Model. *Journal of Cyber Policy*.

Lazanski, D. (2019, April 27). China, Huawei and 5G Standards in the UK. Retrieved June 27, 2019, from https://www.forbes.com/sites/dominiquelazanski/2019/04/27/china-huawei-and-5g-standards-in-the-uk/#208c57f82fbd

Lecher, C. (2019, March 11). US tells Germany to stop using Huawei equipment or lose some intelligence access. Retrieved March 12, 2019, from The Verge website: https://www.theverge.com/2019/3/11/18260344/us-germany-huawei-5g-letter-security

Lessig, L. (2006). *Code: And Other Laws of Cyberspace, Version 2.0* (2nd Revised ed.). New York, NY: Basic Books.

Levy, I. (2019, February 22). Security, complexity and Huawei; protecting the UK's telecoms networks - NCSC Site. Retrieved March 4, 2019, from https://www.ncsc.gov.uk/blog-post/security-complexity-and-huawei-protecting-uks-telecoms-networks

Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure. *Policy & Internet*, *10*(4), 415–453.

Lin, H. (2019, April 3). Huawei and Managing 5G Risk. Retrieved April 4, 2019, from Lawfare website: https://www.lawfareblog.com/huawei-and-managing-5g-risk

Lu-YueYang, M. (2012, March 26). Australia blocks China's Huawei from broadband tender. *Reuters*. Retrieved from https://www.reuters.com/article/us-australia-huawei-nbn-idUSBRE82P0GA20120326

Manuel, A. (2017, October 17). China Is Quietly Reshaping the World. Retrieved March 19, 2019, from The Atlantic website: https://www.theatlantic.com/international/archive/2017/10/china-belt-and-road/542667/

Marks, J. (2019, February 7). Analysis | The Cybersecurity 202: Huawei's access to 5G could expand China's surveillance state, cyber diplomat warns. Retrieved March 4, 2019, from Washington Post website: https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/02/07/the-cybersecurity-202-huawei-s-access-to-5g-could-expand-china-s-surveillance-state-cyber-diplomat-warns/5c5b26fc1b326b66eb09863b/

Mavrakis, D. (2018, December 3). OPINION: Is Europe's 5G spectrum strategy falling behind? Retrieved April 2, 2019, from https://www.mobileeurope.co.uk/press-wire/opinion-is-europe-s-5g-spectrum-strategy-falling-behind

McBride, J., & Chatzky, A. (2019, March 7). Is 'Made in China 2025' a Threat to Global Trade? Retrieved March 19, 2019, from Council on Foreign Relations website: https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade

McGregor, J., & February 17, 2019 4:00 AM ET | Last Updated: (2019, February 17). As if Canada's Huawei decision isn't tricky enough: a 5G ban risks a lawsuit | CBC News. Retrieved March 14, 2019, from CBC website: https://www.cbc.ca/news/politics/huawei-canada-china-fipa-1.5021033

Microsoft. (2003, January 14). Microsoft Announces Government Security Program. Retrieved March 23, 2019, from Stories website: https://news.microsoft.com/2003/01/14/microsoft-announces-government-security-program/

Miles, T. (2019a, April 5). Huawei allegations driven by politics not evidence: U.N. telecoms... *Reuters*. Retrieved from https://www.reuters.com/article/us-usa-china-huawei-tech-un-idUSKCN1RH1KN

Miles, T. (2019b, April 12). China warns Australia at WTO about 5G restriction. *Reuters*. Retrieved from https://www.reuters.com/article/us-huawei-australia-china-wto-idUSKCN1RO20H

Miles, T. (2019c, June 17). China pulls WTO suit over claim to be a market economy - Reuters. Retrieved June 27, 2019, from Reuters website: https://www.reuters.com/article/us-usa-china-wto-eu/china-pulls-wto-suit-over-claim-to-be-a-market-economy-idUSKCN1TI10A

Morris, I. (2018, December 13). Orange Rules Out Huawei for 5G in France. Retrieved March 5, 2019, from Light Reading website: https://www.lightreading.com/mobile/5g/orange-rules-out-huawei-for-5g-in-france/d/d-id/748274

Muller, R. (2018, March 15). Czech president's aides travel to China to look into CEFC chief... *Reuters*. Retrieved from https://www.reuters.com/article/us-china-cefc-czech-idUSKCN1GR3C5

Muncaster, P. (2013, March 28). US bill prohibits state use of tech linked to Chinese government. Retrieved June 27, 2019, from The Register website: https://www.theregister.co.uk/2013/03/28/us_government_crackdown_china_it_firms/

