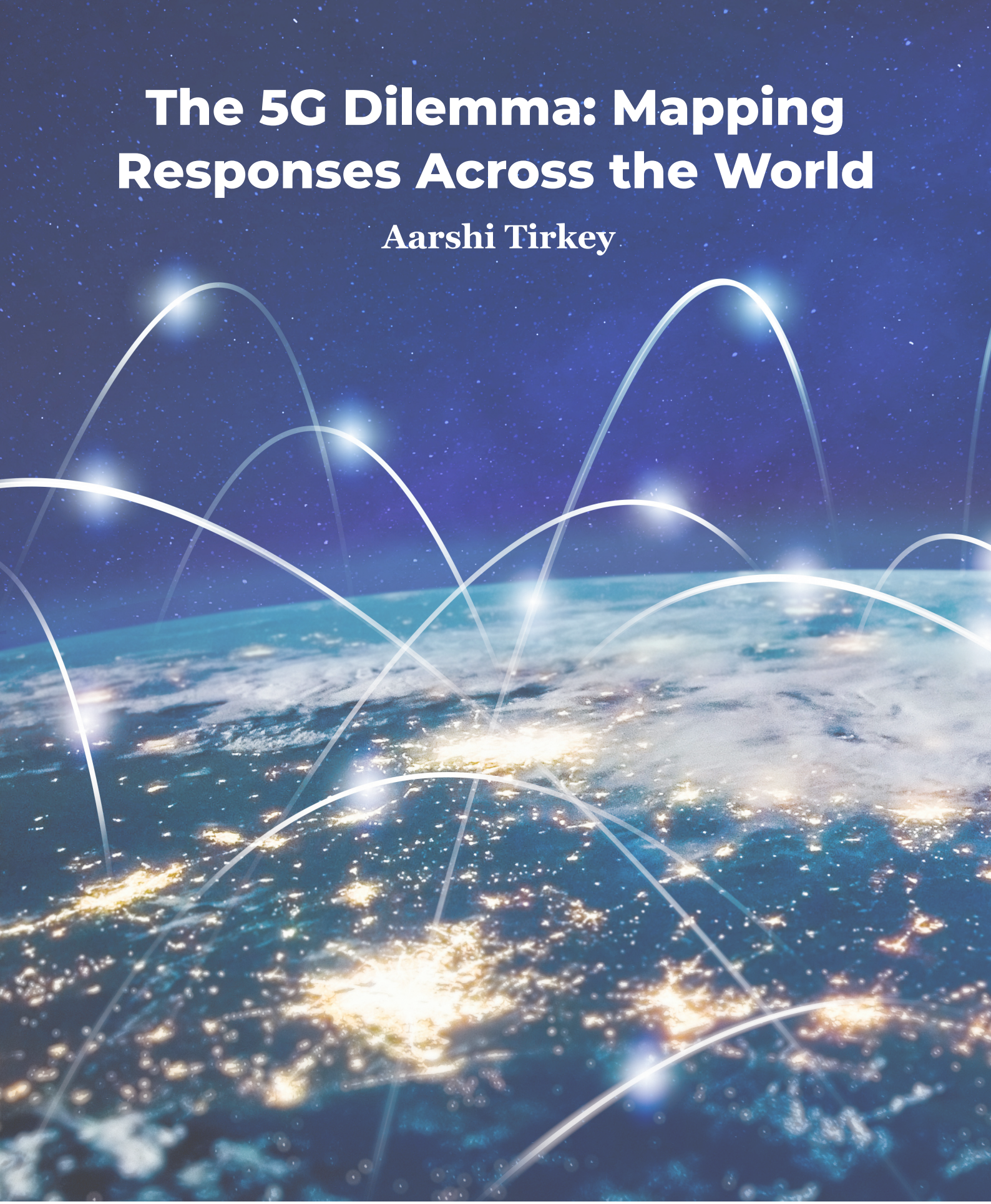
The 5G Dilemma: Mapping Responses Across the World

Aarshi Tirkey



ORF

The 5G Dilemma: Mapping Responses Across the World

Aarshi Tirkey

Attribution: Aarshi Tirkey, *The 5G Dilemma: Mapping Responses Across the World*, Observer Research Foundation, May 2020.

Observer Research Foundation
20 Rouse Avenue, Institutional Area
New Delhi, India 110002
contactus@orfonline.org
www.orfonline.org

ORF provides non-partisan, independent analyses on matters of security, strategy, economy, development, energy and global governance to diverse decision-makers including governments, business communities, academia and civil society. ORF's mandate is to conduct in-depth research, provide inclusive platforms, and invest in tomorrow's thought leaders today.

Design and Layout: simijaisondesigns

Cover image: Getty Images/Traitov and NASA

ISBN: 978-93-89622-95-9
ISBN Digital: 978-93-89622-96-6

CONTENTS

PREFACE

The roll-out of the 5G network, the next generation of global communications, has not only emerged as a critical flashpoint in the emerging geopolitical contestation between China and western countries, led by the United States (US), but it has also engendered an interesting debate in India about its own choices. When it comes to adopting and deploying 5G networks, policymakers across the world are facing a critical choice—one that will require them to carefully weigh and balance a broad range of economic, political, technical, and strategic considerations.

Technology – particularly information and communications technology – has long played an important role in shaping geopolitical contours. In the late 19th century, the United Kingdom (UK) was the first mover of telegraphy and submarine cable systems. By building these extensive communications network, the UK was able to maintain channels of communication with its colonies and consolidate the British Empire. The subsequent development of radar technology by the UK gave it an edge over the German challenge during World War II. Following the war, British hegemony was directly challenged by the US as it made rapid advancements in telephony, becoming one of the first in the world to deploy a satellite communications system. Eventually, the US and its allies used America's extensive satellite networks to intercept and decode information during the Cold War period. The US' use of satellite technology to spy on the flow of information and communication through its satellites has also led to concerns which echo some of the themes of the current debate surrounding the 5G network of Chinese company, Huawei. What makes this debate particularly challenging is the growing distrust around the world over China's rise because of its opaque decision-making system and its growing use of information asymmetry for geopolitical leverage.

While China stands to gain significantly by being the first mover of this technology, the US has continued to put pressure on its allies and partners against accepting Huawei's telecommunications equipment. There are growing concerns about China in the wider West which are likely to lead western nations into giving renewed impetus towards developing alternative 5G networks. This in turn can lead to the development of two politically and geographically divided 5G networks which may not be interoperable, thereby leading to lower economies of scale and higher transaction costs.

This important study by Aarshi Tirkey, Junior Fellow at Observer Research Foundation (ORF), is aimed at informing the wider policy debate in India on this important issue by explicating the responses of various nations across the world on the issue of 5G. It starts by comparing Huawei's position vis-à-vis other major telecommunications equipment manufacturers across several verticals before moving on in the second part to delineate the responses of the US, UK, Australia and Canada. The third part of the monograph explores the responses of nations from Europe and the Indo-Pacific, while the final section broadly examines the Middle East, Latin America, Russia and Central Asia.

I would like to thank Aarshi for taking on this ambitious project, and Vinia Datinguinoo Mukherjee for taking this volume through to publication. If New Delhi is to make the best possible decision on this highly complex matter, then it needs to carefully study global responses to the challenge. While the ongoing Covid-19 pandemic might delay the 5G rollout in India for some time, there is no wishing away this question. The Strategic Studies Programme at ORF brings you this monograph to push an already animated debate on 5G in India towards a more serious policy conversation so that India and its policymakers can make prudent decisions at a time of enormous global flux.

Prof. Harsh V Pant
Director, Studies and Head, Strategic Studies Programme
Observer Research Foundation, New Delhi
May 2020

Abstract

The 5G network, the next generation of wireless technology, is a subject in ongoing tensions between the United States (US) and China. Washington has raised concerns that sourcing 5G equipment from Huawei and other Chinese companies will expose a country to national security risks, such as espionage and surveillance. For its part, Beijing has dismissed these concerns as a flagrant attempt to politicise a technological issue. Their confrontation, however, has transcended to a global level—both the US and China have been engaging in diplomatic lobbying to influence the decision of countries on the sourcing of their 5G equipment. As countries in many parts of the world proceed to upgrade their networks, they are faced with decisions that will not only be based on technological or economic considerations, but will have immense strategic implications as well. This monograph provides an overview of the responses of countries to the 5G dilemma and the factors that have influenced them.

Introduction

The 5G network, the next generation of wireless technology, has emerged as one of the biggest turning points in geopolitical tensions in recent times. 5G's unique features and applications mean that the technology will be critical for economic and technological advancement. At the same time, the country that controls and spearheads development of said technology will also gain the enviable position of becoming a technological leader. As power rivalry between the United States (US) and China intensifies, it is highly likely that the new networks will shape the competition for 21st-century dominance between two leading technology superpowers.[1]

5G is the fifth generation of cellular technology. In contrast with 2G, 3G and 4G networks, 5G will provide fibre-like connectivity over wireless networks through greater speed, higher capacity communication and ultra-low latency. These features will help unlock revolutionary use cases to support the demands of individuals, businesses and governments alike. From reducing movie download time to a few seconds, to supporting industrial automation for manufacturers and to operationalising government initiatives such as smart cities, 5G is viewed as an enabler for social and economic development. The network will also power emerging technologies commonly associated with the Fourth Industrial Revolution (4IR) such as artificial intelligence, robotics, autonomous vehicles, 3D printing, nanotechnology and quantum computing, which can bring long-term gains in efficiency, productivity and quality of life.[2]

An illustration to further demonstrate 5G's potential is its ability to support machine-to-machine communication and enhance Internet of things (IoT)[3] applications utility in aquaculture and fisheries. In Indonesia, Telkomsel—a leading mobile operator—and eFishery (a Bandung-based start-up) have jointly developed a technology that enables a fish farmer to remotely control a fish feeder unit via a smartphone, instead of doing it manually—a method that is both expensive and inaccurate.[4] With 5G, such applications can be deployed on a nationwide scale, improving both productivity and livelihoods for fish farmers. Figure 1 details the three main features of 5G network, and commonly mentioned use cases and examples.

Many countries across the world are keen on swiftly deploying 5G and are well on their way to design policies, strategies and roadmaps to set up these networks. Till

1 "The Geopolitics of 5G and its Impact on Business", *Chatham House*, September 30, 2019, https://www.chathamhouse.org/event/geopolitics-5g-and-its-impact-business.

2 Klaus Schwab, "The Fourth Industrial Revolution: what it means, how to respond", *World Economic Forum*, January 14, 2016, https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

3 The Internet of Things (IoT) refers to a network comprised of physical objects capable of gathering and sharing electronic information.

4 "Mobile IoT Case Study: How Asia Pacific Intelligently Connects to IoT", *GSMA Intelligence,* February 2019, 15, https://www.gsma.com/iot/wp-content/uploads/2019/08/201902_GSMA_APAC_MobileIoT_Case_Study.pdf.

Fig. 1: Three major use cases for 5G

Enhanced mobile broadband (eMBB) including fixed wireless access	Ultrareliable, low-latency communications (URLLC)	Massive machine-type communications (IoT)
❖ More capacity, higher speeds, supports more users ❖ Uses licensed and unlicensed spectrum ❖ Incorporates technologies such as massive MIMO ❖ Examples: o Mobile/4K video o Rich media and entertainment o Augmented reality o Home entertainment, small office/home office (SoHo) (fixed wireless access)	❖ Supports ultralow latency transmission (<1ms) ❖ Supports highly resilient communications with redundancy ❖ Offers reliable device-to-device communication ❖ Examples: o Industrial automation o Autonomous vehicles o Telemedicine	❖ Evolves out of narrowband LTE (eMTC/NB-IoT) ❖ Low complexity, low energy ❖ Follows the ultradense, small cell network model ❖ Eventually adds new waveforms and architectures (e.g. multi-hop mesh) ❖ Examples: o Smart grid o Smart cities o Health monitoring

Source: "5G in the Middle East and Africa", Ovum, 2018, 8, https://www.omdia.com/~/media/informa-shop-window/tmt/whitepapers-and-pr/5g-in-the-middle-east-and-africa-pdf.pdf.

now, mobile operators in these countries have collectively carried out over 300 5G trials, while 60 operators in 31 countries have commercially launched 5G services.[5]

While framing state policies, a critical concern for all stakeholders is sourcing equipment from an affordable, secure and technologically advanced supplier. With major suppliers ready to provide 5G equipment, open market principles will simply mean that the vendor with the best price and technology wins the most contracts. However, these general and logical considerations have become secondary factors in guiding stakeholders' decision on 5G vendors.

This is because the question of sourcing the equipment has become closely interconnected with the ongoing economic and technological rivalry between the US and China. Chinese telecommunications giant Huawei Technologies Co. Ltd. (Huawei), has emerged as the leading supplier for end-to-end 5G equipment, forging ahead of its main competitors, Telefonaktiebolaget LM Ericsson (Ericsson) and Nokia Corporation (Nokia). However, a small group of western nations—led by the US—have raised the alarm against equipment sourced from Huawei and similar Chinese tech companies. Alleging that such equipment could come built with "backdoors" to carry out cyberattacks, cyber-espionage and information warfare, and promote digital authoritarianism at Beijing's behest,[6] countries like the US and Australia have explicitly banned Huawei citing national security risks. Other reasons, such as Huawei's opaque ownership structure and China's framework of intelligence laws, have further weighed against the company's credibility.

The ban also appears to be closely motivated by the US stratagem to prevent China from gaining geopolitical, economic and technological clout by being the first mover of the technology. If Huawei emerges as a leader in 5G technology, China's gains are undeniable and perhaps even inevitable. Beijing may well replace Washington as a leading cyber power, shaping future technological norms for generations to come.

5 "5G & LTE Deployments", 5G Americas, last modified March 17, 2020, https://www.5gamericas.org/resources/deployments/.

6 "5G in the EU and Chinese telecoms suppliers", European Parliament, April 2019, https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637912/EPRS_ATA(2019)637912_EN.pdf.

In this context, it is interesting to follow Washington's attempts to marshal its allies to follow suit, and ban Huawei and other Chinese vendors like ZTE Corporation (ZTE). Washington's methods comprise intensive diplomatic lobbying, scheduling meetings with decision-makers and stakeholders, signing statements and declarations, publicly condemning countries that allow Chinese companies, and proclaiming that it will rethink intelligence ties with states that allow Huawei.

China, for its part, has dismissed these concerns, saying that the consideration of non-technical criteria (namely, potential for foreign interference) in 5G decisions is a "flagrant move to politicize a technology issue".[7] However, Beijing has not been far behind the US in issuing statements that hint towards the use of coercion and reverse sanctions should a country decide to exclude Huawei from its market. Given how China has emerged as an important trade and investment partner for countries across regions, its words and actions carry weight because it may cause potential economic and political repercussions for countries.

In light of the technological cold war between Washington and Beijing, countries face a pressing dilemma: they must either ban Huawei and face repercussions from China, or allow it entry and suffer pushback from the US. As the 5G dilemma unfolds, this study will aim to map the responses of countries across the world and identify which factors have influenced the decision of individual countries, and the extent to which geopolitical and strategic considerations have shaped their approach.

India has also grappled with these complex factors in deciding upon the question of allowing Chinese equipment suppliers to build its 5G networks. In December 2019, the Ministry for Communications, Electronics & Information Technology announced that all vendors—including Chinese companies—will be allowed to participate in 5G trials. Though Huawei can participate in 5G trials, a final decision on whether it will supply equipment to Indian mobile operators is yet to be announced. This analysis, however will not examine the ongoing Indian debate on this question, but instead inform New Delhi's stakeholders by detailing the responses of other governments across the world.

The first part of this study compares Huawei's position vis-à-vis other major telecommunications equipment manufacturers across verticals, such as market share, annual revenues, and ownership of 5G intellectual property rights. It also explores common criticisms and allegations levelled against the company, and examines Huawei's approach to countering them. On the pivotal question of the possible use of telecom equipment for surveillance and intelligence gathering, this study argues why such concerns are not entirely unfounded.

The second section maps the responses of four countries—the US, UK, Australia and Canada to the 5G dilemma and Huawei. Though these four countries—along with New Zealand—are part of a Cold War-era intelligence alliance known as the "Five eyes", their responses to the Huawei question have varied. This is indicative of how domestic considerations are playing out against geopolitical, strategic and security related ones. To this end, this section will explore the reasons for their individual decisions.

---

7 Chinese text of speech by Wang Lei, coordinator for cyber affairs, at the sixth World Internet Conference, October 24, 2019, https://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/fywj_674643/t1710345.shtml; English text of speech by Wang Lei, coordinator for cyber affairs, at the sixth World Internet Conference, October 24, 2019, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/t1710346.shtml.

The third part looks at the responses in the two major geographical regions of Europe, and Asia and the Indo-Pacific. As Europe attempts to strike a delicate balance between its ties with the US and China, the single market of the European Union has attempted to adopt a concerted approach to 5G security, though individual countries are free to respond to the Huawei question as they deem fit. In Asia and the Indo-Pacific, the China factor looms large—mostly because of the nation's geographical proximity—and has largely inhibited countries from taking a hard position against Huawei.

Part four deals with a broad overview of responses in other regions, namely the Middle East, Latin America, Russia and Central Asia, and Africa. In the Middle East—with the exception of Israel—all counties are clear on this technological confrontation. Latin America is, so far, struggling to keep up with the high costs and investments demanded by 5G networks, due to which the 5G dilemma has mostly been confined to the region's largest country, i.e. Brazil. In Russia and Central Asia, and in Africa, the predominance of Huawei, China's burgeoning trade and investment ties, and lack of a clear US strategy appear to play an important role in boosting Huawei as a lucrative option for not just 5G, but also for broader development and technology partnerships.

The study concludes by assessing the economic, technical, security and strategic dimensions that have shaped the 5G strategies of countries, and examines the "balance sheet" —for the US and China in their geopolitical contestation for 5G networks.

CHAPTER 1.
Huawei: The Company and Criticisms

Huawei Technologies Co. Ltd. ("Huawei"), based in Shenzhen, Guangdong region, China, was founded in 1987 by Ren Zhengfei with an initial capital of CNY21,000 ($3,014).[8] Within 30 years of its establishment, Huawei has overtaken Ericsson and Nokia—its primary competitors that are nearly a 100 years older. A combination of factors—government support, financial incentives and diplomatic backing from Beijing have provided a sound market strategy for Huawei's growth. As a result, Huawei has become a dominant market player in information and communications technology (ICT) infrastructure and smart devices.

In the current context of providing 5G equipment, the Chinese telecom giant continues to be one of the few players offering end-to-end 5G solution, with particular strengths on radio access network.[9] It promises to provide the most affordable and technologically advanced alternatives of the technology at home and abroad. This is courtesy Huawei's massive investments in research and development—to the tune of $15.3 billion in research—outstripping American companies like Apple and Microsoft.[10] Table 1 compares the three companies, across various verticals of 5G commercial contracts, market share and annual revenues, among others.

Table 1. Comparing major 5G telecom equipment suppliers across contracts, market share and annual revenues

Company name	Number of 5G commercial contracts	Market Share (2018)	Year established	Annual revenue in 2019 ($ billions)	Employees	Countries
Huawei	91	29%	1987	122	188,000	170
Ericsson	86	13.1%	1876	23.9	99,417	150
Nokia	63	15.7%	1865	25.9	103,000	130

Source: 2019 annual reports of Huawei, Ericsson and Nokia. Market share numbers from Dell'Oro Group (2018), https://www.delloro.com/telecom-equipment-market-2018-2/.

With reference to the number of commercial 5G contracts, it must be noted that the numbers for Huawei[11] and Nokia[12] are based on information released on their website. In this regard, Ericsson is the only vendor to have maintained an unparalleled level of transparency by publishing details of all publicly-announced

8 "Ren Zhengfei, Director, CEO", Huawei, accessed March 25, 2020, https://www.huawei.com/en/about-huawei/executives/board-of-directors/ren-zhengfei.

9 Elsa B. Kania and Lindsey R. Sheppard, "Why Huawei Isn't So Scary", *Foreign Policy*, October 12, 2019, https://foreignpolicy.com/2019/10/12/huawei-china-5g-race-technology/.

10 "No Pay, No Gain: Huawei Outspends Apple on R&D for a 5G Edge", *Bloomberg,* April 2019, https://www.bloomberg.com/news/articles/2019-04-25/huawei-s-r-d-spending-balloons-as-u-s-tensions-flare-over-5g.

11 Lauly Li and Cheng Ting-Fang, "Huawei claims over 90 contracts for 5G, leading Ericsson", *Nikkei Asian Review,* February 21, 2020, https://asia.nikkei.com/Business/China-tech/Huawei-claims-over-90-contracts-for-5G-leading-Ericsson.

12 "Nokia Highlights Momentum with 63 Commercial 5G Deals", *Nokia,* January 9, 2020, https://www.nokia.com/about-us/news/releases/2020/01/09/nokia-highlights-momentum-with-63-commercial-5g-deals/.

commercial agreements, with a regularly updated interactive map indicating the status of the network with individual mobile operators.[13]

A metric used to support Huawei's claim of being the most technologically advanced supplier is an assessment of the number of 5G patents it owns and its role in formulating 5G standards. In a 2019 report, IPlytics (a German market intelligence firm) analysed that Huawei leads across several patents-related parameters, including being the top patent owner of 5G declarations, and the top company to submit technical 5G contributions.[14] However, a study by Bird & Bird, a leading UK law firm found that many of these studies are "too simplistic"[15]; patents need to be distinguished between essential patents (truly integral to the use of the technology and there is no way to design around it) compared to related patents (not essential, and substitutes exist). Its analysis supported the conclusion that at 15.8 percent, Ericsson owns the highest number of 5G patents, whereas Huawei is the fifth highest, owning 10.9 percent 5G patents.[16] While the precise numbers on patent ownership may be difficult to discern, Huawei still stands ahead of the pack and has established itself as one of the largest telecom equipment manufacturers in the world.