Naughton, J. (2016). The evolution of the Internet: from military experiment to General Purpose Technology. *Journal of Cyber Policy*, *1*(1), 5–28. https://doi.org/10.1080/23738871.2016.1157619

NCarnovale. (2018, August 23). Government Provides 5G Security Guidance To Australian Carriers [Text]. Retrieved March 10, 2019, from https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers

Nye, Jr., J. S. (2014, May). *The Regime Complex for Managing Global Cyber Activities*. Retrieved from https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf

Obiodu, E., & Giles, M. (2017). *The 5G era: Age of boundless connectivity and intelligent automation*. Retrieved from GSMA website: https://www.gsmaintelligence.com/research/?file=0efdd9e7b6eb1c4ad9aa5d4c0c971e62&download

O'Hara, K., & Hall, W. (2018). *Four Internets: The Geopolitics of Digital Governance*. (206), 28.

Okano-Heijmans, M., van der Putten, F.-P., & van Schaik, L. (2018, December 18). A United Nations with Chinese characteristics? | Clingendael. Retrieved June 27, 2019, from https://www.clingendael.org/publication/united-nations-chinese-characteristics

Parton, C. (2019, February). China–UK Relations: Where to Draw the Border Between Influence and Interference? | RUSI.

Retrieved March 20, 2019, from https://rusi.org/publication/occasional-papers/china-uk-relations-where-draw-border-between-influence-and

Patton, D., & Nickel, R. (2019, March 5). China blocks some Canada canola shipments, Ottawa expresses concern. *Reuters*. Retrieved from https://www.reuters.com/article/us-china-canada-canola-trade-idUSKCN1QM0P8

Pohlmann, T. (2018, December 12). Who is leading the 5G patent race? | Lexology. Retrieved July 5, 2019, from Lexology website: https://www.lexology.com/library/detail.aspx?g=64ea84d0-f9ce-4c2b-939b-dec5c2560e06

Reed, M. (2018). *5G in the Middle East and Africa*. Retrieved from Ovum website: https://ovum.informa.com/~/media/informa-shop-window/tmt/whitepapers-and-pr/5g-in-the-middle-east-and-africa-pdf.pdf

Research & Development - About Huawei. (2017). Retrieved February 14, 2019, from huawei website: https://www.huawei.com/en/about-huawei/corporate-information/research-development

Reuters. (2019, January 13). Poland calls for "joint" EU-Nato stance on Huawei after spying arrest. *The Guardian*. Retrieved from https://www.theguardian.com/world/2019/jan/12/huawei-sacks-chinese-worker-accused-of-spying-in-poland-wang-weijing

Robertson, A. (2013, July 30). Lenovo reportedly banned by MI6, CIA, and other spy agencies over fear of Chinese hacking (update). Retrieved June 27, 2019, from The Verge website: https://www.theverge.com/2013/7/30/4570780/lenovo-reportedly-banned-by-mi6-cia-over-chinese-hacking-fears

Rogers, M., & Ruppersberger, D. (2012, October 8). *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*. Retrieved from https://stacks.stanford.edu/file/druid:rm226yb7473/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf

Rosen, D. H., & Kennedy, S. (2019, January 28). Building a Better Deal with China. Retrieved February 4, 2019, from https://www.csis.org/analysis/building-better-deal-china

Rushe, D. (2018, March 13). Qualcomm deal over as Trump blocks Singaporean chip maker's bid. *The Guardian*. Retrieved from https://www.theguardian.com/business/2018/mar/12/qualcomm-broadcom-deal-trump

Sacks, S. (2018). *Disruptors, Innovators, and Thieves: Assessing Innovation in China's Digital Economy*. 38.

Schneier, B. (2018, May 10). Supply-Chain Security. Retrieved June 27, 2019, from Schneier on Security website: https://www.schneier.com/blog/archives/2018/05/supply-chain_se.html

Science and Technology Committee. (2019, June 10). Oral evidence - UK telecommunications infrastructure - 10 Jun 2019. Retrieved June 27, 2019, from UK Parliament website: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/uk-telecommunications-infrastructure/oral/102931.html

Scott, M. (2018, July 1). Telcogeopolitics: West vs. China in 5G race – POLITICO. Retrieved January 23, 2019, from https://www.politico.eu/article/5g-telecommunications-infrastructure-china-us-eu-qualcomm-nokia-ericsson-huawei/

Sirilal, R. (2018, June 20). *Chinese firm pays $584 million in Sri Lanka port debt-to-equity deal | Reuters*. Retrieved from https://www.reuters.com/article/us-sri-lanka-china-ports/chinese-firm-pays-584-million-in-sri-lanka-port-debt-to-equity-

deal-idUSKBN1JG2Z6

Steinbock, D. (2017, September 20). The global economic balance of power is shifting. Retrieved March 20, 2019, from World Economic Forum website: https://www.weforum.org/agenda/2017/09/the-global-economic-balance-of-power-is-shifting/

Strange, S. (1992). States, Firms and Diplomacy. *International Affairs (Royal Institute of International Affairs 1944-)*, *68*(1), 1–15. https://doi.org/10.2307/2620458

Tong, S. (2019, March 1). Here's why there's no U.S. telecom giant like Huawei. Retrieved March 5, 2019, from http://www.marketplace.org/2019/03/01/tech/heres-why-theres-no-us-telecom-giant-huawei

Triolo, P., & Allison, K. (2018, November 15). The Geopolitics of 5G. Retrieved March 11, 2019, from https://www.eurasiagroup.net/live-post/the-geopolitics-of-5g

Trubowitz, P., & Harris, P. (2019, May 16). Will Dysfunctional Politics Finally End the American Century? Retrieved June 27, 2019, from Chatham House website: https://www.chathamhouse.org/expert/comment/will-dysfunctional-politics-finally-end-american-century

United Nations. (2019, June). Report of the Secretary General's High-level Panel on Digital Cooperation. Retrieved July 5, 2019, from High Level Panel on Digital Coopearation website: https://digitalcooperation.org/

Vanderklippe, N. (2019, April 10). *Two Canadians detained in China for four months prevented from going outside, official says*. Retrieved from https://www.theglobeandmail.com/world/article-two-canadians-detained-in-china-are-prevented-from-seeing-the-sun-or/

Wessel, M. (2019, February 6). *Prepared Testimony of Commissioner Michael Wessel Before the Senate Commerce, Science & Transportation Committee*. Retrieved from https://www.commerce.senate.gov/public/_cache/files/3b1ad4d5-b73a-4b01-bf93-8e6695095ca8/7FA65EC59FA17F43EAE42CFF3C13D808.02-01-2019wessel-testimony.pdf

Wijnen, P. (2019, February 15). Norway not naïve with regards to Huawei - Norway Today - 5G Security. Retrieved March 10, 2019, from Norway Today website: https://norwaytoday.info/news/norway-not-naive-with-regards-to-huawei/

Winner, L. (1980). Do Artifacts have Politics. *Daedalus*, *109*(1), 121–136.

Withers, T. (2019, February 18). *New Zealand Says China's Huawei Hasn't Been Ruled Out of 5G*. Retrieved from https://www.bloomberg.com/news/articles/2019-02-18/new-zealand-says-china-s-huawei-hasn-t-been-ruled-out-of-5g-role

Wong, E. (2017, December 21). China Approves Sweeping Security Law, Bolstering Communist Rule. *The New York Times*. Retrieved from https://www.nytimes.com/2015/07/02/world/asia/china-approves-sweeping-security-law-bolstering-communist-rule.html

World Bank. (n.d.). High-technology exports (current US$) | Data. Retrieved March 18, 2019, from https://data.worldbank.org/indicator/TX.VAL.TECH.CD?locations=CN

World Trade Organization. (n.d.-a). Dispute settlement - disputes by country/territory. Retrieved July 3, 2019, from World Trade Organisation website: https://www.wto.org/english/tratop_e/dispu_e/dispu_by_country_e.htm

World Trade Organization. (n.d.-b). WTO Services - CBT - Basic Purpose and Concepts - Most-Favoured-Nation Treatment - Page 1. Retrieved March 21, 2019, from https://www.wto.org/english/tratop_e/serv_e/cbt_course_e/c1s6p1_e.htm

Zarroli, J. (2019, March 6). China's Close Government-Business Ties Are A Key Challenge In U.S. Trade Talks. Retrieved March 7, 2019, from NPR.org website: https://www.npr.org/2019/03/06/700474697/chinas-close-government-business-ties-are-a-key-challenge-in-u-s-trade-talks

Zittrain, J. (2008). *The Future of the Internet: And How to Stop It*. Retrieved from https://www.amazon.co.uk/Future-Internet-How-Stop/dp/014103159X