The company has also made efforts to build goodwill, enhance reputation and establish trust-based partnerships with companies and governments alike. These initiatives can be termed as "soft power" approaches and include investments, partnerships, research collaborations, as well as memorandums of understanding with public and private stakeholders. However, this is usual practice for major tech companies across the world. Other telecom equipment manufacturers, such as Ericsson and Nokia, have set up their own research centres and have tie-ups with global universities; for instance, Ericsson has setup a 5G innovation lab and an artificial intelligence lab in India.[17] Nokia's Bell Labs is an industrial research and scientific development company, operates laboratories worldwide, and runs multiple collaborative programmes including the Distinguished Academic Partner Program (DAP), which aims to engage with universities and academic organisations to drive innovation and research.[18]

Nevertheless, Huawei recognises the influence it can wield through the promise of investments and funding tech collaborations. In the case of Poland, such investments are conditioned on reciprocity in the form of a transparent, fair and efficient policy on 5G networks.[19] Table 2 below provides some prominent examples of Huawei's soft power approach initiatives.

---

13 "86 commercial 5G agreements or contracts with unique operators", *Ericsson*, accessed March 25, 2020 https://www.ericsson.com/en/5g/5g-networks/5g-contracts.

14 "Who is leading the 5G patent race?", *IPLytics,* November 2019, 6-9, https://www.iplytics.com/wp-content/uploads/2019/01/Who-Leads-the-5G-Patent-Race_2019.pdf.

15 Matthew Noble, Jane Mutimear and Richard Vary, "Determining which companies are leading the 5G race", *IAM Media,* July/August 2019, 35, https://www.twobirds.com/~/media/pdfs/news/articles/2019/determining-which-companies-are-leading-the-5g-race.pdf?la=en&hash=8ABA5A7173EEE8FFA612E070C0EA4B4F53CC50DE

16 "Who is leading 5G development?", *twoBirds Pattern,* accessed March 25, 2020, https://www.twobirds.com/~/media/pdfs/who-is-leading-5g-development.pdf?la=en&hash=AB57AC4B01AD1F8BE641A590222DE8BDA1D8B082&hash=AB57AC4B01AD1F8BE641A590222DE8BDA1D8B082.

17 Danish Khan, "Ericsson sets up new Artificial Intelligence lab in Bengaluru; to hire 150 engineers in 2019", *ET Telecom*, December 13, 2018, https://telecom.economictimes.indiatimes.com/news/ericsson-sets-up-new-artificial-intelligence-lab-in-bengaluru-to-hire-150-engineers-in-2019/67072413.

18 "About the DAP Program", *Nokia Bell Labs,* accessed March 25, 2020, https://www.bell-labs.com/programs/distinguished-academic-partners/about-dap-program/

19 George Paul, "Huawei plans to sink $800 million into a Brazilian smartphone factory to combat international opposition", *Business Insider,* August 13, 2019, https://www.businessinsider.com/huawei-expanding-presence-in-brazil-with-new-facility-2019-8?IR=T.

Table 2. Illustrations of Huawei's "soft power" initiatives across the world

Country/ Programme name	Description
France	Invest 35 million Euros (US$39 million) in its Paris OpenLab to provide a platform for industry experts to identify their future needs in digital transformation and develop industry-specific solutions.[20]
Singapore	Launch of cloud and artificial intelligence (AI) innovation lab with a pledge to commit "hundreds of millions" worth of investment in the coming years.[21]
Canada	C$56 million (US$40 million) spent in research funding, scholarships and engineering awards to various Canadian higher educational institutes, such as the University of Waterloo and University of British Columbia.[22]
Russia	Promote development of 5G by investing 500 million Roubles ($7.8 million) in training 10,000 specialists over the next five years.
Malaysia	2017 announcement of an OpenLab, which will serve as an open, flexible, and secure platform for joint innovation with local partners.
Brazil	Plans to invest up to $800 million over the next three years to expand its presence in Brazil via a new manufacturing facility in São Paulo.
Italy	Proposal to invest $3.1 billion in Italy over the next three years and create 1,000 jobs.[23]
Poland	Huawei to spend almost 3 billion Złoty ($789 million) over the next five years, though it also said the investment was dependent on its role in Poland's 5G deployments.
Seeds for the Future programme	A global corporate social responsibility (CSR) program wherein top college students visit and study at Huawei's headquarters in China. To date, the programme has benefited over 30,000 students from more than 350 universities worldwide.[24]

As Huawei began to dominate 5G contracts, the US and other Western nations levelled a plethora of criticisms and allegations against its leadership and ownership structure, legal violations and its possible role in supporting China's economic and strategic goals. What makes it tougher to decouple Huawei from Beijing, is the close association of Chinese companies with the Beijing government, which has stoked fears that Chinese equipment could be used for carrying out espionage, surveillance and cyber-attacks. These allegations have extended to ZTE as well, which originated from Beijing's Ministry of Aerospace, maintains close ties with China's military apparatus and allegedly functions as a "hybrid" to serve commercial and military needs[25]. ZTE,

20 "Huawei to invest 35 million euros in Paris Openlab", *Huawei,* May 16, 2019, https://huawei.eu/press-release/huawei-invest-35-million-euros-paris-openlab.

21 Chong Koh Ping, "Chinese tech giant Huawei opens cloud and AI innovation lab in Singapore", *The Straits Times,* April 24, 2019, https://www.straitstimes.com/tech/chinese-tech-giant-huawei-opens-cloud-and-ai-innovation-lab-in-singapore.

22 Peter Armstrong, "Huawei funds $56M in academic research in Canada. That has some experts concerned", *CBC News,* November 29, 2019, https://www.cbc.ca/news/business/huawei-academic-funding-in-canada-1.5372310.

23 Elvira Pollina, "Huawei to invest $3.1 billion in Italy but calls for fair policy on 5G: country CEO", *Reuters,* July 15, 2019, https://www.reuters.com/article/us-huawei-italy/huawei-to-invest-31-billion-in-italy-but-calls-for-fair-policy-on-5g-country-ceo-idUSKCN1UA11V.

24 "Seeds for the Future", *Huawei,* accessed March 25, 2020, https://www.huawei.com/en/about-huawei/sustainability/win-win-development/social-contribution/seeds-for-the-future.

however, has secured 46 commercial contracts and trails behind other market leaders.[26] Table 3 categorises and explores the common criticisms and allegations against Huawei.

Table 3. Exploring common criticisms and allegations against Huawei

Category	Criticisms and Allegations
Against Huawei's company and leadership	**Opaque ownership structure:** Huawei says that it is entirely owned by employees, and that no government agency or outside organisation holds shares in the company. However, details regarding its structure, ownership and internal governance are not readily available. A 2019 research paper concluded that it is clear that employees do not own the company, and it could be effectively state-owned if it follows a regular PRC trade union structure.[27] **Ren Zhengfei, (CEO, Huawei) and his connection to Beijing:** He was previously with the engineering corps of the People's Liberation Army (1974-1983). Though he owns little more than one percent of shares, he still has the right to veto company decisions. This has led to speculation that Zhengfei's background influences the company's operations, since several Huawei employees have collaborated with Chinese armed forces on research projects.[28] **Huawei's legal violations:** The company and its leadership have been indicted for theft of trade secrets and intellectual property, and violation of Iran sanctions.
Espionage and cyber security risks	**Possible installation of backdoors:** "Backdoors" refer to code or software that may allow China to monitor and intercept transmission over Huawei's equipment. This allegation has not yet been established, but in February 2020, Robert O'Brien, US' National Security Advisor said that they now have evidence that Huawei could access "sensitive and personal information" in its systems.[29] **China's intelligence and espionage laws:** The 2015 National Security Law and 2017 National Intelligence Law state that Chinese enterprises have a responsibility and obligation to maintain national security and may be required to support, assist, and cooperate with China's intelligence-gathering authorities.

25 "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE", Permanent Select Committee on Intelligence, U.S. House of Representatives, October 8, 2012, 38-39, https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

26 Juan Pedro Tomás, "ZTE has racked up 46 5G commercial contracts globally", *RCRWireless,* February 25, 2020, https://www.rcrwireless.com/20200225/5g/zte-already-secured-46-5g-commercial-contracts-globally.

27 Christopher Balding and Donald C. Clarke, "Who owns Huawei", SSRN, April 17, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3372669.

28 "Huawei Personnel Worked With China Military on Research Projects", *Bloomberg,* June 27, 2019, https://www.bloomberg.com/news/articles/2019-06-27/huawei-personnel-worked-with-china-military-on-research-projects.

29 Julian E. Barnes, "White House Official Says Huawei Has Secret Back Door to Extract Data", *The New York Times*, February 11, 2020, https://www.nytimes.com/2020/02/11/us/politics/white-house-huawei-back-door.html.

Category	Criticisms and Allegations
Huawei and China's connection	**State subsidies and concessions:** A review of Huawei's grants, credit facilities, tax breaks and other forms of financial assistance reveals that the company had access to roughly $75 billion in state support, allowing it to offer generous financing and compete with rival prices.[30] In comparison, Cisco Systems Inc. received $44.5 million in state and federal subsidies, loans, guarantees, grants and other US assistance. Sweden and Finland have respectively provided $10 billion in credit assistance and $30 billion in annual export credit guarantees to their tech and telecom sector.[31]
Huawei's rise supports China's strategic goals	**Civil and military integration[32] or military and civil infusion in China:** According to the RWR, a Washington-based consulting firm, Beijing aims to bind the defence sector and civilian economy together, outcompete the West in science and technology, and build itself as a preeminent military power. **Complementary to China's strategic goals:** Speeches, statements and Chinese policy documents (2015 Military strategy and the Made in China 2025) aim to establish Beijing as a cyber power. This will be done by securing its position as a global powerhouse in high-tech industry, and to rid China of foreign control over core technologies (often referred to as techno-nationalism). The 2019 Military Strategy Document notes that Beijing's military security is confronted by risks from "technology surprise and growing technological generation gap", and aims to invest towards cutting edge technologies and military modernisation.[33] Huawei could also be bundled with the Digital Silk Road projects, which plan to enhance digital connectivity under the ambitious Belt and Road Initiative (BRI)—considered to be important for expanding China's economic and political influence. Huawei's investments and expansion will provide significant economic dividends to China, and give greater impetus to its future economic and technological advancement.

Huawei has denied all allegations levelled against it through public interviews, press releases, and by launching an extensive online public relations campaign. It has established a "trust centre," which publishes detailed articles and news on the trustworthiness of Huawei's equipment, and its commitment to privacy protection and transparency. This initiative has also published four white papers on cybersecurity, including John Suffolk's (a former UK Chief Information Officer)

30 Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise", *The Wall Street Journal,* December 25, 2019, https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

31 *Ibid.*

32 "Assessing Huawei risk", *RWR Advisory Group,* May 2019, 35-37, https://www.rwradvisory.com/wp-content/uploads/2019/05/Assessing-Huawei-Risk.pdf.

33 "China's National Defense in the New Era", The State Council Information Office of the People's Republic of China (Foreign Languages Press Co. Ltd: Beijing, 2019).

2012 white paper on "Cyber Security Perspectives: 21st century technology and security–a difficult marriage".[34] In this white paper, Suffolk studies the challenges of communications in 21st century and outlines the Huawei approach to cyber security, where he makes an impassioned plea on the company's behalf:

> "... we have never damaged any nation or had the intent to steal any national intelligence, enterprise secrets or breach personal privacy and we will never support or tolerate such activities, nor will we support any entity from any country who may wish us to undertake an activity that would be deemed illegal in any country. In this context, with the eyes of the world always upon us, with us positively encouraging audits and inspections of our capabilities, those that wish a vendor to undertake such an activity is more likely to select a company that is under less scrutiny."[35]

The recent 2020 publication on cybersecurity is designed to address the ongoing allegations against Huawei, and argues that a supplier's country of origin is not a security risk and encourages nations to adopt a "rational, objective, and evidence-based assessment" of cybersecurity risks.[36] Huawei has also followed through with brick-and-mortar initiatives to address cybersecurity risks and vulnerabilities. In 2019, it opened its first Cyber Security Transparency Centre in Belgium, which functions as a platform to enhance communication and joint innovation with all stakeholders, and provides a technical verification and evaluation platform for customers.[37] Huawei has launched a "Facts" page[38] on its website to counter the dominant narrative against it in US media, and publish "official truth and facts" about the company.

Huawei has also maintained that it cannot be compelled by national intelligence laws to comply with the mandate of the Chinese state, and that Beijing's laws do not compel it to install backdoors in its equipment. In a bid to assuage concerns regarding backdoors, the company has proposed entering into "no backdoor" agreements with countries flagging the issue.[39]

Ironically, the allegations at hand become more significant because of Washington's own conduct in the recent past. The 2013 Edward Snowden leaks revealed how the National Security Agency (NSA) attempted to conduct surveillance by intercepting and hacking routers made by Cisco and other US manufacturers, and loading them with backdoors and surveillance software.[40]

Further, there are comparable surveillance laws in the US as well, such as Section 702 of the 1973 Foreign Intelligence Surveillance Act and Section 215 of the 2001 Patriot Act. The former allows the US government to spy on internet and telephone communications of people in both US and abroad–without a warrant–for the

---

34 John Suffolk, "Cyber Security Perspectives 21st century technology and security – a difficult marriage", *Huawei,* 2012, https://www-file.huawei.com/-/media/corporate/pdf/cyber-security/cyber-security-white-paper-2012-en.pdf.

35 *Ibid*, 12-13.

36 "Huawei's Position Paper on Cyber Security", *Huawei*, November 2019, 20-22, https://www-file.huawei.com/-/media/corporate/pdf/public-policy/huaweis_position_paper_on_cybersecurity.pdf.

37 "Huawei Cyber Security Transparency Centre", *Huawei*, accessed March 25, 2020, https://www.huawei.com/en/about-huawei/trust-center/transparency/huawei-cyber-security-transparency-centre-brochure.

38 "Facts", *Huawei,* accessed March 25, 2020, https://e.huawei.com/en/facts.

39 Sankalp Phartiyal, "China's Huawei says open to 'no backdoor' agreement with India", *Reuters,* October 14, 2019, https://www.reuters.com/article/us-huawei-india/chinas-huawei-says-open-to-no-backdoor-agreement-with-india-idUSKBN1WT25H.

40 "Snowden Revelations", *Lawfare,* accessed March 25, 2020, https://www.lawfareblog.com/snowden-revelations.

purpose of gathering "foreign intelligence information",[41] while the latter authorises the collection of data for investigating terrorism, counterespionage, and foreign intelligence. These provisions are one of the primary reasons why NSA's surveillance software, PRISM, is able to collect data from users of services of Google, Facebook and Microsoft, and other major tech companies. However, a key difference between the two countries pertains to the capacity of the judicial system to redress potential violations of privacy and other individual rights. The lack of an independent judiciary in China coupled with its poor track record for protecting individual rights, makes it difficult to picture a scenario where individual rights will be given primacy over Beijing's national imperatives.

No one has denied that the US spies on its allies and adversaries alike; however, by design or otherwise, Washington's espionage activities have not evoked a similar sense of alarm and outrage as in the case of the Chinese state. To be sure, any form of such intrusion should not be condoned, and ought to be flagged at the highest level of state leadership. What this does illustrate is how the responses of countries to espionage allegations differ on the basis of a single, important strategic question. Between the US and China, which country is viewed as an adversary, and which one as an ally? Vladimir Rubanov, former executive manager of Russian IT company Rosplatform and now CTO Software Engineering at Russia's Huawei R&D, said "...there is a joke among Russian tech professionals. If you use Apple, Washington listens to your calls. If you use Huawei, Beijing listens to your calls. Which is better?"[42] This statement adequately illustrates the negative reaction of countries to possible surveillance from Beijing.

41 "Q & A: US Warrantless Surveillance Under Section 702 of the Foreign Intelligence Surveillance Act", *Human Rights Watch,* September 14, 2019, https://www.hrw.org/news/2017/09/14/q-us-warrantless-surveillance-under-section-702-foreign-intelligence-surveillance.

42 Dimitri Simes, "Russia and Huawei team up as tech cold war deepens", *Nikkei Asian Review,* October 28, 2019, https://asia.nikkei.com/Politics/International-relations/Russia-and-Huawei-team-up-as-tech-cold-war-deepens.

CHAPTER 2.

Responses: Four Cases

A. The United States (US)

The United States (US) has categorically prohibited Chinese vendors, namely Huawei and ZTE from supplying any equipment to the country. Given how modern communications infrastructure are an integral part of the economy, the US is keen to protect its networks from Chinese surveillance, cyberattacks, and loss of integrity and confidentiality of services. As such, lawmakers, executives and members of the intelligence community have repeatedly stressed the importance of identifying and eliminating potential security vulnerabilities in communications networks and their supply chains.

As far back as 2011, the US has been suspicious of the entry of Chinese technology due to its tradition of civil and defence integration and the purported extent of state control on Huawei's technology. Table 4 below provides an overview of various government reports that have made a case against China and Huawei, citing national security risks.

An oft-cited document is the 2012 investigation report by the House Permanent Select Committee on Intelligence, which examined the national security issues posed by Chinese telecommunications companies Huawei and ZTE. In a two-step investigation, the committee first reviewed open source information on the companies and their ties to China's PLA government, and then, reviewed classified US intelligence to evaluate supply chain risk. The report found that the companies could not provide credible evidence to sufficiently establish their disassociation from Beijing's government. It recommended that US government systems, particularly sensitive systems, should not include equipment from Huawei and ZTE; and private sector entities should also consider long term security risks associated with doing business with them.

Table 4. An overview of U.S. government reports on China and Huawei

Year	Report	Department	Description
2011	Annual Report to Congress on Military and Security Developments Involving the People's Republic of China	U.S. Department of Defense	Underscored China's increasing civil and military integration, and how informational technology companies such as Huawei maintain close ties to the PLA. Such associations are believed to help advance China's defence industries.
2011	The National Security Implications of Investments and Products from the People's Republic of China in the Telecommunications Sector	United States China Economic and Security Review Commission	Telecommunications is labelled as a strategic industry in China; and Huawei retains a hybrid entity as a "national champion" that receives favourable treatment from Beijing.
2012	Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE	House Permanent Select Committee on Intelligence, US House of Representatives	Investigated the security threat posed by Chinese telecommunications companies with possible ties to the Chinese government or military.
2015, updated in 2018	Counterintelligence Note on Huawei	Federal Bureau of Investigation	Explored the possibility that Chinese Government-supported telecom equipment may be exploited through Chinese cyber activity, with intelligence services operating as a persistent threat to US networks. Beijing makes no secret that its cyber warfare strategy is predicated on controlling global communications network infrastructure.[43]

43 "Huawei", Counterintelligence Strategic Partnership Intelligence Note (spin), *Federal Bureau of Investigation*, March 2018, https://info.publicintelligence.net/FBI-Huawei-2018.pdf.

Year	Report	Department	Description
2019	Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress	Congressional Research Service	Evaluates different issues, including security, that the Congress should consider in framing policies for 5G deployment.
	The 5G Ecosystem: Risks & Opportunities for DoD	Defense Innovation Board	Highlights security risks associated with supply chain, infrastructure and 5G services (such as backdoors), should Chinese vendors become dominant suppliers of the technology.[44]
	National Security Implications of Fifth Generation (5G) Mobile Technologies	Congressional Research Service	Examines national security concerns related to 5G, and the risks associated with using Chinese 5G infrastructure.[45]

Washington, of course, wishes to be a leader in the deployment of 5G networks. The 2017 National Security Strategy (NSS) of the Trump Administration, identified that economic prosperity is an important pillar of national security, and places priority on improving America's digital infrastructure, including 5G networks.[46] Likewise, market analysts estimate that in the US, 5G could create up to 3 million new jobs and add $500 billion to the nation's gross domestic product (GDP).[47] As such, the US' Federal Communication Commission (FCC) released a comprehensive strategy in 2018 titled Facilitate America's Superiority in 5G Technology (the 5G FAST Plan) to support the deployment of the new network. The plan comprised three components, i.e. addressing spectrum allocation, infrastructure policy, and modernising outdated regulations. While full 5G coverage across the US is yet to be achieved, the GSMA's Mobile Economy North America 2019 report estimates that the US will be a leader in 5G adoption, and have 50 percent 5G connections by 2025.[48] Today, 5G is a reality in America and major mobile operators such as Verizon, AT&T, Sprint and T-Mobile have commercially launched 5G services across the US. The companies have used Nokia, Ericsson, Samsung and Qualcomm as their suppliers,[49] and none of them carried out trials with Huawei or have announced any contracts with Chinese companies.

At all stages of the process, Washington has placed immense emphasis on blocking Chinese technology companies. The FCC approved rules in November 2019 prohibit the use of public funds under the Universal Service Fund (USF) to purchase or obtain any equipment or services from Huawei and ZTE, which are deemed as companies

44 "The 5G Ecosystem: Risks & Opportunities for DoD", *Defense Innovation Board*, April 3, 2019 https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.

45 "National Security Implications of Fifth Generation (5G) Mobile Technologies", *Congressional Research Service,* June 12, 2019, https://assets.documentcloud.org/documents/6153171/IF11251.pdf.

46 "National Security Strategy of the United States of America", December 2017, 18-19, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

47 "Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress", *Congressional Research Service*, January 30, 2019, 7, https://fas.org/sgp/crs/misc/R45485.pdf.

48 "The Mobile Economy North America 2019", *GSMA Intelligence*, 2019, 6, https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_North_Am.pdf.

49 "The Mobile Economy North America 2019", *GSMA Intelligence*, 2019, 23, https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_North_Am.pdf.

that pose a national security threat to the integrity of communications networks and supply chain.[50] This could be costly for rural carriers, who may not only have to opt for expensive 5G equipment, but will also need to spend more on replacing existing Huawei and ZTE equipment from their networks.[51] The FCC announced a $9 billion rural 5G fund to solve this issue, but questions remain regarding its timely availability and disbursement.[52]

More troublesome for Huawei, was its 2019 entry in the US entity list, which imposes cumbersome license requirements for American companies that choose to do business with the Chinese telecom giant. The move will prevent US technology from being used by foreign-owned entities in ways that potentially undermine US national security or foreign policy interests.[53] Because of this measure, companies such as German chipmaker Infineon Technologies have suspended their shipment to Huawei from the US[54], while other companies like Micron Technology have said that this requirement will in turn hurt US tech competitiveness and reduce US market share in tech areas.[55]

Table 5 takes a look at extant mechanisms the US has put in place to restrict Huawei and ZTE within the US.

Table 5. Mechanisms to ban Huawei and ZTE from the U.S.

Year	Measure	Method
2018	Controlling foreign investment from China and expanding the government's authority to block transactions involving investments in critical technologies.	Implemented by the inter-agency Committee on Foreign Investment in the United States (CFIUS), and the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA).
2018	Ban on federal agencies and their contractors from using equipment from Huawei or ZTE on national security grounds.[56]	Amendment to the John S. McCain National Defense Authorization Act for Fiscal Year 2019

50 "Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs", *Federal Communications Commission*, November 26, 2019, 28-66, https://docs.fcc.gov/public/attachments/FCC-19-121A1.pdf.

51 Lily Hay Newman, "The FCC's Push to Purge Huawei From US Networks", *Wired,* December 10, 2019, https://www.wired.com/story/fcc-rip-replace-huawei-zte/.

52 *Ibid.*

53 "US blacklists Huawei, places it on entity list", *The Economic Times,* May 16, 2019, https://economictimes.indiatimes.com/news/international/business/us-blacklists-huawei-places-it-on-entity-list/articleshow/69353632.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

54 Cheng Ting-Fang and Lauly Li, "Germany's Infineon suspends US shipments to Huawei", *Nikkei Asian Review,* May 21, 2019, https://asia.nikkei.com/Economy/Trade-war/Germany-s-Infineon-suspends-US-shipments-to-Huawei.

55 Jenny Leonard and Ian King, "Five months after Huawei export ban, U.S. companies are confused", *Los Angeles Times,* October 24, 2019, https://www.latimes.com/business/story/2019-10-24/huawei-export-ban-us-companies-confusion.

56 John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, https://www.congress.gov/bill/115th-congress/house-bill/5515/text.

Year	Measure	Method
2019	Bar on US companies from doing business with companies subject to jurisdiction of "foreign adversaries". [57]	Executive Order under the Trump administration
	Huawei and 68 of its non-US affiliates added to the entity list. This list identifies entities that are involved in activities contrary to the national security or foreign policy interests of the United States, and imposes restrictive licensing requirements on them.[58]	Designation under the Entity list of the Export Administration Regulations (EAR)
	Prohibition on the use of Universal Service Fund to purchase or obtain any equipment or services from Huawei and ZTE	Rules issued by the Federal Communications Commission
2020	Established a mechanism to: (1) prevent communications equipment or services that pose a national security risk from entering US networks, and (2) a programme to remove any such equipment or services currently used in US networks. A reimbursement programme has been set up for small suppliers to offset the cost of removing and replacing prohibited equipment or services.	Secure and Trusted Communications Network Act of 2019

Other measures appear to be on the anvil, with a 2018 draft bill which aims to prohibit federal agencies from contracting with entities that use equipment from Huawei, ZTE or an entity reasonably believed to be owned or controlled by China.[59] In January 2020, Senator Tom Cotton introduced another bill that would stop the United States from sharing intelligence with countries that use Huawei equipment for their 5G networks.[60] In the same month, the "Secure 5G and Beyond Act of 2020" was introduced to call on the President to develop a strategy to ensure the security of next generation mobile telecommunications systems and infrastructure and to assist allies and strategic partners in maximising the security of similar systems, infrastructure, and software.[61]

Further, reports produced by major NGOs funded by the US government, such as Freedom House have produced research and analysis detailing Huawei's surveillance and possible interference in elections. Table 6 provides extracts from three such reports, alluding to the use of Huawei's tech to support undemocratic regimes.

57 "Executive Order on Securing the Information and Communications Technology and Services Supply Chain", The White House, May 15, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

58 "Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List", A Rule by the Industry and Security Bureau (United States Department of Commerce), August 21, 2019, https://www.federalregister.gov/documents/2019/08/21/2019-17921/addition-of-certain-entities-to-the-entity-list-and-revision-of-entries-on-the-entity-list.

59 "Defending U.S. Government Communications Act", H.R.4747 — 115th Congress (2017-2018), https://www.congress.gov/bill/115th-congress/house-bill/4747.

60 "Cotton Introduces Bill Banning Intelligence Sharing With Countries Using Huawei", Website of Tom Cotton (Arkansas Senator), January 8, 2020, https://www.cotton.senate.gov/?p=press_release&id=1288.

61 "Secure 5G and Beyond Act of 2020", H.R.2881 — 116th Congress (2019-2020), https://www.congress.gov/bill/116th-congress/house-bill/2881/text.

Table 6. *Freedom House* reports alleging Huawei's surveillance

Country	Year	Extracts from reports
Sri Lanka	2017	"State agencies are believed to possess some technologies that could facilitate surveillance... Digital activists in Sri Lanka believe Chinese telecoms ZTE and Huawei, who collaborated with Rajapaksa's government in the development and maintenance of Sri Lanka's ICT infrastructure, may have inserted backdoor espionage and surveillance capabilities."[62]
Uganda	2019	"...Huawei allegedly helped the government surveil prominent opposition Parliament member and presidential hopeful Robert Kyagulanyi, better known as Bobi Wine."[63]
Zambia	2019	"New reporting in 2019 revealed the close relationship between the Zambian government and Huawei, a Chinese tech company. Huawei apparently helps the Zambian government monitor communications, including online. In one case, Huawei helped identify and track the administrators of a Facebook page who were later arrested."[64]

Washington has also accused Huawei of intellectual property theft, economic espionage and violations of sanctions regime. These are part of a broader campaign against China, which allegedly uses these methods to rob, replicate and replace American technologies to promote domestic manufacturing and conquer global markets. According to indictments on misappropriation of intellectual property, Huawei adopts means such as violation of confidentiality agreements, recruitment of former IT employees, and use of proxies such as professors and researchers to obtain cutting edge technology. Table 7 provides an overview of indictments and lawsuits in the US against Huawei.

62 "Freedom on the Net: Sri Lanka", *Freedom House*, 2017, https://freedomhouse.org/country/sri-lanka/freedom-net/2017.

63 "Freedom on the Net: Uganda", *Freedom House*, 2019, https://freedomhouse.org/country/uganda/freedom-net/2019.

64 Freedom on the Net: Zambia", *Freedom House*, 2019, https://freedomhouse.org/country/zambia/freedom-net/2019.

Table 7. U.S. cases and indictments against Huawei and its personnel

Year	Description	Details
2003	Lawsuit against Huawei for intellectual property theft.	Filed by Cisco Systems, an American multinational technology conglomerate. The case was settled confidentially in 2004.
2017	Huawei was found liable for stealing robotic technology from T-Mobile, an American wireless network operator.	Outcomes of a lawsuit filed by T-Mobile
2019	US charges Huawei and its Chief Financial Officer, Meng Wanzhou, with evading U.S. sanctions against Iran.[65]	Indictment by the US Department of Justice
	Indictment against Huawei for attempting to steal design information from a T-Mobile robot.[66]	Indictment by the US Department of Justice
2020	Indictment against Huawei for racketeering conspiracy and conspiracy to steal trade secrets.[67]	Indictment by the US Department of Justice

While the US ban against Huawei has largely been based on risks of espionage and cyber-attacks, analysts have rightly discerned that the American push against Huawei is related to first mover advantage vis-à-vis China, political values, economic competitiveness and the setting of future technological standards.[68] Washington classifies China, as well as Russia, as revisionist powers, that wish to shape the world consistent with their authoritarian model and gain veto authority over other nations' economic, diplomatic, and security decisions[69]; it fears that this will magnify through Beijing's Huawei outreach and spread digital authoritarianism. The US also recognises the importance of obtaining first mover advantage; a 2019 report by the Defense Innovation Board notes that in 2G deployments, Europe gained the first competitive advantage and quickly advanced to deploying 3G at a time when US was still trying to implement 2G.[70] Lessons from history itself can be gleaned to understand and appreciate the role of technology in supporting a nation's economic and political power. Washington's own first mover advantage in developing and shaping the internet is also a case in point.

On the contrary, critics say that Washington's ruse against the Chinese company smacks of economic protectionism. A primary reason for this is that there is yet to be any concrete evidence or any evaluation of the Huawei's network equipment to determine that it is indeed equipped by backdoors. A bigger reason has been that allowing Huawei in domestic markets would build and count as tacit support

65 "Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged With Financial Fraud", Office of Public Affairs, The US Department of Justice, January 28, 2019, https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial.

66 *United States of America v. Huawei Device Co. Ltd. & Anr.*, Indictment No. CR19-010 RSM, January 16, 2019, https://www.justice.gov/opa/press-release/file/1124996/download.

67 "Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets", Office of Public Affairs, The US Department of Justice, February 13, 2020, https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering.

68 Kaan Sahin and Didi Kirsten Tatlow, "Berlin's Preliminary 5G Decision", *German Council on Foreign Relations*, DGAP Policy Brief No. 3, November 2019, 4, https://dgap.org/sites/default/files/article_pdfs/dgap_policybrief_nr3-nov2019_5g.pdf.

69 "Summary of the 2018 National Defense Strategy of United States of America", *U.S. Department of Defense*, 2018, 2, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

70 "The 5G Ecosystem: Risks & Opportunities for DoD", *op. cit.*, 6.

to Beijing's ambitions to be a global cyber power, and shift in global technological leadership from the US to China. The US stratagem, as supported by its allies such as Australia, is intended to be a containment strategy against China.

Currently, US homegrown companies such as Intel, Cisco and Qualcomm have smaller market shares as opposed to Huawei, and even Ericsson and Nokia. Perhaps this explains why the US is rallying behind Ericsson and Nokia, to establish them as feasible and attractive alternatives to Huawei. In late 2019, US government officials contemplated issuing credit to these companies to enable them to compete with Huawei.[71] Other voices within the US government; such as US Attorney General William Barr said that Washington should consider taking a "controlling stake" in Nokia and Ericsson, stating that putting America's "large market and financial muscle" behind the companies will make it a formidable competitor against Huawei.

The US ban on Huawei has been comprehensive, direct and unambiguous, and is based on both national security concerns, as well as the larger, ongoing geopolitical rivalry between Washington and Beijing, which has further intensified and moved to new areas–such as emerging technologies–since the trade war began.

B. The United Kingdom (UK)

In July 2018, UK's Department for Digital, Culture, Media & Sport (DCMS) released the Future Telecoms Review (FTR), which describes how 5G can generate significant economic benefit for the UK and sets the target of full coverage by 2027. [72] Through investments and a favourable policy environment—such as the 2017 UK Digital Strategy—the development and uptake of next generation digital infrastructure, including full fibre and 5G, has been swift.[73] Major UK telecom operators, namely EE, Vodafone UK, Three UK, and O2 UK have commercially launched 5G, where two operators—EE and Vodafone UK—have confirmed the use of Huawei equipment in their networks.[74] These developments took place well before the UK formally tendered its final decision on Huawei on 28 January 2020, which allows the Chinese company but directs its operators to limit its presence in 5G networks.[75]

The Huawei debate is not new to the UK; it has been aware of the risks associated with Huawei's gear as early as 2010. The discussion on risks associated with Huawei and its equipment have centred around the company's link to Beijing, risks in its equipment and implications for UK's national security. However, despite deeming the company as a "high risk vendor", London has refrained from imposing a ban and has, instead, chosen to allow it subject to special oversight and regulation. Resultantly, Huawei has a big presence in UK's 4G buildup and has the highest market share standing at 35 percent.[76]

---

71 Kiran Stacey, "US pushes to fund western rivals to Huawei", *Financial Times*, October 8, 2019, https://www.ft.com/content/94795848-e6e3-11e9-b112-9624ec9edc59.

72 "Future Telecoms Infrastructure Review", *Department for Digital, Culture, Media & Sport (United Kingdom)*, 2018, 1, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/732496/Future_Telecoms_Infrastructure_Review.pdf.

73 "UK Digital Strategy", Policy paper: Executive summary, March 1, 2017, https://www.gov.uk/government/publications/uk-digital-strategy/executive-summary.

74 "Vodafone's 5G UK service to launch in July", *BBC*, May 14, 2019, https://www.bbc.com/news/technology-48265421; Paul Sandle, "EE keeps Huawei in first British 5G network but halts handsets", *Reuters*, May 22, 2019, https://www.reuters.com/article/us-bt-5g/ee-keeps-huawei-in-first-british-5g-network-but-halts-handsets-idUSKCN1SS0SQ.

75 "NCSC advice on the use of equipment from high risk vendors in UK telecoms networks", *National Cyber Security Centre (United Kingdom)*, January 28, 2020, https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks#section_3.

76 "UK Telecoms Supply Chain Review Report", *Department for Digital, Culture, Media & Sport (United Kingdom)*, July 2019, 29, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf.

Various government reports acknowledge the theoretical potential for the Chinese state to exploit vulnerabilities in Huawei's equipment to intercept or disrupt UK communications, but none recommend prohibiting the company altogether. All reports observe: *firstly*, the focus of UK's cybersecurity concerns is not about one country, one company or the 'flag of origin' of the equipment,[77] but about building a resilient network that can withstand any attack from any corner. *Secondly*, it believes that blocking Chinese companies is impractical—given the predominance of Chinese manufactured and developed equipment—and is unlikely to result in the national security protection envisaged. *Lastly*, though risks cannot be entirely eliminated, they can be managed or mitigated through a range of measures, such as oversight, regulation, self-policing, and implementing a competitive, multi-vendor approach. The multi-vendor model has been fundamental to UK's reasoning to allow Huawei. It reduces dependence on one vendor and increases competition, both of which encourages vendors to improve their security standards and helps build resilience.

Table 8 below provides an overview of the discussion that has taken place in the UK, vis-à-vis Huawei, and its associated risks and vulnerabilities.

Table 8. UK government reports on risks associated with Huawei

Year	Document Title	Department	Description
2013	Foreign involvement in the Critical National Infrastructure: The implications for national security	Intelligence and Security Committee (British Parliament)	Telecom networks form a part of critical national infrastructure. With Huawei's entry in the UK telecom market, it examined common security concerns related to its equipment and proposed measures to manage possible risks.
2017	Cyber Security of UK Infrastructure	Parliamentary Office of Science and Technology	Box 5 of the document details supply chain risks from foreign involvement, notably Huawei, in UK's critical national infrastructure. There is potential for China to exploit vulnerabilities and disrupt/ intercept communications.

77 "Statement on 5G suppliers", Intelligence and Security Committee, http://isc.independent.gov.uk/files/20190719_ISC_Statement_5GSuppliers_Web.pdf?attredirects=0.

Year	Document Title	Department	Description
2019	Telecoms supply chain review	Department for Digital, Culture, Media & Sport	5G creates new challenges for security and resilience, including threats from hostile state actors who may exploit weaknesses in telecoms and carry out espionage, sabotage and destructive or disruptive cyberattacks. UK's National Cyber Security Centre (NCSC) has publicly attributed malicious cyber activity to China, Russia, North Korea and Iranian actors.[78]
	Statement on 5G suppliers[79]	Intelligence and Security Committee (British Parliament)	Gives an overview of the key technical and geopolitical issues arising from the Huawei question.
	5G Briefing Paper	House of Commons Library	Contains a chapter titled "5G and security" and details the risks associated with foreign involvement (particularly China) in telecommunications networks, and also looks at broader strategic and geopolitical concerns of UK's choice.

London has established specific institutional mechanism to manage risks associated with Huawei's kit. In 2010, through an arrangement between UK government and Huawei, the Huawei Cyber Security Evaluation Centre (HCSEC) was set up to mitigate risks arising from its involvement in UK's critical national infrastructure. However, the 2013 Intelligence and Security Committee report identified that the HCSEC was entirely funded by Huawei–an arrangement that raised questions regarding the credibility of its work. In 2014, the HCSEC Oversight Board, chaired by the Chief Executive Officer of the NCSC, was set up to report every year to the National Security Adviser (NSA), the Intelligence and Security Committee (ISC), the parliament and the public. Despite the fact that the reports from the Oversight Board (2018 and 2019)[80] raised some serious issues regarding Huawei's software engineering and cyber security capabilities, members from the government argue that the model has worked for the past eight years. They note that because of this mitigation model, the UK operators that use HCSEC have unparalleled information to help them manage the risk of using Huawei equipment.[81]

78 "UK Telecoms Supply Chain Review Report", *op. cit.,* 23.

79 "Statement on 5G suppliers", *op. cit.*

80 Annual Report 2019, Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, March 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf; Annual Report 2018, Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, July 2018, 2-4, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf.

81 Ian Levy, "Security, complexity and Huawei; protecting the UK's telecoms networks", *National Cyber Security Centre (United Kingdom),* February 22, 2019, https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks.

In addition to institutions, the UK has introduced or is proposing to introduce new law and policy measures related to investment and network security to further strengthen its 5G build-up. The most significant measure is the 2020 National Cyber Security Centre (NCSC) guidance on the use of equipment from high risk vendors, such as Huawei. The NCSC is a part of the Government Communications Headquarters (GCHQ)–the British intelligence agency–and provides advice, guidance and support on cyber security to the public and private sector. The directive effectively allows Huawei to build its 5G networks, and provides sufficient flexibility to carriers to determine how far and to what extent they will allow Huawei's equipment in core networks. Based on the guidance, mobile operators are recommended to exclude Huawei or other high risk vendors from, (1) security safety related and safety critical networks in Critical National Infrastructure, (2) security critical network functions and, (3) have a limited presence subject to the cap of 35 percent in remaining networks.[82] Table 9 summarises the measures that the UK has taken, or is planning to take to manage risks associated with Huawei's equipment.

Table 9. UK's measures to manage risks associated with Huawei

Year	Institution/ Measure	Description
2010	Huawei Cyber Security Evaluation Centre (HCSEC)	Opened under a set of arrangements between the UK government and Huawei to mitigate risks associated with Huawei and its presence in critical national infrastructure.
2014	HCSEC Oversight Board	Chaired by the Chief Executive Officer of the NCSC, and an executive member of GCHQ's (Government Communications Headquarters) Board with responsibility for cyber security. Publishes yearly reports on whether the HCSEC is complying with its mandate.
2018	Amendment to the Enterprise Act 2002	Enables ministers to scrutinise mergers in the economy on national security grounds that previously fell outside the scope of the Act. These measures amend the thresholds for the turnover and share of supply tests within the Enterprise Act for military and dual use technologies, quantum technology, and computing hardware.[83]
2018	National Security and Investment: A consultation on proposed legislative reforms	A consultation process to reform the UK's powers to protect national security from hostile actors using ownership of, or influence over, businesses and assets to harm the country.[84] The consultation will aid the introduction of primary legislation in this regard.

82 "NCSC advice on the use of equipment from high risk vendors in UK telecoms networks", *op. cit.*; UK telecommunications: Written statement - HCWS70, Department for Digital, Culture, Media and Sport, UK Parliament, January 28, 2020, https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2020-01-28/HCWS70/.

83 Reply by the UK Cabinet Office to Question on "Foreign Investment in UK: Infrastructure: Written question – 183493", UK Parliament, October 24, 2018, https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2018-10-24/183493/.

84 UK Department for Business, Energy & Industrial Strategy, *National Security and Investment: A consultation on proposed legislative reforms*, (London: 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/728310/20180723_-_National_security_and_investment_-_final_version_for_printing__1_.pdf.

Year	Institution/ Measure	Description
2020	NCSC advice on the use of equipment from high risk vendors in UK telecoms networks	It sets out how NCSC will determine whether a vendor is high risk, the precise restrictions it advises should be applied to high risk vendors in the UK's 5G and full fibre networks, and what mitigation measures operators should take when using high risk vendors.
Proposed	UK Telecom Security Requirements (TSR)	The purpose of the Telecoms Security Requirements (TSR) is to ensure that providers of public electronic communications networks and services take appropriate and proportionate measures to prevent, remove or manage risks posed to the security of networks and services. The TSR will be first introduced as a regulation and will then become a law.

Regardless of these rigorous mechanisms, the UK government faced increasing pressure from the US over the last year to ban Huawei in its 5G networks. Box 1 takes a look at statements from government personnel and diplomats from both Beijing and Washington, on the UK's 5G decision. Opposition to Huawei's entry in 5G also came from a group of senior Conservatives in the UK Parliament who tabled an amendment to the Telecommunications Infrastructure (Leasehold Property) Bill in March 2020, to end Huawei's involvement in UK networks by 2022.[85] This Bill, however, was defeated by the government.

A major influencing factor for UK's decision was its membership of the Five eyes partnership, a Cold War era intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States. The alliance is important to the UK; in a BBC interview PM Boris Johnson said that he would not want to "prejudice" the country's ability to share intelligence among the Five eyes alliance members. Additionally, this decision for London also came at a time when its process of exit from the European Union (or "Brexit") meant that its policies needed to maintain and balance its ties with both the US and China. With Brexit, London would want to reinforce its economic relations with China to hedge its economic and political impact. At the same time, however, its exit from the EU means that the single market will no longer rally behind London, thereby affecting its ability to mitigate China's potential to retaliate and exert pressure.[86]

85 Lizzy Buchan, "Boris Johnson facing Tory revolt over Huawei 5G decision", *Independent,* March 6, 2020, https://www.independent.co.uk/news/uk/politics/boris-johnson-huawei-5g-decision-trump-tories-a9380561.html.

86 Janka Oertel, "Europe and China after Brexit: The 5G question", *European Council on Foreign Relations,* December 19, 2019, https://www.ecfr.eu/article/commentary_europe_and_china_after_brexit_the_5g_question.

Box 1. US and China's statements on UK's 5G dilemma

US National Security Adviser, Robert O'Brien (December 2019): "They are just going to steal wholesale state secrets, whether they are the UK's nuclear secrets or secrets from MI6 or MI5... It is somewhat shocking to us that folks in the UK would look at Huawei as some sort of a commercial decision. 5G is a national security decision."
China's Ambassador Liu Xiaoming's article in *The Sunday Telegraph* (January 2020): "To wall off Huawei would be to move against a new round of technological revolution, which could lead to serious loss in time, expense and competitiveness... banning Huawei equipment would delay Britain's 5G, leaving it trailing far behind in this latest industrial revolution. The image of Britain as an open and inclusive partner for cooperation would also bear the brunt. So would the confidence of foreign investors and the cooperation between China and the UK."
US Secretary of State, Mike Pompeo said that Britain has a chance to "relook" its decision to allow Huawei and "...our view is that we should have western systems with western rules, and American information only should pass through trusted networks, and we'll make sure we do that." (January 2020)
China's ambassador to the UK, Liu Xiaoming (February 2020): "I think what they are doing is a kind of a witch-hunt...Huawei is a private-owned company, nothing to do with the Chinese government... the only problem they have is they are a Chinese company."

Government officials from the UK have said that the 5G debate should not be characterised as a "pro-China" or "anti-China" one.[87] London's policy on Huawei is a technical decision and it has been taken with due consideration to the existing mechanism to monitor Huawei's equipment, and its robust security policy to combat cyberattacks. What this means for the UK's relationship with the US remains to be seen; while the Trump administration has been particularly vocal about its disappointment in the UK, a new dispensation in Washington post the 2020 elections may approach the matter differently. At the same time, Huawei has not been entirely satisfied by the UK's approach to high risk vendors in its January 2020 guidance. While this may not be enough to invite any form of reproach from Beijing–given how big markets like the US have entirely shut out Huawei–the PRC government may have leverage to push the UK to further improve Huawei's role in 5G networks.

C. Canada

According to the GSMA's 2019 Mobile Economy North America report, Canada is also well positioned to deploy 5G on a large scale and will reach a 42-percent adoption rate by 2025. [88] 5G promises to deliver immense economic benefits to Ottawa by 2026 and can create 2,50,000 permanent jobs and lead to an annual increase of nearly $40 billion to its gross domestic product.[89] To date, Rogers communication, a top carrier in Canada, has commercially launched 5G in four cities (Vancouver, Toronto, Ottawa and Montreal) in partnership with Ericsson.[90]

87 "Statement on 5G suppliers", *op. cit.*

88 "The Mobile Economy North America 2019", *GSMA Intelligence*, 2019, 6, https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_North_Am.pdf.

89 Loprespub, "5G Technology: Opportunities, Challenges and Risks", *HillNotes,* Library of Parliament, February 13, 2020, https://hillnotes.ca/2020/02/13/5g-technology-opportunities-challenges-and-risks/.

90 "Rogers Starts Rollout of Canada's First 5G Network and Joins Global 5G Forum", *Rogers,* January 15, 2020, https://about.rogers.com/news-ideas/rogers-starts-rollout-of-canadas-first-5g-network-and-joins-global-5g-forum/.

However, Canada is yet to decide on the question of allowing Chinese suppliers to build its 5G network. It is currently undertaking a comprehensive security review of Huawei's potential role in 5G, and several agencies, such as Public Safety Canada, the Canadian Security Intelligence Service, the Communications Security Establishment, Global Affairs, and Innovation, Science and Economic Development are taking part in it.[91]

The debate has also been ongoing in the Canadian Parliament. A January 2020 parliamentary research document on 5G technology discusses the risks associated with Huawei's equipment, such as security breaches and its possible use for espionage and surveillance. [92] Another platform for the 5G discussion has been the House of Commons standing committee on Public Safety and National Security, which released a report on "Cybersecurity in the Financial Sector as a National Security Issue" in June 2019. Here, the report explicitly discusses 5G, Huawei and its impact on the cyber supply chain security. In its discussions, members of the academia who testified in the committee proceedings, brought forth various contentions related to Huawei, such as IP theft, China's national intelligence laws, and the close connection between the company and the Chinese government.[93] Canada's Communications Security Establishment (CSE)—the nation's cryptologic agency said that it will follow a multi-vendor approach and a zero trust philosophy with reference to all equipment.

However, not all stakeholders agree on what would be the best for Canada. For instance, Canada's intelligence agencies, namely the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE) have reportedly been divided on this issue. While the CSE considers this as a manageable technical question, CSIS is opposed to opening the door to possible espionage.[94] Leading telecom operators in Canada have also been keen on collaborating with Huawei for 5G networks. In February 2020, mobile operator Telus Corporation announced that it plans to use Huawei equipment in its 5G build-up.[95] On the other hand, though Bell Canada Enterprises (BCE) Inc. has signed an agreement with Nokia, it wants to keep the option of Chinese firms[96]open and is waiting to hear from the government's security review[97].

---

91 Jim Bronskill, "Looming Huawei 5G decision puts Trudeau government under mounting political pressure", *Financial Post,* January 2, 2020, https://business.financialpost.com/technology/political-pressure-mounts-as-ottawa-moves-closer-to-5g-decision-on-huawei.

92 Loprespub, "5G Technology: Opportunities, Challenges and Risks", *HillNotes,* Library of Parliament, February 13, 2020, https://hillnotes.ca/2020/02/13/5g-technology-opportunities-challenges-and-risks/.

93 "Cybersecurity in the Financial Sector as a National Security issue", Committee Report No. 38, Standing Committee on Public Safety and National Security, House of Commons (Canada), June 20, 2019, https://www.ourcommons.ca/DocumentViewer/en/42-1/SECU/report-38/page-102#26.

94 David Ljunggren, "Canada, isolated over Huawei 5G, is studying British decision", *Reuters*, January 29, 2020, https://www.reuters.com/article/us-usa-huawei-tech-canada/canada-isolated-over-huawei-5g-is-studying-british-decision-idUSKBN1ZR2JJ.

95 "Telus plans rollout of 5G network using Huawei technology", *CBC News,* February 13, 2020, https://www.cbc.ca/news/business/telus-5g-huawei-1.5462994.

96 James McLeod and Vanmala Subramaniam, "BCE Inc. announces Nokia as 'first' 5G partner, hikes dividend 5%", *Financial Post,* February 6, 2020, https://business.financialpost.com/technology/bell-signs-5g-partnership-with-nokia-hikes-dividend-as-earnings-rise.

97 Michael Bellusci, *Financial Post,* January 6, 2020, "BCE's new CEO calls Huawei's equipment 'top notch' and wants option to work with them on 5G", https://business.financialpost.com/telecom/huawei-equipment-top-notch-says-new-ceo-of-canadian-telco-bce.

Regardless, as Canada deliberates upon the 5G question, it continues to face pressure from the US to drop Huawei. In November 2019, US President Donald Trump's national security advisor Robert O'Brien likened the inclusion of Huawei infrastructure into Canada's future 5G network to a "Trojan Horse."[98] Ottawa, of course, has a strong imperative to maintain its relationship with its immediate neighbour given their shared history and values, and extensive commercial ties. However, the dichotomy between the priorities of the Trump administration and the Trudeau government, irritants pertaining to areas–such as the NAFTA renegotiations–continue to impede bilateral relations.

At the diplomatic level, however, Canada has become deeply embroiled in the geopolitical confrontation between US and China. In December 2018, on the basis of an extradition request from the US, Canada arrested Meng Wanzhou, Huawei's Chief Financial Officer and daughter of Huawei CEO Ren Zhengfei, on allegations of violating Iran sanctions. This move angered Beijing, and two Canadians working in China (Michael Kovrig and Michael Spavor) were arrested soon after on accusations of endangering national security–a move widely seen as retaliation against Canada's government.[99] Canadian Prime Minister Justin Trudeau made efforts to diffuse political tensions surrounding the issue and maintains that Canada "will abide by the rule of law" in this extradition case.[100] In January 2019 he went so far as to fire the then Canadian Ambassador to China, John McCallum who commented that Meng could make a "good case against extradition", which was clearly a political statement.[101]

However, Meng's arrest prompted further action from Beijing in the form of trade restrictions on major Canadian exports. This means that Ottawa's economic and trade priorities will be an important factor in its decision going forward. China is Canada's second largest export destination (following the US), and its merchandise trade to Beijing has been steadily increasing over the years (See Figure 2).

Beijing has been central to Trudeau's trade diplomacy. In the third Canada-China Annual Leaders' Dialogue, Trudeau and China's Premier Li Keqiang committed to double agricultural trade by 2025 and to continue exploratory discussions towards a potential comprehensive trade agreement.[102] Canola seeds and wood pulp,

98 David Lao, "'Trojan Horse': Trump's national security advisor warns Canada against Huawei's 5G", *Global CA,* November 23, 2019, https://globalnews.ca/news/6209240/huawei-national-security-halifax/.

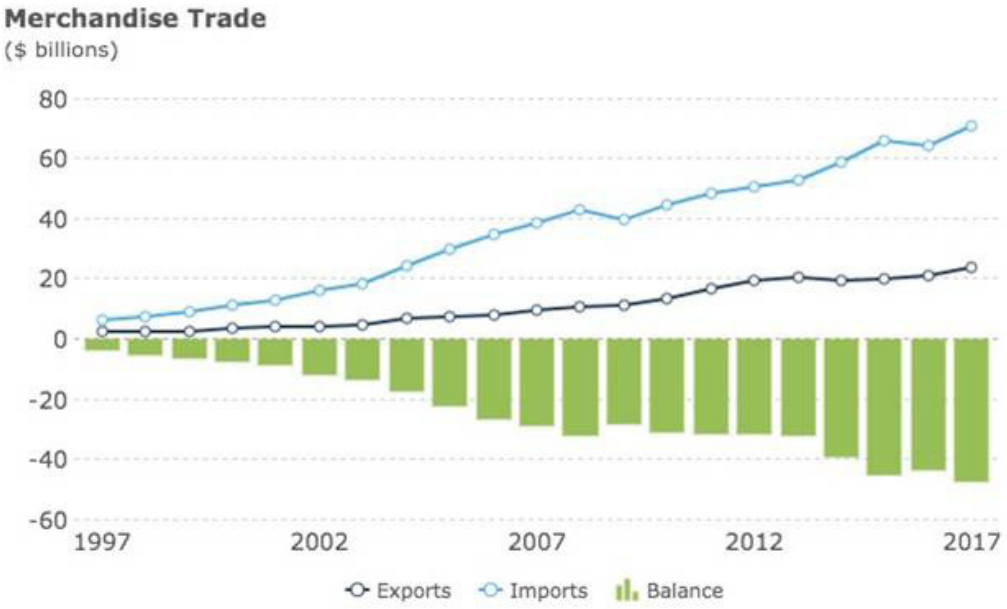
99 Chris Buckley, Javier C. Hernández and Dan Bilefsky, "China Arrests 2 Canadians on Spying Charges, Deepening a Political Standoff", *The New York Times,* May 16, 2019, https://www.nytimes.com/2019/05/16/world/asia/china-canadian-arrested.html.

100 Michael Taube, "Trudeau and Trump Team Up on China", *The Wall Street Journal*, January 30, 2020, https://www.wsj.com/articles/trudeau-and-trump-team-up-on-china-11580428513.

101 *Ibid.*

102 "Prime Minister announces strengthened partnership with China", Justin Trudeau, Prime Minister of Canada, November 14, 2018, https://pm.gc.ca/en/news/news-releases/2018/11/14/prime-minister-announces-strengthened-partnership-china.

Fig 2. Canada's merchandise trade with China



Source: Marie Dumont, "Canadian Trade and Investment Activity: Canada–China", Economics, Resources and International Affairs Division, Library of Parliament, November 16, 2018, https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/TradeAndInvestment/2018588E

together account for 21.4 percent of the total value of Canadian exports to China, with Canola seeds alone accounting for $2.6 billion in exports in 2016 (See, fig. 3). Doubling two-way trade will provide a permanent solution to Canadian canola exporters and ensure market access to China.[103] This would be massive benefit for the country's canola farming industry which employs 43,000 canola farmers, contributes $26.7 billion to the Canadian economy each year, and provides more than 250,000 Canadian jobs and $11.2 billion in wages.[104]

Unfortunately, the progress on trade liberalisation was halted when Beijing banned meat products and canola imports from Canada in 2018 and 2019 respectively. Coincidentally, these measures were imposed by Beijing soon after Meng's arrest in Canada. The canola and meat restrictions now apply on C$4.9 billion in Canadian shipments, putting almost one-fifth of total exports to the country from Canada at risk.[105] Given the impact of the ban on Canola seed producers, Ottawa in September 2019 filed a complaint against China before the World Trade Organization (WTO).[106]

With due regard to the factors at play, Canadian Public Safety Minister Bill Blair said that the Huawei decision is a complex one, where both economic and security

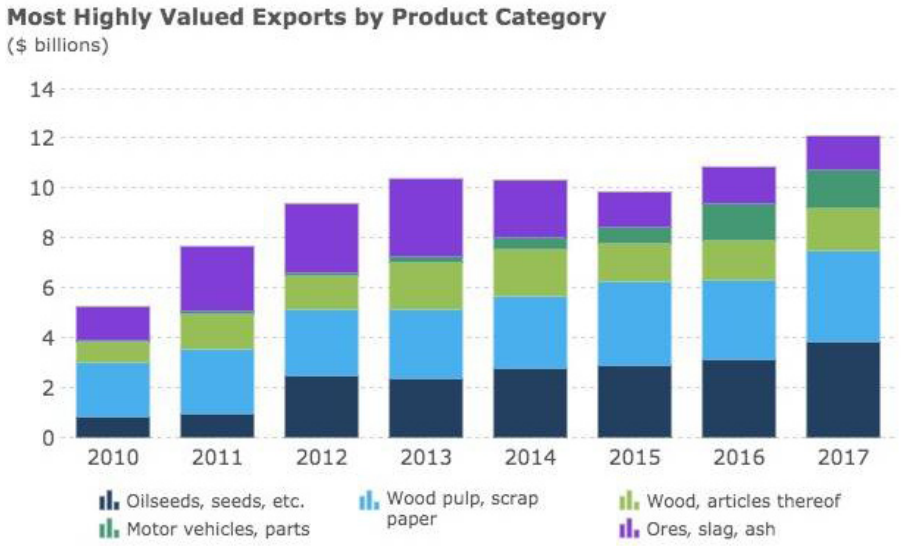
103 Theophilos Argitis, "Canada, China Deepen Ties With Trade Talks and Canola Deal", *Bloomberg,* September 22, 2016, https://www.bloomberg.com/news/articles/2016-09-22/trudeau-says-canada-china-exploring-possible-free-trade-talks-itek0u2e.

104 "Industry Overview", *Canola Council of Canada*, accessed March 26, 2020, https://www.canolacouncil.org/markets-stats/industry-overview/.

105 Erik Hertzberg and Theophilos Argitis, "Trudeau's Chinese Trade Headache Worsens With Meat-Export Ban", *Bloomberg,* June 28, 2019, https://www.bloomberg.com/news/articles/2019-06-27/trudeau-s-chinese-trade-headache-worsens-with-meat-export-ban.

106 China — Measures Concerning the Importation of Canola Seed from Canada (DS589), World Trade Organization, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds589_e.htm.

Fig. 3: Canada's most highly valued exports by category to China



Source: Marie Dumont, "Canadian Trade and Investment Activity: Canada–China", Economics, Resources and International Affairs Division, Library of Parliament, November 16, 2018, https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/TradeAndInvestment/2018588E

issues need to be addressed.[107] In a strongly worded statement, Navdeep Bains, Canada's Minister of Innovation, Science and Industry, said that Ottawa will not be "bullied by other jurisdictions" and will make a decision based on national interest.[108] As of 29 January 2020, Blair noted Canada's interest in examining the British decision on Huawei and said that it will carefully make its own assessment of potential security risks.[109]

As Ottawa deliberates upon the 5G dilemma, factors such as its membership of the Five eyes and its extensive commercial, diplomatic and military ties with the US will play an important influencing factor. At the same time, Canada is the only country that is facing actual repercussions by being caught between the standoff between the UK and China, in relation to Meng Wanzhou's arrest. The Trudeau government faces tough choices ahead, and here, it may indeed be useful to study UK's decision, which can be seen as a middle ground between either banning the company or allowing it in its entirety.

D. Australia

In October 2017, the Australian Department of Communications and the Arts launched its 5G strategy titled "5G—Enabling the future economy" which recognises its role in enabling productivity and innovation, and enunciates that its rollout will produce far-reaching economic and social benefits and support growth of Australia's digital economy.[110] While discussing telecommunications regulatory arrangements, the strategy notes that cybersecurity will be critical to 5G, and that

107 Catharine Tunney, "New public safety minister says Huawei 5G review 'a priority' but offers no timeline", *CBC News,* November 21, 2019, https://www.cbc.ca/news/politics/5g-huawei-china-bill-blair-1.5367002.

108 Kait Bolongaro, "Bains Says Canada 'Won't be Bullied' on Huawei 5G", *Bloomberg*, March 6, 2020, https://www.bloomberg.com/news/articles/2020-03-06/trudeau-minister-says-canada-won-t-be-bullied-on-huawei-5-g?sref=NDAgb47j.

109 Theophilos Argitis, "U.K. Huawei Decision Needs 'Careful Examination' Canada Says", *Bloomberg*, January 29, 2020, https://www.bloomberg.com/news/articles/2020-01-28/u-k-huawei-decision-needs-careful-examination-canada-says.

110 "5G—Enabling the future economy", Department of Infrastructure, Transport, Regional Development and Communications (Australian Government), October 2017, 1, https://www.communications.gov.au/documents/5g-enabling-future-economy.

the government will take steps to assess cybersecurity and privacy issues for the network.[111]

Consequently, security has been central to Australia's conversation on 5G networks. In addition to security risks, strategic and geopolitical concerns also contributed to the government decision to ban Huawei from Australia's 5G infrastructure projects. Canberra and Washington are old allies, beginning their bilateral relations during the Cold War era and have continued to strengthen them over the years. While Australia recognises the importance of its trade and investment partnership with China, it is cautious of its approach towards the South China Sea and the Indo-Pacific.

With respect to 5G, in August 2018, Canberra banned "high risk vendors" and expressed concerns regarding the involvement of vendors who could be subject to extrajudicial directions from a foreign government, and that this may risk failure by the carrier to protect its network from unauthorised access or interference. The statement did not explicitly name a vendor, but Huawei Australia confirmed in a tweet that both Huawei and ZTE have been banned from providing 5G technology to Australia.[112] This development subsequently lead to closing of Huawei's $60 million research and development centre in Victoria, citing uncertainty in federal regulatory changes and the ongoing "negative environment".[113]

On the same date, the Telecommunications Sector Security Reforms (TSSR) was introduced to empower the Ministry of Home Affairs and obligate telecom operators to take steps to ensure security and resilience of Australia's telecommunications infrastructure. From 18 September 2018, TSSR imposed legal obligations on carriers, carriage service providers and carriage service intermediaries to comply with its provisions.[114] The Australian Parliament is also considering amending its key telecommunications laws to establish a regulatory framework to manage national security risks of espionage, sabotage and foreign interference to telecommunications networks and facilities.[115] Previously, in mid-2018, the Australian government also passed the National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018[116] to revamp a package of counterintelligence laws and introduce tough penalties against espionage activities–such as interference in public infrastructure–and combat foreign interference.[117] While official statements express that the amendment is not designed to target a country, China's response to the amendment was lukewarm with Lu Kang, spokesman for the Chinese Foreign Ministry, stating that countries should "…cast off Cold War mind-set" and "strengthen exchanges and cooperation on the basis of mutual respect and equal treatment".[118] Key requirements of the TSSR are given in Box 2 below:

---

111 *Ibid.*, 12.

112 Michael Slezak and Ariel Bogle, "Huawei banned from 5G mobile infrastructure rollout in Australia", *ABC News,* August 23, 2018, https://www.abc.net.au/news/2018-08-23/huawei-banned-from-providing-5g-mobile-technology-australia/10155438.

113 Jewel Topsfield, "Huawei closes research centre in Victoria blaming 'negative environment'", *The Sydney Morning Herald,* August 12, 2019, https://www.smh.com.au/national/huawei-closes-research-centre-in-victoria-blaming-negative-environment-20190812-p52gdi.html.

114 "Telecommunications Sector Security - Frequently Asked Questions", Critical Infrastructure Centre (Australian Government), accessed March 25, 2020, https://cicentre.gov.au/tss/faqs.

115 Telecommunications and Other Legislation Amendment Bill 2017, Parliament of Australia, https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=s1051.

116 National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018, No. 67, 2018, Federal Register of Legislation, Australian Government, accessed March 27, 2020, https://www.legislation.gov.au/Details/C2018A00067.

117 Evelyn Douek, "What's in Australia's New Laws on Foreign Interference in Domestic Politics", *Lawfare,* July 11, 2018, https://www.lawfareblog.com/whats-australias-new-laws-foreign-interference-domestic-politics.

118 Damien Cave and Jacqueline Williams, "Australian Law Targets Foreign Interference. China Is Not Pleased.", *The New York Times*, June 28, 2018, https://www.nytimes.com/2018/06/28/world/australia/australia-security-laws-foreign-interference.html

Box 2. Australia's Telecommunications Sector Security Reforms[119]

Security obligation All carriers, carriage service providers and carriage service intermediaries are required to do their best to protect networks and facilities from unauthorised access and interference–including a requirement to maintain 'competent supervision' and 'effective control' over telecommunications networks and facilities owned or operated by them.
Notification requirement Carriers and nominated carriage service providers are required to notify government of proposed changes to their networks and services that could compromise their ability to comply with the security obligation.
Information gathering power The Secretary of the Department of Home Affairs has the power to obtain information and documents from carriers, carriage service providers and carriage service intermediaries, to monitor and investigate their compliance with the security obligation.
Directions power The Minister for Home Affairs has a new directions power to direct a carrier, carriage service provider or carriage service intermediary to do, or not do, a specified thing that is reasonably necessary to protect networks and facilities from national security risks.

Australia, thus, effectively banned Huawei and ZTE from the country. The question which arises is whether the ban was introduced because of Washington's diplomatic pressure–courtesy Australia's membership in the Five eyes, or whether the decision was taken by Canberra on its own account. News reports mention that in February 2018, former Australian Prime Minister Malcolm Turnbull was briefed on US concerns about Chinese involvement in 5G networks,[120] following which Huawei's involvement was given a full national security assessment by the Home Affairs department.[121] However, in April 2019, Turnbull publicly declared that it was he who had discussed the issue with President Trump and members of his administration on various occasions.[122] In 2017, Simeon Gilding, a former intelligence official with the Australian Signals Directorate (ASD)–a government agency responsible for foreign signals intelligence–studied the risks associated with Huawei's equipment.[123] The ASD recommended that given how Huawei originates from China, it would be much easier for cyber offensive teams in China to penetrate the network; as such, a ban was essential as there was no way to mitigate this particular risk. The potential to infiltrate and compromise Australia's critical infrastructure–from electrical power to water supply–could do vast economic damage to the country. The assertion that

119 "Telecommunications Sector Security – About", Critical Infrastructure Centre (Australian Government), accessed March 25, 2020, https://cicentre.gov.au/tss/about.

120 John Kehoe, Angus Grigg and Lisa Murray, "US warns Malcolm Turnbull not to use Huawei for 5G network", *Financial Review,* February 24, 2018, https://www.afr.com/policy/economy/us-warns-turnbull-not-to-use-china-for-5g-network-20180223-h0wkcl.

121 Angus Grigg and Lisa Murray, "China's Huawei gets full security check on involvement with 5G phone networks", *Bloomberg*, February 26, 2018, https://www.afr.com/companies/telecommunications/chinas-huawei-getsfull-security-check-on-involvement-with-5g-phone-networks-20180226-h0wniw.

122 "American Australian Association Veterans' Lunch", Speech of Mr. Malcolm Turnbull, the 29th Prime Minister of Australia 2015-2018, April 25, 2019, https://www.malcolmturnbull.com.au/media/american-australian-association-veterans-lunch.

123 Nick McKenzie and Anthony Galloway, "The man who stopped Huawei: A former spook speaks out", *The Sunday Morning Herald,* January 31, 2020, https://www.smh.com.au/national/the-man-who-stopped-huawei-a-former-spook-speaks-out-20200131-p53wi6.html.

Australia was the first to sound the Huawei alarm has been mentioned in various news reports.[124]

However, this is not the first time that Canberra has taken such action against Huawei–in 2012, Huawei was blocked from tendering for contracts in Australia's $38 billion National Broadband Network (NBN) due to cyber security concerns. The NBN project aimed to connect 93 percent of Australian homes and workplaces with optical fibre, providing broadband services in urban and regional areas.[125]

Both China and Huawei responded negatively to the present ban, with Huawei warning that the ban could cost Canberra 1,500 contracting jobs. A Huawei-sanctioned Oxford Economics report puts forth that by banning the company, Australian economy will lose US$8.2 billion, while three million Australians—mostly in rural and regional areas—will miss out on access to 5G technology by 2023.[126] China raised objections to the ban before the WTO's Council for Trade in Goods, terming it as discriminatory market access prohibition on 5G equipment.

The loss of a major equipment supplier from the market has had its own implications for carriers. While Australia's largest telecom operators, Optus Mobile and Telestra commercially launched 5G in November 2019 with Ericsson as their supplier,[127] Vodafone Hutchison Australia (VHA), another leading telecom operator in Australia, stated that the government's decision has set it back by 12 months. Its use of Huawei in existing networks will be phased out; and it has signed a new five-year deal with Nokia to supply equipment for its 5G rollout.[128]

Nonetheless, the Australian government has been confident about its decision. It has also expressed scepticism about UK's position on the 5G dilemma, which has chosen to manage risks associated with Huawei by limiting its presence in 5G networks. In an official statement, Huawei's Australian CEO confirmed that the Chinese company has given up involvement in Australia's 5G network and will "abide by the rules and regulations of the country in which it is operating".[129] The full consequence of the Huawei ban on Australia's 5G market–if any–can only be determined with time.

---

124 Cassell Bryan-Low, Colin Packham and et. al., "Special report - Hobbling Huawei: Inside the U.S. war on China's tech giant", *Reuters*, May 21, 2019, https://www.reuters.com/article/us-huawei-usa-5g-specialreport/special-report-hobbling-huawei-inside-the-u-s-war-on-chinas-tech-giant-idUSKCN1SR1EU; Danielle Cave, "Australia and the great Huawei debate: risks, transparency and trust", *The Strategist,* Australian Strategic Policy Institute, September 11, 2019, https://www.aspistrategist.org.au/australia-and-the-great-huawei-debate-risks-transparency-and-trust/.

125 Maggie Lu Yueyang, "Australia blocks China's Huawei from broadband tender", *Reuters*, March 26, 2012, https://www.reuters.com/article/us-australia-huawei-nbn/australia-blocks-chinas-huawei-from-broadband-tender-idUSBRE82P0GA20120326.

126 Byron Connolly, "3 million Australians won't get 5G: Oxford Economics", CIO, January 20, 2019, https://www.cio.com/article/3515028/3-million-australians-won-t-get-5g-oxford-economics.html.

127 "Optus launches 5G in Australia", *Ericsson,* November 28, 2019, https://www.ericsson.com/en/news/2019/11/optus-partners-with-ericsson-for-5g; Catherine Sbeglia, "5G in the land down under: Australia after Huawei ban", *RCR Wireless,* September 10, 2019, https://www.rcrwireless.com/20190910/5g/5g-australia-huawei-ban.

128 Jennifer Duke, "Vodafone signs Nokia for 5G, Huawei sites to be scaled back", *The Sunday Morning Herald,* December 30, 2019, https://www.smh.com.au/business/companies/vodafone-signs-nokia-for-5g-huawei-sites-to-be-scaled-back-20191230-p53ni6.html.

129 "Huawei Throws In The 5G Towel Down Under", *Channel News,* March 11, 2020, https://www.channelnews.com.au/huawei-throws-in-the-5g-towel-down-under/.

CHAPTER 3.

Key Concerns in Major Geographical Regions

A. Europe

Europe not only represents a fragmented response to the 5G dilemma, but has also refrained from rallying behind the US' calls to ban Huawei. This coincides with the challenges being faced by the European Union's (EU) enduring transatlantic partnership with the US, such as Trump's criticism of the North Atlantic Treaty Organization (NATO), withdrawal from the Iran nuclear deal, ongoing bilateral trade disputes,[130] and the European proposal to introduce the digital services tax—a measure that would impact major American companies like Google and Facebook.[131]

European countries have the largest number of commercial 5G launches, standing at 22 out of the 60 commercial launches across the world.[132] These launches have taken place in Austria, Finland, Germany, Ireland, Italy, Monaco, Portugal, Spain, Switzerland, Hungary, Latvia, and Romania. As many as 181 5G trials have taken place in the EU alone, where several telecom operators from countries such as Germany, Finland and Switzerland have conducted trials with Huawei.[133]

Within Europe, the EU–now comprising 27 member states (Fig. 4) following UK's exit–has taken measures to coordinate the efforts of individual member states for both 5G deployment and cybersecurity. Given the steps taken by the EU for a concerted approach towards establishing a seamlessly connected Europe, this section will first examine the EU's response to Huawei and its associated risks, followed by the responses of its individual 27 member states, and will lastly focus on countries outside the EU's single market.

European Union

For the EU, the 5G and Huawei question has been central to its efforts to adopt a joint approach towards network deployment, cybersecurity risk assessment and framing mitigation strategies. The reason for such efforts is simple; 5G is recognised as a key asset to help Europe compete in the global market, and cybersecurity is not only essential to protect economies and societies, but is also crucial for the strategic autonomy of the Union. The EU has recognised that a lack of coordination in national rollouts of 5G increases risk of fragmentation in standards and spectrum availability; and will "delay the creation of critical mass" to enable innovation in the digital single market (DSM).[134]

---

130 "U.S.-European Relations in the 116th Congress", *Congressional Research Service,* February 5, 2020, https://fas.org/sgp/crs/row/IF11094.pdf.

131 Alan Rappeport and Jim Tankersley, "Digital Tax Fight Emerges as Global Economic Threat", *The New York Times,* February 22, 2020, https://www.nytimes.com/2020/02/22/us/politics/digital-tax-economy-europe-united-states.html.

132 "5G & LTE deployments", *5G Americas,* accessed March 27, 2020, https://www.5gamericas.org/resources/deployments/.

133 "Major European 5G Trials and Pilots", *European 5G Observatory,* accessed March 27, 2020, https://5gobservatory.eu/5g-trial/major-european-5g-trials-and-pilots/.

134 "5G for Europe: An Action Plan", Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, COM 588 (2016) final, September 14, 2016, 3, https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-588-EN-F1-1.PDF.

The DSM strategy–released in 2015–refers to the free movement of goods, persons, services and capital in the EU, where every individual and business can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence.[135] Achieving a DSM will ensure that Europe maintains its position as a world leader in the digital economy, and help European companies grow globally. A concerted approach to 5G is also essential for achieving its 2016 goal of a European "Gigabit society", which envisages access to 1Gbps broadband for all institutional entities, access to 100Mbps broadband for all households and mobile broadband coverage for all.[136] With the purpose to realise these objectives, the EU set out to frame a coordinated approach towards 5G networks deployment.

As such, the following table presents an outline of major EU-level initiatives, such as funding and strategies, to boost and coordinate 5G deployments.

Table 10. EU initiatives, documents and programmes to support 5G deployment

Year	Initiative and description
2013	5G Infrastructure Public Private Partnership (5G PPP): a €1.4 billion ($1.5 billion) initiative to create the next generation of communication networks and services.
2015	A Digital Single Market Strategy for Europe: will bring down barriers and allow seamless access to online activities for individuals and businesses; contribute an additional €415 billion ($450 billion) to European GDP.[137]
2016	5G for Europe Action Plan:[138] an initiative for all stakeholders to make 5G a reality by 2020.
	Connectivity for a Competitive Digital Single Market—Towards a European Gigabit Society: sets the vision of a European Gigabit society, where availability and take-up of high capacity networks enables the Digital Single Market.
2017	Making 5G a success for Europe:[139] signed by EU telecom ministers and commits to roll out 5G between 2018-2025 and setup a Gigabit society by 2025.
2019	Digital Europe Programme: a proposed €9.2 billion ($9.9 billion) funding for 2021-2027[140], which will boost investment in digital technologies.

135 "A Digital Single Market Strategy for Europe", Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, COM (2015) 192 final, May 6, 2015, 3 and 15, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN.

136 "European Gigabit Society", *World Bank Group,* accessed March 26, 2020, https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2019/Telecom19/4.%20Je%20Myung%20Ryu.pdf.

137 "A Digital Single Market Strategy for Europe", *op. cit.*

138 "5G for Europe: An Action Plan", *op. cit.*

139 "5G Roadmap - Information from the Presidency", *Council of the European Union,* 14931/17, November 28, 2017, http://data.consilium.europa.eu/doc/document/ST-14931-2017-INIT/en/pdf.

140 "Digital Europe Programme: a proposed €9.2 Billion of funding for 2021-2027", *European Commission,* June 26, 2019, https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu92-billion-funding-2021-2027.

Since the discussions regarding 5G and Huawei have been ongoing, Brussels has been facing geopolitical pressure from the US and China. While Washington's warnings lean on national security and risks to critical infrastructure, China's responses defend Huawei and threaten reverse economic sanctions, should Chinese telecom companies be banned. Table 11 below looks at a few examples of statements made by the two countries, in an attempt to influence the decision of both EU and its member states.

Table 11. Statements from relevant actors to EU and its member states

Region/ Country	Statement made by	Statement
EU	Gordon Sondland, Former United States Ambassador to EU	"We can't risk being interconnected with someone who has vulnerable technology... we don't want you to put yourself in a position where we can't continue to be closely tied as we are today because you made the wrong technology choice."[141]
Slovakia	Lin Lin, Former Chinese Ambassador to Slovakia	"Huawei has been accused of being a threat without any evidence. The EU has to show concrete evidence that Huawei is a security threat."
Germany	Peter Altmaier, Federal Minister for Economic Affairs and Energy (Germany)	Defended the government's decision to not ban Huawei, saying that Germany did not issue a "boycott" of US companies in the wake of espionage accusations against the US' national security agency in 2013.[142]
	Richard Grenell, US Ambassador to Germany	"The recent claims by senior German officials that the United States is equivalent to the Chinese Communist Party are an insult to the thousands of American troops who helped ensure Germany's security and the millions of Americans committed to a strong Western alliance... There is no moral equivalency between China and the United States and anyone suggesting it ignores history – and is bound to repeat it." [143]
	Wu Ken, China's Ambassador to Germany	"If Germany were to make a decision that led to Huawei's exclusion from the German market, there will be consequences... The Chinese government will not stand idly by."
France	Statement by Spokesperson of Chinese Embassy in France	"We do not want to see the development of European companies in the Chinese market affected because of the discrimination and protectionism of France and other European countries towards Huawei."[144]

141 Alexandra Brzozowski, "US ambassador: Europe should forget Huawei, embrace Western tech", *Euractiv,* June 17, 2019, https://www.euractiv.com/section/global-europe/interview/us-ambassador-europe-should-forget-huawei-embrace-western-tech/.

142 Patrick Donahue and Stefan Nicola, "Trump Germany Envoy Calls U.S.-China Spying Comparison Insulting", *Bloomberg,* November 25, 2019, https://www.bloomberg.com/news/articles/2019-11-25/germany-s-altmaier-defends-huawei-with-jab-at-u-s-spies-on-tv.

143 *Ibid.*

144 "Déclaration du Porte-parole de l'Ambassade de Chine en France sur la question de Huawei et de la 5G", February 9, 2020, http://www.amb-chine.fr/fra/zfzj/t1742545.htm.

Region/ Country	Statement made by	Statement
Romania	Adrian Zuckerman, US Ambassador to Romania	"There's no safe place for Chinese companies in 5G networks. The only way to protect the security of 5G is to build it with companies we can trust. Allowing Chinese equipment into any part of a 5G network creates unacceptable risks to national security, critical infrastructure, privacy, and human rights. We look forward to working with our NATO Allies to build a strong, secure, and prosperous digital future that supports and defends our values and way of life."[145]
Portugal	Ajit Varadaraj Pai, Chairman of the US Federal Communication Commission	He met representatives of the Portuguese government for talks on the security of the 5G network in Portugal. US representatives reiterated that the security of critical communication infrastructures was paramount and that Huawei's presence in Portugal could ultimately damage US-Portugal relations.
Ireland	Statement by a senior White House official	Says there may be "implications" for Ireland because Eir has adopted Huawei in its 5G network. He warned against Ireland's vast data centre and tech sector "having an unsafe and insecure underlying telecommunications infrastructure". "Any country that includes Huawei in its 5G infrastructure jeopardises our ability to share information and intelligence at the highest level," he said.[146]

Source: News reports.

Regardless, concerns regarding cybersecurity in 5G networks have been at the forefront for all EU stakeholders. Given the emphasis of a seamlessly connected 5G network across Europe and achieving the goals of DSM and a Gigabit society, the EU recognised that without cooperation on 5G, a "patchwork of divergent national decisions would be detrimental to the digital single market". Thus, the EU took measures to frame a coordinated response to security risks and this approach has been endorsed at all levels of the EU decision-making–namely, the European Council, European Commission and the European Parliament.[147]

While there is a possibility for collective action in evaluating security risks and recommending measures to harmonise a non-binding response, Brussels was pragmatic about how it could not impose a ban on Chinese vendors for its member states. Firstly, matters of security and national defence policy are predominantly the

145 "U.S. Ambassador In Bucharest Slams Huawei", *Romania Journal,* February 21, 2020, https://www.romaniajournal.ro/business/u-s-ambassador-in-bucharest-slams-huawei/.

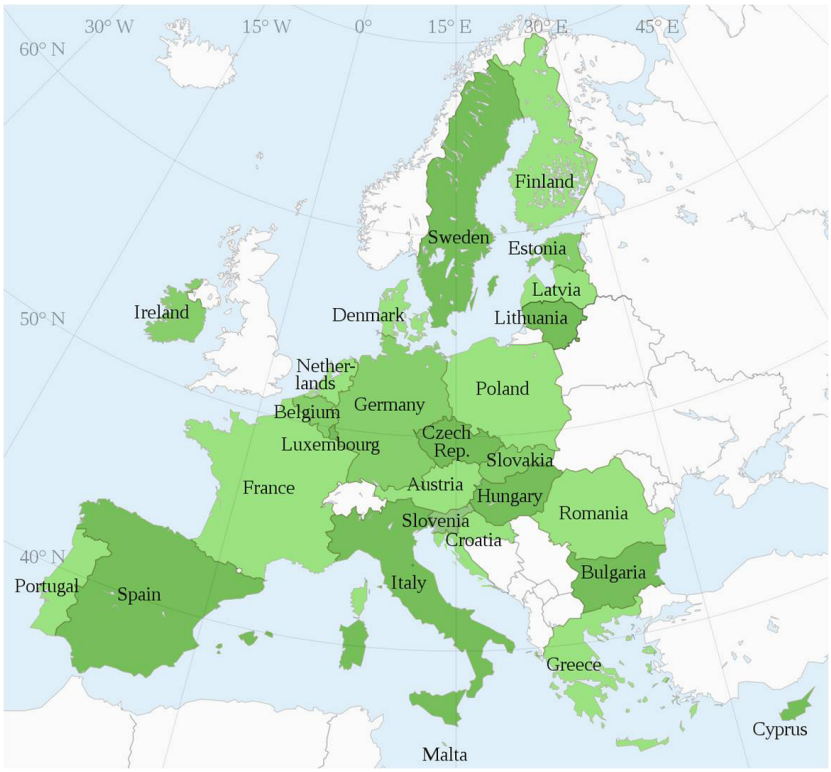
146 Adrian Weckler, "There could be 'implications' for Ireland as Eir adopts Huawei in its 5g network, senior White House official says", *Independent,* February 17, 2020, https://www.independent.ie/business/technology/there-could-be-implications-for-ireland-as-eir-adopts-huawei-in-its-5g-network-senior-white-house-official-says-38964671.html.

147 "European Council meeting (21 and 22 March 2019) – Conclusions", *European Council,* EUCO 1/19, March 22, 2019, https://data.consilium.europa.eu/doc/document/ST-1-2019-INIT/en/pdf; "Security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them", *European Parliament,* 2019/2575(RSP), March 12, 2019, https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_EN.pdf?redirect.

competence of individual member states.[148] Secondly, the reluctance to impose a EU-level ban can be understood in the context of the outcome of the May 2019 Prague 5G Security Conference. Representatives from 30 European nations, NATO and other countries, including the US, met at Prague and highlighted risks of influence of a third country on suppliers, and aimed to formulate a coordinated approach to shared security and policy measures.[149] Despite shared concerns that clearly referenced China, they were not ready to sign any document as they had not taken a conclusive decision in their home countries.

Thirdly, economic realities in the EU, such as high levels of dependence on Chinese equipment, cost, potential delays, and the need to maintain an open and competitive business environment with diversity of supply meant that it was not desirable to ban Huawei at the outset.[150] Lastly, given how individual member states may wish to frame their own response to 5G based on national priorities and foreign policy imperatives, Brussels found it prudent to leave the decision of a ban to individual member states. This position can also be understood with reference to divisions between members of the EU regarding China, and the significance of its trade, foreign direct investment, and its consumption of European business services.[151] Whereas some member states like Germany have developed close economic ties with China, others view greater

Fig 4. Countries of the European Union



Source: Member States of the European Union, Wikipedia, https://en.wikipedia.org/wiki/File:Member_States_of_the_European_Union_(polar_stereographic_projection)_EN.svg.

148 Elena Lazarou with Alina Dobreva, "Security and defence", European Parliament Briefing, June 2019, 1, https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/635533/EPRS_BRI(2019)635533_EN.pdf

149 Michael Kahn and Jan Lopatka, "Western allies agree 5G security guidelines, warn of outside influence", *Reuters*, May 3, 2019, https://in.reuters.com/article/us-telecoms-5g-security/western-allies-agree-5g-security-guidelines-warn-of-outside-influence-idINKCN1S91D2.

150 Gisela Grieger, "5G in the EU and Chinese telecoms suppliers", European Parliamentary Research Service, April 2019, https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637912/EPRS_ATA(2019)637912_EN.pdf.

151 John Farnell and Paul Irwin Crookes, *The Politics of EU-China Economic Relations*, (London: Palgrave Macmillan, 2016), 201.

economic integration as a threat to their domestic industries. The role of the US also creates a complex triangulation in the EU-China relations, due to its shared cultural heritage, and focus on political pluralism and human rights, that may find resonance with individual member states.[152]

Nonetheless, network security is of strategic importance to the EU, which is why it undertook the prerogative to coordinate risk assessment and mitigation measures for member states.[153] Table 12 provides details of the efforts taken by EU towards ensuring cyber security of 5G networks. Of particular interest is the 2019 EU Report on coordinated risk assessment in 5G Networks, which is based on national risk assessments taken by individual 28 EU member states (including the UK). Based on information on main assets, threats and vulnerabilities related to 5G infrastructure, it described potential ways whereby threat actors could exploit networks and adversely impact national objectives.[154] The report details that 5G brings greater complexity to the supply chain and reduces distinction between the core and edge networks, thereby increasing network vulnerabilities for attack.

Specifically, it identifies how a third party supplier can be subject to interference from another country because of (1) a strong link with the government; (2) the third country's legislation (absence of data protection and privacy laws); (3) characteristics of the supplier's corporate ownership; and (4) the ability for the third country to exercise any form of pressure, including in relation to the place of manufacturing of the equipment. This section is a clear nod to US allegations against Huawei and Beijing, and flags it as a cyber security risk that needs to be addressed. The EU's concern with respect to China, and the influence it can exert via foreign investment and acquisitions in strategic sectors, critical assets, technologies and infrastructure, are recognised as risks to EU's security. The 2019 European Commission joint communication on "EU-China – A strategic outlook" mentions that for these reasons it would be essential to strengthen the security of critical infrastructure and retain the strategic autonomy of the EU.[155]

152 *Ibid. 204.*

153 "Secure 5G networks: Questions and Answers on the EU toolbox", *European Commission,* January 29, 2020, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127.

154 "EU coordinated risk assessment of the cybersecurity of 5G networks", *NIS Cooperation Group,* October 9, 2019, 22, https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049.

155 "EU-China – A strategic outlook", European Commission and HR/VP contribution to the European Council, JOIN (2019) 5 final, March 12, 2019, 9, https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf.

Table 12. EU efforts to coordinate cyber security risk mitigation

Year	Name	Description
2019	Council decision concerning restrictive measures against cyber-attacks threatening the Union or its member states[156]	This framework allows the EU to impose sanctions on persons or entities that are responsible for cyberattacks, or who provide financial, technical or material support for such attacks. Sanctions include travel bans and asset freezes on persons and entities. This can help tackle cyberattacks emerging from 5G networks.
	EU Coordinated Risk Assessment on Cybersecurity in 5G Networks	This report identifies the main threats and threat actors, vulnerabilities and associated risks with 5G networks.
	ENISA (European Union Agency for Cybersecurity) report on threat landscape for 5G Networks	The report adds to existing studies, and identifies important assets (asset diagram), assesses threats affecting 5G (threat taxonomy), identifies asset exposure (threats – assets mapping) and provides an initial assessment of threat agent motives.[157]
2020	Cybersecurity of 5G networks EU Toolbox of risk mitigating measures	The objectives of this toolbox are to identify a possible common set of measures which are able to mitigate the main cybersecurity risks of 5G networks.

The EU toolbox consists of a combination of strategic and technical measures, as well as ancillary supporting actions that can be adopted and utilised by countries to design risk mitigation plans. Strategic measures aim to assess risks caused by "non-technical factors", including the risk of interference by a third country or dependency risks. The specific measures include gauging risk profile of vendors, applying restrictions for high-risk vendors, and even excluding them from key assets.[158] This measure is designed to mitigate risks associated with Huawei, and ensure that key assets in critical infrastructure are protected from Chinese influence.

In addition to the cyber security assessment and toolbox, the EU has also put in place other law and policy instruments to not only vet digital products and services, but also oversee procurement and investment in sensitive areas. An overview of these law and policy efforts are detailed in Table 13 below.

156 "Cyber-attacks: Council is now able to impose sanctions", *Council of the European Union,* May 17, 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/.

157 "ENISA threat landscape for 5G Networks", *European Union Agency for Cybersecurity,* November 21, 2019, https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

158 "Cybersecurity of 5G networks EU Toolbox of risk mitigating measures", *NIS Cooperation Group,* January 2020, 12, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

Table 13. EU Law and Policy efforts to tackle foreign influence

Year	Law and policy framework	Description
2014	EU Rules on Public Procurement[159]	In awarding public contracts, states – under certain conditions – can reject contracts that do not respect security, labour and environmental standards. It also enables states to impose measures necessary to protect public security or essential security interests.
2016	NIS Directive (Directive on Security of Network and Information Systems)[160]	Operators of essential services (including digital service providers) must take security measures and notify serious incidents to relevant authorities.
2018	European Electronic Communications Code (EECC)	Member states are required to ensure network integrity and security and manage risks. It also empowers national regulatory authorities to issue binding instructions and ensure compliance.[161]
2019	EU Cybersecurity Act	It revamps and strengthens the EU Agency for Cybersecurity (ENISA) and establishes an EU-wide cybersecurity certification framework for digital products, services and processes.
	EU's Foreign Direct Investment (FDI) Screening Regulation[162]	Addresses potential security risks related to FDI in sensitive areas, such as critical technologies and critical infrastructures.

The EU has therefore, attempted to coordinate the responses of its member countries to the cybersecurity issues posed by 5G networks–but has stopped short of banning Huawei, much to the chagrin of Washington. However, the measures recommended by the toolbox are flexible enough to leave all options on the table for member states. They could choose to ban Huawei or other Chinese telecommunications companies, should they prefer.[163] Huawei welcomed the announcement in a statement, and lauded the "non-biased and fact-based approach" towards security and the rollout of 5G networks. The official US response to this action was measured; it welcomed the EU acknowledgment of "unacceptable risks" posed by untrusted 5G suppliers, and called on individual member states to exclude high risk vendors from critical and sensitive parts of individual networks.[164]

159 Directive 2014/24/EU of 26 February, 2014 on Public Procurement, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0024&from=EN; Directive 2009/81/EC of 13 July, 2009 in the fields of defence and security, C (2019)5494 Guidance of 24 July, 2019 on the participation of 3rd country bidders and goods in the EU procurement market, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0081&from=EN.

160 Directive (EU) 2016/1148 of 6 July, 2016 concerning measures for a high common level of security of network and information systems across the Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

161 "Cybersecurity of 5G networks EU Toolbox of risk mitigating measures", *op. cit.,* 6.

162 Regulation (EU) 2019/452 of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0452&from=EN.

163 Matina Stevis-Gridneff, "E.U. Recommends Limiting, but Not Banning, Huawei in 5G Rollout", *The New York Times,* January 29, 2020, https://www.nytimes.com/2020/01/29/world/europe/eu-huawei-5g.html.

164 "United States Welcomes the EU's Acknowledgement of the Unacceptable Risks Posed by Untrusted 5G Suppliers", Statement of Michael R. Pompeo, Secretary Of State, US Department of State, January 30, 2020, https://www.state.gov/united-states-welcomes-the-eus-acknowledgement-of-the-unacceptable-risks-posed-by-untrusted-5g-suppliers/.

Through its approach to 5G and Huawei, Brussels is clearly trying to balance and maintain its relations with both the US and China, and has refrained from relenting to pressure to choose a side. While it has launched efforts to harmonise its risk assessment and mitigation strategies, it has left the decision of banning Huawei and other Chinese tech companies to individual member states.

European Union 27

Individually, the 27 member states of the EU have been at the forefront of 5G deployment and by 2025, 5G will be present in 34 percent of mobile connections, which is only behind North America (48 percent) and China (47 percent).[165] Most of the EU-27 countries have framed 5G roadmaps and strategies well ahead in time to describe policies related to spectrum allocation, 5G trials and 5G launches (Table 14). These national strategies have helped plan and streamline 5G deployments in EU member states, and accordingly propelled their upgrade to 5G networks.

Table 14. EU 27 plans and strategies for 5G deployment

Country	Plan	Country	Plan
Austria	5G strategy for Austria (2018)	Italy	5G for Italy (2016)
Denmark	5G Action Plan for Denmark (2019)	Luxembourg	5G Strategy (2018)
Finland	Digital infrastructure strategy 2025 (2019)	Netherlands	Connectivity Action Plan (2018)
France	5G roadmap (2018)	Poland	5G Strategy for Poland (2018)
Germany	5G for Germany (2016)	Romania	National Strategy for the Implementation of 5G in Romania (2018)
Hungary	"Digital Success Programme 2.0": Strategic study (2017)	Spain	5G National plan 2018-2020

Source: 5G Observatory, Quarterly Report 6, Up to December 2019, http://5gobservatory.eu/wp-content/uploads/2020/01/90013-5G-Observatory-Quarterly-report6_v16-01-2020.pdf.

Details of the publicly announced 5G trials and 5G commercial launches are provided in Table 15. Out of 27 member states, 15 have conducted trials with Chinese equipment suppliers like Huawei and ZTE. With reference to commercial launches of 5G, Austria, Germany, Italy and Portugal have launched 5G services with either Huawei and ZTE, or both. Finland, Hungary, Latvia and Romania may be using Huawei equipment in their 5G networks, however their public announcements do not specify this.

165 "The Mobile Economy 2020", *GSMA Intelligence,* 2020, 8-9, https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf.

Table 15: 5G Trials and Commercial Launches with Huawei among EU27

Country	5G trials with Huawei and ZTE	Details	Commercial 5G launches with Huawei and ZTE	Details
Austria		Trials with Huawei and ZTE		Hutchison Drei Austria, with ZTE
Belgium		With Huawei, ZTE and Nokia	N/A	N/A
Bulgaria		Huawei and Nokia	N/A	N/A
Croatia		VIPnet	N/A	N/A
Cyprus		N/A	N/A	N/A
Czechia		Trials with Ericsson	N/A	N/A
Denmark		With Huawei and Ericsson	N/A	N/A
Estonia		With Ericsson, Intel, Nokia and Huawei	N/A	N/A
Finland		Huawei, Nokia and Omnitele		DNA Finland and Elisa may be using Huawei
France		Huawei, Nokia, Ericsson, Qualcomm, Samsung	N/A	N/A
Germany		Huawei, Ericsson, Nokia, Intel, Qualcomm, Siemens		Deutsche Telekom and Vodafone Germany are reportedly using Huawei equipment
Greece		Nokia and Ericsson	N/A	N/A
Hungary		Ericsson		Vodafone Hungary may be using Huawei equipment
Ireland		Ericsson		Eir uses Huawei and Ericsson
Italy		ZTE, Huawei, Qualcomm, Ericsson		Telecom Italia and Vodafone Italy had announced that they would work with Huawei. They have launched 5G, but no confirmation on use of Huawei equipment

Country	5G trials with Huawei and ZTE	Details	Commercial 5G launches with Huawei and ZTE	Details
Latvia		Nokia		Tele2 Latvia has launched commercial 5G, but no formal Huawei announcement.
Lithuania		Nokia	N/A	N/A
Luxembourg		Trial by operator Tango, but no vendor announced.	N/A	N/A
Malta		N/A	N/A	N/A
Netherlands		Nokia, Huawei, ZTE, Ericsson	N/A	N/A
Poland		Nokia, Huawei, Ericsson	N/A	N/A
Portugal		Huawei and Ericsson		Nos (Portugal) uses Huawei equipment.
Romania		Cisco, Samsung, Ericsson, Huawei		3 telecom operators have launched 5G, RCS&RDS(DIGI) uses Ericsson's equipment. Unclear if others are using Huawei.
Slovakia		ZTE	N/A	N/A
Slovenia		N/A	N/A	N/A
Spain		Ericsson, Nokia, Huawei, ZTE, Interdigital, Cisco, Lenovo.		Vodafone Spain, with Huawei.
Sweden		Intel, Ericsson and Qualcomm	N/A	N/A

Key:

	With Huawei/ZTE
	Without Huawei/ZTE
	May or may not have Huawei/ZTE

Source: 5G Observatory EU (for 5G trials), and news reports for commercial launches.

Huawei has a strong presence in the region, and has undertaken research collaborations, partnerships, investments and engagements with both government and non-government stakeholders in the European Union. As per a 2015 Transparency International report, Huawei has the 10th highest lobbying budget in the EU, with the top two companies being ExxonMobil and Microsoft.[166] The headquarters of the EU–Belgium–is also Huawei's European headquarters of public relations, where it carries out extensive lobbying activities in establishments such as the Belgian Chamber of Commerce and the Flanders-China Chamber of Commerce to improve trade and investment between the two countries through events, networking and conferences.[167] In May 2019, it also opened the first Cyber Security Transparency Centre in Brussels to enhance communication and joint innovation with stakeholders, and address cybersecurity challenges.[168]

Table 16 gives examples of Huawei's major "soft power" initiatives with the EU 27, which includes investment, development partnerships and establishment of brick and mortar research labs.

Table 16. Huawei's soft power initiatives in the EU region

Country	Name and description of Initiative
France	Huawei and the Paris National Opera opened a Digital Academy to facilitate the online transmission of works, archives and creations and promote access to interactive content—especially educational—to students and researchers.
Sweden	With around 600 employees, Huawei's first European research and development hub was set up here in 2009.
Portugal	Huawei's Portugal Innovation & Experience Center opened in 2016, and commits to investment, innovation and support for local industry and partnership.
Germany	Huawei's German Research Centre is part of the HiPEAC European Network, which functions as a focal point for training and collaboration between researchers, industry and policy makers. It is responsible for advanced technology research, architecture evolution, design and strategic technical planning.
Italy	In 2016, Sardinia and Huawei established a Joint Innovation Centre within CRS4 (Center for Advanced Studies, Research and Development, Sardinia) to conduct research on smart cities, big data and cybersecurity.
Ireland	Huawei recently announced a €70 million ($76 million) investment in research and development (R&D) in three locations across Ireland.
Hungary	Location of Huawei's European Supply Centre, launched in 2019, which is reportedly Huawei's biggest production base outside China.

Source: "Europe and 5G: the Huawei case Part 2", Institute Montaigne, accessed March 26, 2020, https://www.institutmontaigne.org/en/publications/europe-and-5g-huawei-case-part-2.

166 "Lobby meetings of the European Commission", *Transparency International,* December 1, 2016, 7, https://transparency.eu/wp-content/uploads/2016/10/Lobby-Meetings-European-Commission.pdf.

167 "La Chine à l'assaut de Bruxelles: un réseau d'organisations influents", *Asie Pacifique News,* December 11, 2018, https://asiepacifique.fr/lobbying-chine-bruxelles-ue-reseau/.

168 "Huawei Cyber Security Transparency Centre", *Huawei,* accessed March 27, 2020, https://www.huawei.com/en/about-huawei/trust-center/transparency/huawei-cyber-security-transparency-centre-brochure.

Among the largest EU countries by GDP, i.e. Germany, France, Italy and Spain, no decision has been made to ban Huawei. Moreover, mobile operators in Germany, Italy and Spain are already reportedly using Huawei equipment in their 5G networks. Eastern European countries, such as Estonia, Czechia, Poland and Romania appear to be the only EU members who may likely ban Huawei and other Chinese telecom companies, for reasons related to security and the possible intrusion of Beijing through Huawei's kit.

Within ***Germany***, the 5G debate has been exceptionally fierce and has divided members of Chancellor Angela Merkel's ruling coalition. In October 2019, two German technical agencies, the Federal Network Agency (Bundesnetzagentur, BNetzA) and the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI)[169] issued a draft 5G "security catalogue," which said that Berlin will not exclude any company from 5G networks and will adopt a multi-vendor approach. The regulations were criticised domestically for deciding a question of strategic importance on purely technical criteria, [170] and without non-technical criteria, such as the degree of independence and transparency of the company, the laws and strategic objectives of its country of origin.[171] Bruno Kahl, head of Germany's Federal Intelligence Service (BND), echoed similar concerns and said that trust in a "state company that has a very high level of dependence on the Communist Party and [China's] intelligence apparatus" is not present.[172] In order to arrest the implementation of this measure, some members of the ruling Christian Democratic Union drafted a bill to impose a ban on "untrustworthy 5G vendors".

Germany's decision appears to be taken in light of robust economic ties between China and Germany. Beijing is Berlin's largest trading partner, and China is the biggest single market for German cars such as Volkswagen AG, BMW AG and Mercedes-Benz maker Daimler AG.[173] This rationale for decision-making was initially criticised by Norbert Röttgen, chair of German parliament's foreign affairs committee, who said that Berlin cannot afford to surrender its "digital security" for "fear of economic retaliation".[174] In February 2020, however, dissenting members of the political party conceded and voted in unison[175] to not ban high risk vendors but, instead, called for assurances from 5G suppliers that their infrastructure is not subject to foreign influence. They also advocated for increased reliance on strong cryptography, and avoiding "monocultures" in 5G infrastructure, where a single supplier gets a disproportionate share of the network.[176] Chancellor Angela Merkel and Arne Schönbohm, head of German federal cyber security agency, have also proposed seeking guarantees–in the form of a "no spy" deal from both Huawei and China, to ensure that the integrity of data in their

169 Kaan Sahin and Didi Kirsten Tatlow, "Berlin's preliminary decision 5G decision: limiting damage and learning lessons", *German Council on Foreign Relations*, Policy Brief No. 3, November 2019, 2, https://dgap.org/sites/default/files/article_pdfs/dgap_policybrief_nr3-nov2019_5g.pdf.

170 *Ibid.*, 3.

171 *Ibid.*, 4.

172 Patrick Donahue, "German Spy Chief Says Huawei Can't Be 'Fully Trusted' in 5G", *Bloomberg,* October 29, 2019, https://www.bloomberg.com/news/articles/2019-10-29/german-spy-chief-says-huawei-can-t-be-fully-trusted-in-5g.

173 Tony Czuczka and Steven Arons, "China Threatens Retaliation Should Germany Ban Huawei 5G", *Bloomberg,* 15 December 15, 2019, https://www.bloomberg.com/news/articles/2019-12-14/china-threatens-germany-with-retaliation-if-huawei-5g-is-banned?sref=NDAgb47j.

174 Hans Von Der Burchard, "Senior lawmaker: Germany not planning to restrict 5G security requirements", *Politico,* September 14, 2019, https://www.politico.eu/article/senior-lawmaker-germany-not-planning-to-restrict-5-g-security-requirements/.

175 Philipp Grüll, "German Conservatives vote 'in unison' against excluding Huawei from 5G network", *Euractiv,* February 12, 2020, https://www.euractiv.com/section/5g/news/german-conservatives-vote-in-unison-against-excluding-huawei-from-5g-network/.

176 *Ibid.*

5G networks is not compromised.[177] An agreement of this nature could work as a tool to ensure accountability and provide an opportunity to Huawei, to demonstrate its commitment towards network security. However, in 2015, then US president Barack Obama and Chinese president Xi Jinping entered into a similar deal to stop cyber espionage; a deal that US feels has been violated by China. With this history, for Beijing, the agreement can function as a method of censure against espionage and surveillance–with its global image and its ambitions to become a technological power, at stake.

Similarly, in ***Italy***, there is a divergence of view on the Huawei question among members of the government. Italy's parliamentary body on intelligence and security (COPASIR) has told the government to "very seriously" consider banning Huawei[178]. An Italian minister–on the other hand–asserted that Huawei should be given a role in Italy's future 5G networks,[179] and this appears to be the latest position of Rome as per a January 2020 news report.[180] Likewise, Italian mobile operators Telecom Italia and Vodafone Italy have announced that they will be using Huawei in their 5G networks.

Nonetheless, Italy has erred on the side of caution and introduced legal mechanisms to address potential strategic and security threats emanating from Huawei's kit. In April 2019, Law Decree No. 22 was introduced which designates 5G technology as strategic for national defence and security system and gives the government the right to either veto, or impose certain conditions, on transactions involving broadband electronic communications services based on 5G technology. If the government's directions are not adhered to, severe sanctions are likely to follow. [181] In July 2019, Law Decree No. 64/2019 was adopted which amends Italy's "Golden Power Legislation" (GPL) to cover 5G technology transactions. The GPL governs the State's authority to intervene in deals involving companies operating in strategic sectors, such as defence, national security and communications, and gives Rome broad powers to impose restrictions if there is a threat to national security and public order.[182] These measures are similar to those put in place by France, which has also chosen to not ban Huawei, but has implemented measures to combat security risks and check the possible influence of China on the company.

In ***France***, a March 2020 news report states that the country will allow Huawei's equipment in non-core part of 5G networks.[183] Nonetheless, telecom operators will have to seek permission from the prime minister for their 5G network projects, and

177 Guy Chazan, "German cyber security chief backs 5G 'no spy' deal over Huawei", *Financial Times,* February 28, 2019, https://www.ft.com/content/5a0fe826-3b34-11e9-b856-5404d3811663.

178 Daniele Lepido, "Italian Lawmakers Urge Government to Consider Huawei 5G Ban", *Bloomberg,* December 20, 2019, https://www.bloomberg.com/news/articles/2019-12-20/italian-lawmakers-urge-government-to-consider-huawei-5g-ban?sref=NDAgb47j; https://www.analisidifesa.it/2019/12/per-il-copasir-occorre-valutare-lesclusione-delle-aziende-cinesi-dalle-reti-5g/.

179 "Huawei should be allowed 5G role in Italy: Industry minister", *Reuters,* December 22, 2019, https://www.reuters.com/article/us-italy-5g-security-patuanelli/huawei-should-be-allowed-5g-role-in-italy-industry-minister-idUSKBN1YQ0D7.

180 "Italy has no plans to exclude Chinese firms from 5G network, minister says", *Reuters,* January 31, 2020, https://www.reuters.com/article/us-italy-huawei-tech-5g/italy-has-no-plans-to-exclude-chinese-firms-from-5g-network-minister-says-idUSKBN1ZT2P3.

181 "FDI screening expended to cover 5G technology", Investment Policy Monitor, United Nations Conference on Trade and Development, March 26, 2019, https://investmentpolicy.unctad.org/investment-policy-monitor/measures/3354/italy-fdi-screening-expended-to-cover-5g-technology.

182 Leah Dunlop, *et. al.,* "Italy: Italian Government Acts To Strengthen Further Its "Golden Powers"", *Mondaq,* August 9, 2019, https://www.mondaq.com/italy/Government-Public-Sector/830534/Italian-Government-Acts-To-Strengthen-Further-Its-Golden-Powers.

183 Mathieu Rosemain and Gwénaëlle Barzic, "Exclusive: France to allow some Huawei gear in its 5G network – sources", *Reuters,* March 13, 2020, https://www.reuters.com/article/us-france-huawei-5g-exclusive/exclusive-france-to-allow-some-huawei-gear-in-its-5g-network-sources-idUSKBN20Z3JR.

receive clearance based on national security considerations.[184] Amendment 1722 introduced a "prior authorisation regime, on grounds of national defence and security, for radioelectric network equipment" and covers 5G equipment. Other legislative measures to address cyber security concerns include amendment 874 of the PACTE Law (Plan d'Action pour la Croissance et la Transformation des Entreprises, or Action Plan for Business Growth and Transformation) and strengthens ANSSI's role (France's cybersecurity agency) in the approval of 5G devices.[185] However, major French telecom operators such as SFR have expressed concerns that such security measures could have a negative impact on competition.[186] Another carrier, Orange France – which has conducted 5G trials with Nokia[187] – agreed with this position and stated that some fears surrounding Huawei Technologies is unfounded, and could threaten the delay of 5G rollout.[188]

Spain has allowed Huawei to build its 5G networks, with Vodafone Spain launching the region's first commercial 5G network with Huawei. The Spanish government has MoUs (memorandum of understanding) with Huawei, such as the 2016 MoU with Spanish National Institute of Cyber security (INCIBE) to collaborate on cybersecurity initiatives.[189] Its national 5G plan, however, puts security measures at the forefront of 5G regulation. Since 5G will be a key component of strategic and critical services such as energy, transport and security, the national plan mentions laws such as the General Telecommunication Law 9/2014 and Law 8/2011, which set out measures to guarantee the integrity and security of networks, and also introduces measures to protect critical infrastructure – including ICTs in strategic areas.[190]

Similarly, in 2018, ***Portugal's*** main telecom operator, Altice Portugal, tied up with Huawei for 5G. Xi Jinping travelled to Portugal in 2018, and on this occasion, Prime Minister Antonio Costa declared that the 5G network remained open to Huawei.[191] Nonetheless, following EU's release of the cybersecurity toolbox, Portugal is considering limiting the extent of Huawei in its 5G networks.[192] Telecom operators like NOS use Huawei equipment, but have refrained from deploying it in core networks–a position that is likely to be followed by Altice as well.[193]

---

184 "France will not exclude China's Huawei from 5G rollout: minister", *Reuters,* November 25, 2019, https://www.reuters.com/article/us-france-huawei-minister/france-will-not-exclude-chinas-huawei-from-5g-rollout-minister-idUSKBN1XZ1U9.

185 "5G in Europe: Time to Change Gear!", *Institut Montaigne*, Note, May 2019, 14, https://www.institutmontaigne.org/ressources/pdfs/publications/5g-europe-time-change-gear-part-1-note.pdf.

186 Mathieu Duchâtel and François Godemen, "Europe and 5G: the Huawei Case – part 2", *Institut Montaigne*, accessed March 26, 2020, https://www.institutmontaigne.org/en/publications/europe-and-5g-huawei-case-part-2.

187 "Orange is getting ready for the arrival of 5G in Marseille, a new testing ground", *Orange,* July 3, 2018, https://www.orange.com/en/Press-Room/press-releases/press-releases-2018/Orange-is-getting-ready-for-the-arrival-of-5G-in-Marseille.-a-new-testing-ground; "Orange prepares for the arrival of 5G with three new tests", *Orange,* February 7, 2018, https://www.orange.com/en/Press-Room/press-releases/press-releases-2018/Orange-prepares-for-the-arrival-of-5G-with-three-new-tests

188 Mathieu Rosemain, "Some fears about Huawei are 'complete nonsense', Orange's boss says", *Reuters,* December 18, 2019, https://in.reuters.com/article/orange-5g/some-fears-about-huawei-are-complete-nonsense-oranges-boss-says-idINKBN1YM1MY.

189 "Huawei Spain and INCIBE sign a MoU for the Development of Cyber security", *Huawei,* February 26, 2016, https://www.huawei.com/en/press-events/news/2016/2/Huawei-Spain-and-INCIBE-sign-a-MoU.

190 "Spain's 5G National Plan 2018-2020", Ministry of Energy, Tourism and Digital Agenda (Spain), accessed March 27, 2020, 31, https://avancedigital.gob.es/5G/Documents/plan_nacional_5G_en.pdf.

191 "Portugal to cooperate with China to create 'new Silk Roads' of trade", *Channel News Asia,* December 6, 2018, https://www.channelnewsasia.com/news/business/portugal-to-cooperate-with-china-to-create-new-silk-roads-of-11000866.

192 Natasha Donn, "Limits on Huawei in Portugal's developing 5G network "expected today"", *Portugal Resident,* February 6, 2020, https://www.portugalresident.com/limits-on-huawei-in-portugals-developing-5g-network-expected-today/.

193 "MEO rules out Huawei 5G development in Portugal", *Portugal Resident,* March 10, 2020, https://www.portugalresident.com/meo-rules-out-huawei-5g-development-in-portugal/.

In 2019, ***Hungary's*** Foreign Minister Péter Szijjártó announced that Huawei would cooperate with Vodafone and Deutsche Telekom in the Hungarian 5G build-up.[194] In January 2020, Hungarian Innovation and Technology Minister László Palkovics also said that it has not been proven that Huawei's technology would pose any risk to Hungary, as they "...have seen no (data) to support that," and until this happens, Budapest will treat Huawei as any other technology company.[195]

Belgium is yet to commercially launch 5G services; however, two of its major mobile operators–Proximus and Telenet–have conducted trials with Huawei and ZTE, while Orange conducted a trial with Nokia. Carriers in this region have partnerships with Chinese suppliers; Telenet and Orange are collaborating with China's ZTE, while Proximus has already been working with Huawei for some time now.[196] Brussels is also Huawei's headquarters for public relations and the location for its newly opened Cyber Security Transparency Centre. Additionally, a recent assessment by Belgium's cybersecurity agency found that there is no evidence that Huawei's equipment could be used for spying.[197] In January 2020, however, telecom minister Philippe De Backer and Belgium's security services supported the view that with 5G, limits need to be placed on equipment coming from "unreliable suppliers".[198] Nevertheless, the country's strong ties with the Chinese tech giant makes it unlikely that the country will ban Huawei.

Ireland has no publicly announced 5G trials and is yet to commercial launch 5G networks. Two of the three major mobile networks—Vodafone and Three—have chosen Ericsson as their 5G network provider, while Eir has opted for a combination of Ericsson and Huawei. Some smaller wireless operators, such as Imagine, have based their networks on Huawei equipment.[199]

Finland is home to Nokia Corporation, one of Huawei's major rivals. Here, majority of the mobile operators like Telia, DNA, and Sonera have carried out trials with Nokia. Elisa, on the other hand, carried out trials with both Nokia and Huawei, and has a partnership with Huawei to develop 5G[200]. Timo Harakka, Finnish Minister for Transport and Communication said that Finland will offset any 5G associated security risks by including several equipment suppliers, and that the government has already defined national security requirements and quality requirements for these networks.[201] Consequently, Finland has not announced any plans to ban Huawei.

---

194 "Huawei Building 5G Network in Hungary, says Trade Minister", *Hungary Today,* May 11, 2019, https://hungarytoday.hu/huawei-building-5g-network-in-hungary-says-trade-minister/.

195 Gergely Szakács, "Hungary has no evidence of Huawei threat, plans rapid 5G rollout: minister", *Reuters,* June 20, 2019, https://www.reuters.com/article/us-hungary-telecoms-5g-huawei/hungary-has-no-evidence-of-huawei-threat-plans-rapid-5g-rollout-minister-idUSKCN1TL2AP.

196 "Huawei boasts 5G contracts with European operators", *The Brussels Times,* February 21, 2020, https://www.brusselstimes.com/all-news/96382/huawei-reports-47-contracts-for-5g-in-europe/.

197 "Belgian cybersecurity agency finds no threat from Huawei", *Reuters,* April 15, 2019, https://www.reuters.com/article/us-huawei-tech-security-belgium/belgian-cybersecurity-agency-finds-no-threat-from-huawei-idUSKCN1RR1GP.

198 "Belgian security services call to restrict 5G technology", *The Brussels Times,* January 9, 2019, https://www.brusselstimes.com/belgium/88263/belgian-security-services-want-second-highest-security-level-for-huawei-5-g-technology/.

199 Adrian Weckler, "There could be 'implications' for Ireland as Eir adopts Huawei in its 5g network, says senior White House official", *Indepdent,* February 17, 2020, https://www.independent.ie/business/technology/there-could-be-implications-for-ireland-as-eir-adopts-huawei-in-its-5g-network-senior-white-house-official-says-38964671.html.

200 "Finnish telecom operator Elisa signs 5G commercial contract with Huawei", *C114 Communication Network,* March 22, 2019, http://www.c114.com.cn/news/126/a1082925.html.

201 "Tensions over Huawei's position on the 5G network are growing in Europe - Finland does not rule out individual players", *Uutiset,* December 23, 2019, https://yle.fi/uutiset/3-11131015.

For ***Sweden***, its major telecom operator Telia has a strategic partnership with Huawei to cooperate in the research and development of 5G technologies.[202] In February 2020, Chinese media reported that the Swedish Post and Telecom Authority (PTS) has said that there will be no ban on Huawei in the country, but all vendors will need to undergo a review by the Swedish Armed Forces and the Swedish Security Service.[203]

In ***Denmark***, Huawei has been active since 2007 and has a strategic partnership with major telecom operator, TDC. TDC carried out 5G trials with both Huawei and Ericsson,[204] but announced a surprise decision to shun long time supplier Huawei, choosing Ericsson to rollout the 5G network.[205] Though Denmark has not come forth with a Huawei ban, the official position of the Danish government vis-à-vis China has been conservative at best. The Danish Cyber and Information Security Strategy underlines the importance of information and cyber security in telecommunications, and asserts that telecom providers must ensure accessibility, integrity and confidentiality in their networks and have a contingency plan in place in case of cyberattacks.[206] With reference to cyberattacks, the government's Foreign and Security Policy Strategy alarmingly notes that cyber threats are evolving and many countries–including China–seek to achieve political objectives through cyberattacks, disinformation and cyber espionage.[207]However, Denmark acknowledges the importance of engaging with the growing Chinese market[208], but is still keen on establishing a secure, free and open global IT infrastructure based on common rules and cooperation.[209]

Remarkably, the technological rivalry between the US and China has reached an acute stage in a remote self-governing archipelago in Denmark, i.e. the ***Faroe Islands***. According to a *New York Times* report, the salmon industry is integral to the economy of Faroe Islands and more than 90 percent of its exports are fish and are destined to its biggest market—China. For Faroe Islands, retaining its competence in salmon exports to the Chinese market is of utmost importance, which is why the question of allowing Huawei in 5G networks is closely tied with the need to maintain trade relations with Beijing. While America's ambassador to Denmark, Carla Sands, publicly warned against Huawei saying that there would be "dangerous consequences" if the company is allowed, China's ambassador to Denmark, on the other hand, threatened to block a trade deal—and more fish sales—if Huawei was not used for the 5G network.[210]

Netherlands has a similar position with respect to China, Huawei and 5G networks. An October 2019 Foreign Affairs ministry document on Netherland's China policy underscored the importance of trade and investment relations, but cautiously notes China's influence in emerging technologies–like 5G–and would like to put in place law and policy measures to monitor its investments and unfair trade practices in

---

202 "Teliasonera & Huawei Will Jointly Innovate In 5G", *Telia Company,* February 2, 2019, https://www.teliacompany.com/en/news/news-articles/2016/teliasonera--huawei-will-jointly-innovate-in-5g/.

203 "No "Huawei ban" as Sweden takes next step toward 5G", *Xinhua News Agency,* February 8, 2020, rollouthttp://www.xinhuanet.com/english/2020-02/08/c_138765821.htm.

204 "Major European 5G trials and pilots", *op. cit.*

205 "Denmark's TDC shuns China's Huawei for 5G rollout", *The Local,* March 19, 2019, https://www.thelocal.dk/20190319/denmarks-tdc-shuns-chinas-huawei-for-5g-rollout.

206 "Danish Cyber and Information Security Strategy 2018-2021", Ministry of Finance, The Danish Government, May 2018, 7-8, https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf.

207 "Foreign and Security Policy Strategy 2019-2020", *The Danish Government,* November 2018, 13, https://www.dsn.gob.es/sites/dsn/files/2018_Denmark%20Foreign%20and%20security%20policy%20strategy%202019-2020.pdf.

208 *Ibid.,* 9.

209 *Ibid.,* 22.

210 Adam Satariano, "At the Edge of the World, a new battleground for the US and China", *The New York Times,* December 20, 2019, https://www.nytimes.com/2019/12/20/technology/faroe-islands-huawei-china-us.html.

this area.[211] With reference to security concerns, the 2018 Annual Report by the Dutch General Intelligence and Security Service (AVID), explicitly states that China is at the vanguard of economic espionage and covert political influencing, and is attempting to use initiatives like 'Made in China 2025' and the 'New Silk Roads' to expand its geopolitical influence.[212] Consequently, a Dutch General Administrative Order (AMvB) on the security and integrity of telecommunication networks was introduced to ensure that critical parts of telecom networks only come from reliable suppliers. Through this order, service providers can also be instructed via the AMvB to exclude suppliers on the criteria of espionage or suspected abuse.[213] The Netherlands government has, however, not come forth to ban Huawei, but has taken steps to safeguard its 5G networks.

In 2018, ***Czech Republic's*** National Cyber and Information Security Agency (NÚKIB), the government's cybersecurity watchdog, issued a warning that "the use of technical or program tools of Huawei Technologies and ZTE Corporation poses a cyber security threat".[214] Following this warning, in January 2019, the General Finance Directorate excluded Huawei from a Czech tender valued at 500 million crowns ($22 million) to build a tax portal in the country.[215] Czechia was, thus, deemed to be the loudest critic of Huawei in Europe. This position changed in late 2019 when Czech Industry Minister Karel Havlíček made a restrained statement– that the country is following how the issue plays out in Europe.[216]

Poland, Romania and Estonia have signed agreements and memorandums of understanding with the US to review companies if they are subject to control by a foreign government–a move that could result in the blocking of Huawei and ZTE.

In September 2019, ***Poland*** signed an agreement with the US committing to review any company interested in building 5G and to ascertain "whether the supplier is subject to control by a foreign government".[217] This position finds resonance with the statement of Poland's Minister of Digitization Marek Zagórski who said that "Huawei's presence in the construction of 5G infrastructure and security are two things that are mutually exclusive".[218] Poland's position may derive from the fact that in January 2019, a Chinese employee from Huawei and a Polish national were arrested over allegations of spying for Beijing.[219] Following the arrest, Huawei offered to build a cybersecurity centre, in a bid to re-establish Poland's trust in the company.

---

211 "The Netherlands and China: a new balance", Ministry of Foreign Affairs, Government of the Netherlands, October 2019, 23, https://www.government.nl/documents/policy-notes/2019/05/15/china-strategy-the-netherlands--china-a-new-balance.

212 "AIVD Annual Report 2018", General Intelligence and Security Service AVID, Ministry of the Interior and Kingdom Relations, Netherlands, May 2019, 8-11, https://english.aivd.nl/publications/annual-report/2019/05/14/aivd-annual-report-2018.

213 Witold Kepinski, "Government opens registration for auction of mobile communication frequencies", *Dutch IT Channel,* March 6, 2020, https://dutchitchannel.nl/641151/overheid-opent-inschrijving-voor-veiling-mobiele-communicatie-frequenties.html; "Consultation Dutch auction of fast mobile communication has started", Government of the Netherlands, December 12, 2019, https://www.rijksoverheid.nl/actueel/nieuws/2019/12/05/consultatie-nederlandse-veiling-snelle-mobiele-communicatie-gestart.

214 Filip Brokes, "Huawei Hoopla: 'Business As Usual' After Czech 5G Warning*", Reporting Democracy*, November 1, 2019, https://balkaninsight.com/2019/11/01/huawei-hoopla-business-as-usual-after-czech-5g-warning/.

215 Jason Hovet and Robert Muller, "China's Huawei excluded from Czech tax tender after security warning", *Reuters,* January 30, 2019, https://www.reuters.com/article/us-czech-security/chinas-huawei-excluded-from-czech-tax-tender-after-security-warning-idUSKCN1PO10G.

216 "Czechs unlikely to differ from Germany on Huawei approach: Minister", *Reuters,* October 24, 2019, https://www.reuters.com/article/us-czech-telecoms/czechs-unlikely-to-differ-from-germany-on-huawei-approach-minister-idUSKBN1X30TV.

217 Catherine Lucey and Drew Hinshaw, "U.S. Signs 5G Agreement With Poland Amid Huawei Concerns", *The Wall Street Journal*, September 2, 2019, https://www.wsj.com/articles/u-s-signs-5g-agreement-with-poland-despite-huawei-concerns-11567434905.

218 "Marek Zagórski: Huawei 5G and security are mutually exclusive", *Rzeczpospolita*, September 5, 2019, https://www.rp.pl/Telekomunikacja-i-IT/190909641-Marek-Zagorski-5G-od-Huawei-i-bezpieczenstwo-wykluczaja-sie.html

219 Adam Satariano and Joanna Berendt, "Poland Arrests 2, Including Huawei Employee, Accused of Spying for China", *The New York Times,* January 11, 2019, https://www.nytimes.com/2019/01/11/world/europe/poland-china-huawei-spy.html.

However, following these developments, Warsaw is keen on implementing stricter security criteria for 5G networks[220] and supports coordination at the EU-level to develop 5G security standards.[221] Poland is also seeking to introduce tough controls to limit the use of vendors who are high risk or untrustworthy and is working on a telecom security law that will further toughen controls[222]. This is in addition to legislation based on the EU toolbox that has already been drafted.[223]

Estonia signed a similar memorandum of understanding (MoU) with the US, which will restrict the use of Huawei equipment in Estonia's 5G mobile core networks.[224] Estonia has also introduced a draft bill, which would require telecom companies to seek state permission when introducing new hardware and software, and the security of any new tech will additionally be monitored by Estonia's Information System Authority (RIA), the Internal Security Service (ISS) and the state's foreign intelligence agency.[225] Huawei protested against this bill in a letter to Interior Minister Mart Helme arguing that the Bill does not constitute fair and transparent regulation and would in effect exclude it from the market.[226]

Romania also signed a MoU with the US, agreeing to ensure that only trusted and reliable vendors are used, and that they must be evaluated to see if they are under the control of a foreign government, have a transparent ownership structure, and a history of ethical corporate behaviour.[227] In 2019, the opposition party in Romania sought to trigger a public inquiry into Huawei's contribution to critical infrastructure and seek to bar it from 5G network development due to mounting security concerns.[228] Currently, Romania is yet to tender a decision on Huawei and the 5G dilemma.

Outside the European Union

This section will examine countries outside the European Union and will be limited to those that have either carried out 5G trials or have commercially launched 5G services in their territory.

220 "Zagórski on the Polish idea for 5G security", *Telko,* December 18, 2019, https://www.telko.in/reuters-zagorski-o-polskim-pomysle-na-bezpieczenstwo-5g.

221 "The EU will set common 5G security standards", Ministry of Digitization (Poland), March 28, 2019, https://www.gov.pl/web/cyfryzacja/ue-okresli-wspolne-standardy-bezpieczenstwa-5g.

222 Laurens Cerulus and Laura Kayali, "Poland wants to go beyond EU on 5G security, says minister", *Politico,* February 3, 2020, https://www.politico.eu/article/poland-wants-to-go-beyond-5g-security-toolbox-restrictions/.

223 https://legislacja.rcl.gov.pl/docs//522/12329501/12658511/12658512/dokument435747.pdf

224 "Estonia limits use of Huawei gear in 5G rollout", *Comms Update,* November 4, 2019, https://www.commsupdate.com/articles/2019/11/04/estonia-limits-use-of-huawei-gear-in-5g-rollout/.

225 "Telecoms security bill may exclude Huawei from Estonian market, firm says", *ERR,*January 6, 2020, https://news.err.ee/1020859/telecoms-security-bill-may-exclude-huawei-from-estonian-market-firm-says.

226 *Ibid.*

227 "Memorandum of Understanding between The Government of Romania and the Government of the United States", *Ministry of Communication and Information Society,* Romanian Government, August 20, 2019, https://www.comunicatii.gov.ro/wp-content/uploads/2019/11/memorandum-5g.pdf

228 Radu-Sorin Marinas, "Exclusive: Romania's opposition seeks Huawei ban in telecom infrastructure", *Reuters*, March 6, 2019, https://www.reuters.com/article/us-romania-china-huawei-tech-exclusive-exclusive-romanians-opposition-seeks-huawei-ban-in-telecom-infrastructure-idUSKCN1QM2H8.

Table 17. Other European trials and commercial launches with Huawei and ZTE

Country	Trials with Huawei and ZTE	Details	Commercial launch with Huawei/ ZTE	Details
Monaco	N/A	N/A		Monaco Telecom with Huawei
Norway		Huawei and Nokia	N/A	N/A
Switzerland		Ericsson, Qualcomm, Nokia, Huawei		Sunrise with Huawei

In ***Norway***, intelligence agencies issued warnings regarding close ties between China and Huawei, and the possible threat to Norwegian interests. In a 2019 report, the Norwegian Police Security Service (PST)—the domestic intelligence and security service—highlighted that Russia and China can conduct intelligence activities against Norway.[229] While presenting the report, the PST chief Marie Benedicte Bjørnland, drew particular attention to Chinese companies like Huawei, which have close ties and cooperation with Chinese authorities and could be a potential national security threat.[230] Though 5G networks have not been launched in Norway, its leading operator Telenor picked Ericsson as a technology provider for 5G, and stated that it will gradually phase out Huawei equipment from its network.[231]

Switzerland, on the other hand, is open to Huawei and other Chinese telecom companies. In a discussion on Huawei in the Federal Assembly of the Swiss Parliament, it reasoned that firstly, the US government has not provided any evidence to support any espionage allegation; secondly, the UK's cybersecurity evaluation of Huawei has outlined vulnerabilities in the network, but has not found any proof of spy functions in the equipment; thirdly, Switzerland has no alternatives to the predominant solutions of the major players in the telecommunications market, and will find it difficult to break free from dependencies of the two technology leaders, i.e. the US and China; fourthly, Switzerland is not dependent on security alliances that force other countries to take sides for one side or the other; and lastly, in terms of security, existing Swiss laws, such as Article 48a of the Telecommunications Act obliges network operators to combat unauthorized manipulation of their telecommunications systems, and in addition to this, the Swiss Federal Council will enact new regulations on security of information and telecom infrastructures.[232]

Nonetheless, MELANI, Switzerland's authority that deals with cyber incidents, described cyber threats that originated from China, such as the espionage operation carried out by the APT40–a group thought to have links with the Chinese government

229 "Threat Assessment 2019", Norwegian Police Security Service (PST), 2019, 7, https://www.pst.no/globalassets/artikler/trusselvurderinger/annual-threat-assesment-2019-single-pages.pdf.

230 "Norway Intelligence Service Adds Huawei on National Security Threat List", *The Nordic Page,* accessed March 27, 2020, https://www.tnp.no/norway/panorama/norway-intelligence-service-adds-huawei-on-national-security-threat-list.

231 Bevin Fletcher, "Telenor ditches Huawei, taps Ericsson for 5G RAN in Norway", *Fierce Wireless,* December 13, 2019, https://www.fiercewireless.com/5g/telenor-ditches-huawei-taps-ericsson-for-5g-ran-norway.

232 "Huawei and the challenges of 5G. Risks and opportunities for Switzerland", Interpellation by Regazzi Fabio, The Federal Assembly of the Swiss Parliament, March 6, 2019, https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193051.

in its 2018 semi-annual report.[233] The MELANI report also criticizes the negative impact of US sanctions measures on Huawei, its risks to global supply chain and how it can adversely affect small, open markets like Switzerland who are dependent on foreign suppliers.[234] All three major Swiss telecom operators–Salt, Sunrise and Swisscom–are approved to cover the country in 5G, and all have Huawei equipment in their fixed and mobile networks.[235] As of today, Switzerland has not banned Huawei from 5G networks and appears unlikely to do so. Sunrise, its major carrier, has launched 5G network with Huawei, while Swisscom has chosen Ericsson as its supplier.

For Europe, a region with a longstanding military and economic partnership with the US, the appeal to ban Huawei has found little support. For the political and economic union of the EU, collective action towards 5G networks has focused on harmonising cybersecurity, risk assessment and mitigation strategies–without placing a ban on Chinese equipment. While EU's reports acknowledge that 5G networks could be susceptible to influence by a foreign country–a clear acknowledgment towards suspicions regarding Huawei–it has left the decision of banning the company to individual member states.

Among members of the EU, the response to the Huawei question has varied widely. Germany, France, Italy and Spain have not placed a prohibition on the company, while Estonia, Romania and Poland consider Huawei's kit with mistrust. Regardless of individual responses, EU countries have put in place law and policy measures to strengthen cybersecurity, check foreign influence, and establish stringent checks for 5G equipment. Outside the EU, Norway has expressed concerns regarding Huawei. On the other hand, Switzerland, which categorically recognised its limitations as a middle power, believes that it has more to gain by steering clear of the technological cold war between US and China.

B. Asia and the Indo-Pacific

Countries in the Asia and Indo-Pacific region represent an interesting inflection point for the ongoing rivalry between US and China. In terms of economic capacity, technological advancement and current status of telecommunications, 5G deployment in the region will vary. While developed markets like South Korea, Japan and New Zealand will be at the forefront to deploy commercial 5G networks, other countries such as Malaysia and Indonesia are likely to be late adopters of the technology (Fig. 5).

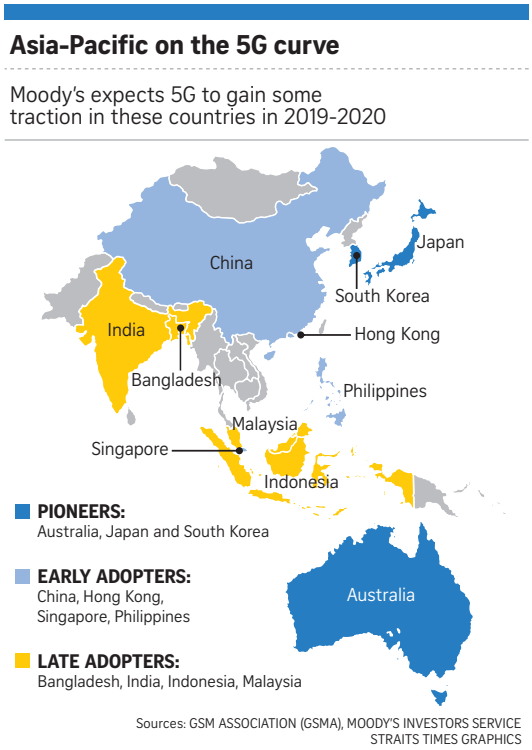
In this region, however, China's geographical proximity, backed by its vast territorial reach, economic prowess and military power will play a key role in influencing national policies on allowing Huawei in 5G networks. China's expanding trading relationships–supported by FTAs (free trade agreements)–its investments, foreign aid, as well as ongoing technology partnerships will weigh against a ban on Chinese technology companies. Beijing is also important to the region due to its infrastructure and connectivity initiatives, such as China's Belt and Road initiative (BRI) which, according to a study, will increase the GDP of East Asian and Pacific developing countries by

233 "Semi-annual report 2018/2", Reporting and Analysis Centre for Information Assurance (MELANI), Switzerland, 2018, 15, https://www.melani.admin.ch/melani/en/home/dokumentation/reports/situation-reports/semi-annual-report-2018-2.html.

234 *Ibid.,* 49-50.

235 Jessica Davis Plüss and Jie Guo Zehnder, "5G tests Switzerland's limits on cybersecurity", *Swiss Info,* October 18, 2019, https://www.swissinfo.ch/eng/safe-bet-_5g-tests-switzerland-s-limits-on-cybersecurity/45298646.

Fig. 5. Estimated 5G Deployments in Asia and the Indo-Pacific



Source: Claire Huang, "The fuss over 5G", The Straits Times, December 20, 2018, https://www.straitstimes.com/asia/the-fuss-over-5g.

2.6 percent to 3.9 percent on average.[236] Consequently, the BRI is witnessing the participation of major Asian countries (Fig. 6), with members of ASEAN, namely Indonesia (US$171bn), Vietnam (US$152bn), Cambodia (US$104bn), Malaysia (US$98bn) and Singapore (US$70bn) seeing the largest BRI related capital flow.[237]

Fig 6. China's Belt and Road Initiative (BRI) in Asia

Source: "Debate: What China's new Silk Road means for Europe", Geopolitical Intelligence Services, November 27, 2017, https://gisreportsonline.com/debate-what-chinas-new-silk-road-means-for-europe,2425,c.html.

236 "Belt and Road Initiative ensures all parties gain real benefits: report", *Xinhua News Agency,* April 22, 2019, http://www.xinhuanet.com/english/2019-04/22/c_137998950.htm.

237 LSE Ideas and CIMB ASEAN Research Institute, "China's Belt and Road Initiative (BRI) and Southeast Asia", October 2018, 6, http://www.lse.ac.uk/ideas/Assets/Documents/reports/LSE-IDEAS-China-SEA-BRI.pdf.

On the other hand, though US reach in the region is influential, it has largely remained relevant for countries that wish to contain China and its aggressive overtures in the South China Sea, Indo-Pacific and the East China Sea. With China's large footprint in the region, it is difficult to see a Huawei ban in national 5G networks. While some, such as Japan, South Korea and New Zealand may feel inclined to ban Huawei and other Chinese technology companies due to their close ties with the US, others may not adopt such an assertive approach given the economic costs associated 5G deployment, and the influence that Beijing may hold over them as the strongest economic, political and military neighbour in the region. Further, the fact that US aid and assistance is often conditioned on democracy and human rights reforms does not resonate with several governments in the region, who have gradually adopted authoritarian features of governance. Individual country dynamics with both Washington and Beijing, along with prevailing national priorities to swiftly rollout 5G networks will guide the 5G dilemma in Asia and the Indo-Pacific.

Table 19. Details of commercial 5G deployments in Asia and the Indo-Pacific

Country	Telecom Operator	5G equipment vendor
South Korea	KT	Ericsson and Samsung
	SK Telecom	Ericsson
	LG U+	Huawei, Ericsson, Samsung, Nokia
New Zealand	Vodafone New Zealand	Nokia
Maldives	Dhiraagu	Huawei
Thailand	Advanced Info Service (AIS)	MoU with Huawei for 5G services
	True Corp	News reports do not reveal name of supplier

Source: News reports and company websites

South Korea is one of the first countries to launch commercial 5G services on a nationwide basis. By April 2019, all three of its major mobile operators–SK Telecom, KT Corp and LG Uplus–launched commercial 5G services to consumers.[238] Two factors were vital for Seoul's early 5G deployment, namely a favourable environment (such as infrastructure cost sharing) coupled with the highest subscriber base and mobile penetration rate in the continental Asia region. SK Telecom and KT have used Ericsson's equipment; though LG Uplus uses Huawei equipment, it has announced that it will scale up the use of Samsung and Ericsson (Table 19).[239] Nonetheless, South Korean operators have been tight-lipped about the use of Huawei, and the government response has been largely subdued.[240]

In this region, South Korea's strategic and foreign policy interests are influenced by a complex host of factors, such as its needs to balance its relations with the US and Japan, and also address potential economic and military threats from China. South Korea is aware of the economic threat that China could pose to it; following its 2017 establishment of the Terminal High Altitude Area Defense (THAAD) system, Beijing

238 "The Mobile Economy: Asia Pacific", *GSMA Intelligence*, 2019, 12, https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_APAC.pdf.

239 Cho Mu-Hyun, "LG Uplus expands 5G coverage with Samsung equipment", *ZD Net,* May 6, 2019, https://www.zdnet.com/article/lg-uplus-expands-5g-coverage-with-samsung-equipment/.

240 J. James Kim, "Opportunities and Challenges for South Korea in the New Era of 5G", *The Asan Institute for Policy Studies,* March 21, 2019, http://en.asaninst.org/contents/opportunities-and-challenges-for-south-korea-in-the-new-era-of-5g/.

retaliated with trade-restrictive measures on Korea's tourism and distribution service companies.[241] China is important to South Korea; they have a free trade agreement between them, and Beijing is Seoul's top export destination.[242] Further, an overriding factor is its relations with North Korea, for which its partnership with Beijing becomes particularly important. In a trilateral meeting between South Korea, China and Japan in December 2019, both Seoul and Beijing reaffirmed their commitment to maintaining the momentum of North-Korea US dialogue.[243] While the US has urged South Korea to reject Huawei products, a government response in this direction has not been forthcoming.

In ***New Zealand***, the government is yet to announce its official position on Huawei's entry in its 5G network. In November 2018 however, the country's intelligence agency—Government Communications Security Bureau (GCSB)—prohibited telecommunications service provider, Spark, from using Huawei's equipment in its 5G network on grounds of national security.[244] GCSB is empowered by the Telecommunications (Interception Capability and Security) Act 2013 (TICSA)[245] to administer New Zealand's telecommunications network security. Part 3 of the TICSA requires network operators to notify the GCSB of any proposed changes to their network infrastructure within areas of specified security interest. Accordingly, the GCSB undertook an assessment of Huawei, and informed Spark that a significant network security risk was identified in the equipment.[246] Later, in 2019, China's *Global Times* reported that New Zealand's position on Huawei has "relaxed", since Spark announced a private 5G trial with Huawei.[247] New Zealand's GCSB published a clarification, saying that the report was misleading and that there has been no change in its current stand on the Chinese company.[248]

Wellington's position can be attributed to two factors: first, concerns regarding the rise of incidents of state-sponsored cyberattacks. New Zealand's National Cyber Security Centre (NCSC), noted that 39 percent of cybersecurity incidents were linked to known state-sponsored cyber actors, and that such incidents have registered a nearly 10 percent rise from the previous year.[249] It publicly attributed two of these threats to China and Russia, and found that these cybersecurity incidents were designed to generate revenue, disrupt businesses, undermine democracy or facilitate theft of intellectual property.[250] The second factor would be New Zealand's membership of the Five eyes alliance. However, Prime Minister Jacinda Ardern has publicly stated that Wellington is yet to have a final say on Huawei, and that it will not be a "political decision".[251]

---

241 "China denies Thaad retaliation against South Korea: WTO report", *The Straits Times,* October 23, 2017, https://www.straitstimes.com/asia/east-asia/china-denies-thaad-retaliation-against-south-korea-wto-report.

242 South Korea, *The Observatory of Economic Complexity,* accessed March 26, 2020, https://oec.world/en/profile/country/kor/.

243 Zehra Nur Duz, "South Korea, China agree to advance bilateral relations", *Anadolu Agency,* December 23, 2019, https://www.aa.com.tr/en/asia-pacific/south-korea-china-agree-to-advance-bilateral-relations/1681798.

244 Fumi Matsumoto, "New Zealand's 5G plan 'not a political decision'", *Nikkei Asian Review,* September 19, 2019, https://asia.nikkei.com/Editor-s-Picks/Interview/New-Zealand-s-5G-plan-not-a-political-decision.

245 "Annual Report", Government Communications Security Bureau (New Zealand), 2018, 22, https://www.gcsb.govt.nz/assets/GCSB-Annual-Reports/2018-GCSB-Annual-Report.pdf.

246 "Opening statement to the Intelligence and Security Committee", Government Communications Security Bureau (New Zealand), February 20, 2019, https://www.gcsb.govt.nz/news/opening-statement-to-the-intelligence-and-secuirty-committee/.

247 Harrison Christian, "Chinese media reports 'softening' of Huawei 5G ban in NZ", *Stuff,* November 12, 2019, https://www.stuff.co.nz/business/117327656/chinese-media-reports-softening-of-huawei-5g-ban-in-nz.

248 *Ibid.*

249 "Opening statement to the Intelligence and Security Committee", *op. cit.*

250 Cyber Threat Report 2018/19, National Cyber Security Centre, Government Communications Security Bureau (New Zealand), 6, https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Cyber-Threat-Report-2018-2019.pdf.

251 Fumi Matsumoto, "New Zealand's 5G plan 'not a political decision", *Nikkei Asian Review,* September 19, 2019, https://asia.nikkei.com/Editor-s-Picks/Interview/New-Zealand-s-5G-plan-not-a-political-decision.

Singapore's overall 5G vision and strategy is framed by the Infocomm Media Development Authority (IMDA), which is a statutory board under the Ministry of Communications and Information.[252] In its policy, it vouches to follow principles such as "Defence-in-Depth" and "Zero-Trust Environment", where the former refers to layering defence mechanisms to protect critical information, while the latter means that no equipment is trusted automatically and all are subject to stringent verification requirements. The policy also requires 5G networks to meet key resilience and security requirements, and subject their equipment to independent security testing in accordance with international standards.[253]

Singapore has not yet made any decision on the Huawei question, however the company did take part in IMDA's public consultations with industry players and individuals over 5G. Singapore's Foreign Minister Vivian Balakrishnan notes that as competition between the US and China intensifies, Singapore has to "avoid choosing sides and instead find ways to deepen and enhance cooperation with both parties". The US and Singapore have a 2004 FTA, and Washington is the island nation's largest foreign direct investor by country. Singapore is also China's largest foreign investor, and enjoys robust economic ties with the country, but differs on the South China Sea dispute. As such, it remains to be seen if Singapore will ban Huawei from its 5G networks.

In ***Japan***, the Radio Policy Vision Council of the Ministry of Internal Affairs and Communications presented the roadmap for 5G in 2014. Following the establishment of the 5GMF (5G Mobile Forum) in September 2014, Japanese operators target the launch of 5G for August 2020 in time for hosting the Summer Olympic and Paralympic Games.[254]

However, a December 2018 policy excluded telecommunications equipment that could be embedded with "malicious functions including information theft and destruction", from public procurement.[255] Though no companies were named in the document, the directive is expected to exclude both Huawei and ZTE from public procurement.[256] This prohibition was extended to businesses and other organisations handling key infrastructure in 14 sectors, such as power grids and railways.[257]

Till now, Japan's major telecom operators like NTT Docomo and Softbank Group have carried out testing and trials with Huawei (Table 20).[258] However, in May 2019, Softbank Group eventually selected Nokia and Ericsson as its vendors, excluding long time

---

252 "Ahead Of The Curve: Singapore's Approach To 5G", Infocomm Media Development Authority, Ministry of Communications and Information (Singapore), October 17, 2019, https://www.imda.gov.sg/-/media/Imda/Files/About/Media-Releases/2019/Annex-A---5G-Policy-and-Use-Cases.pdf.

253 "Policy For Fifth-Generation (5G) Mobile Networks And Services In Singapore", Infocomm Media Development Authority, Ministry of Communications and Information (Singapore), October 17, 2019, 5, https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/Consultations/Consultation-Papers/Second-Public-Consultation-on-5G-Mobile-Services-and-Networks/5G-Second-Consultation-Executive-Summary.pdf; "Roll-Out Of 5G Telecommunication Services From 2020", Reply of S Iswaran, Minister for Communications and Information (Singapore) to Parliamentary Question, https://sprs.parl.gov.sg/search/sprs3topic?reportid=written-answer-5394.

254 "Major International 5G Trials And Pilots", *European 5G Observatory,* accessed March 26, 2020, https://5gobservatory.eu/5g-trial/major-international-5g-trials-and-pilots/#1535643083453-4f945012-8813.

255 "Japan sets policy that will block Huawei and ZTE from public procurement as of April", *The Japan Times,* December 10, 2018, https://www.japantimes.co.jp/news/2018/12/10/business/japan-sets-policy-will-block-huawei-zte-public-procurement-april/#.Xb7StC2B3q3.

256 *Ibid.*

257 Yukio Tajima, Yusuke Hinata and Minoru Satake, "Japan moves to keep Huawei out of power grids and railways", *Nikkei Asian Review,* December 13, 2018, https://asia.nikkei.com/Politics/Japan-moves-to-keep-Huawei-out-of-power-grids-and-railways.

258 "NTT DOCOMO 5G Trials: List of Publications", *NTT Docomo,* March 14, 2018, https://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/rd/tech/5g/docomo_5GTrials_List_of_Publications_English.pdf.

suppliers Huawei and ZTE.[259] Other carriers like NTT Docomo and KDDI also decided to not use Chinese equipment in their 5G networks due to rising security concerns that spurred the Japanese government to block Huawei Technologies and other Chinese companies from public procurement.[260] Thus, the government's policy measures made major telecom operators risk averse to using Huawei's equipment in their 5G build-up–effectively resulting in an implicit Huawei ban. Given Tokyo's enduring partnership with Washington, it remains to be seen if Japan would enforce an explicit ban. But recent developments, such as Trump's withdrawal from the Trans-Pacific Partnership, impediments in bilateral trade talks and tough rhetoric on the cost of US basing agreements in Japan have created difficulties in bilateral ties.[261] As a result, Tokyo's increasing rapprochement with Beijing supported by the need to maintain positive economic ties,[262] may indicate that Japan will maintain the status quo of not taking a hard stance.

Table 20. Publicly announced 5G trials with Huawei or ZTE in Asia and the Indo-Pacific

Country	Trials with Huawei or ZTE
Singapore	M1[263]
Japan	NTT Docomo and Softbank
South Korea	LG Uplus
Sri Lanka	Dialog Axiata, Mobitel and Sri Lanka Telecom
Myanmar	Mytel
Thailand	TOT Public Company Ltd., and True Move
Indonesia	Telkomsel, XL Axiata, Telekom Indonesia and Smartfren
Bangladesh	Bangladesh's Ministry of Posts, Telecommunications and Information Technology and Robi

Source: News reports and company websites

In ***Vietnam***, major mobile carriers like Viettel, are exploring options instead of Huawei,[264] and have carried out trials with Nokia and Ericsson. Viettel—a state owned enterprise operated by Vietnam's ministry of defence—has also announced that it has developed its own 5G equipment and plans to begin mass production of hardware and software by 2020-21. However, analysts remain sceptical of this declaration; firstly, because other vendors have spent large amounts of money to develop 5G technology and it is difficult for Viettel's R&D budget to compete with this, and secondly, because it will be financially unrealistic for the company to manufacture and sell its infrastructure since it will have to pay patent and royalty fees to other suppliers.[265]

259 "Huawei loses key 5G contract in Japan to Nokia and Ericsson", *The Straits Times,* May 31, 2019, https://www.straitstimes.com/asia/east-asia/huawei-loses-key-5g-contract-in-japan-to-nokia-and-ericsson.

260 Minoru Satake, "Japan's 4 carriers to shun Chinese 5G tech", *Nikkei Asian Review,* December 10, 2018, https://asia.nikkei.com/Business/Companies/Japan-s-4-carriers-to-shun-Chinese-5G-tech.

261 Eleanor Albert, "China and Japan's Rapprochement Continues – For Now", *The Diplomat,* May 16, 2019, https://thediplomat.com/2019/05/china-and-japans-rapprochement-continues-for-now/.

262 Zijia He, "A Friend of a Friend: How Better China-Japan Relations Benefit the United States" in New Perspectives in Foreign Policy, Issue 17, April 8, 2019, https://www.csis.org/friend-friend-how-better-china-japan-relations-benefit-united-states.

263 Corinne Reichert, "Huawei conducts 5G trials in Singapore with M1", *ZD Net,* June 21, 2018, https://www.zdnet.com/article/huawei-conducts-5g-trials-in-singapore-with-m1/.

264 "Vietnam quietly avoids Huawei in building 5G network", *Bangkok Post,* July 19, 2019, https://www.bangkokpost.com/tech/1715339/vietnam-quietly-avoids-huawei-in-building-5g-network.

265 Leo Kelion, "Vietnamese firm Viettel's 5G claim raises eyebrows outside", *BBC News,* January 20, 2020, https://www.bbc.com/news/technology-51178369.

It is believed that this cautious stand is attributed to Hanoi's sour relations with Beijing on the question of South China Sea, East Sea and the 2014 construction of an oilrig off the coast of Vietnam.[266] While no official government statement has been issued on Huawei and 5G, Vietnam–for now–appears to be joining the US camp.

In ***Thailand*****,** Huawei has established strong relations with the current government. The government's 2017 white paper on digitalisation of the Thailand industry was prepared in association with Huawei. Further, the flagship national development model called "Thailand 4.0", which prescribes the use of technology and innovation to become a high-income economy, also took direction from Huawei Technologies.[267] Huawei is an important contributor to Thailand's ICT industry, and has participated in its build-up of 2G, 3G and 4G networks.[268] One of the biggest initiatives by the Chinese telecom giant is the inaugural of a 5G test bed in Chonburi, the heart of the Thai military government's $45 billion Eastern Economic Corridor (EEC), which places Huawei at the centre of Thailand's 5G strategy. Huawei partnerships extend to Bangkok's telecom operators as well; for instance, it has signed an MoU with the Thailand-based mobile service operator Advanced Info Service (AIS) to mobilise 5G technology and services. AIS and True Corp have launched commercial 5G services in Thailand, but news reports do not reveal the name of their equipment supplier.

During the Cold War era, Thailand developed and maintained a treaty alliance with the US and became reliant on its military assistance and weaponry. However, it has been increasingly developing its partnership with China, as the Thai military–with the support of the monarchy–is gaining greater prominence in the country. Democratic politics in the region is being replaced by authoritarianism. As such, Bangkok has been deepening its defence partnership with Beijing, and has contracted with China to buy an amphibious ship, cruise missiles, and anti-ship missiles.[269] As Thailand's ties with China progresses–in the absence of shared strategic interests with the US–Huawei will prove to be central to the Thai 5G network.

Philippines has long been a part of America's network of alliances in the Asia-Pacific. Amid China's increasing military assertiveness, the two allies have maintained robust bilateral security cooperation governed by various military agreements such as the 1951 Mutual Defense Treaty (MDT) and the 2014 Enhanced Defense Cooperation Agreement (EDCA), through which the US enjoys access to Philippines' strategic bases.[270] The biggest hurdle to bilateral ties between Manila and Beijing came in the form of the 2013 arbitration by Philippines to the Permanent Court of Arbitration (PCA) on the South China Sea dispute–where the PCA's award invalidated China's expansive "nine-dash line" claim over the entirety of the South China Sea.

However, current Philippine President Rodrigo Duterte has undertaken a policy of rapprochement towards China, which is reflected in Manila's approach to 5G networks. Philippines' telecom operators, Globe Telecom and Smart Communications, have welcomed the adoption of Huawei's 5G technology, while a deal has also been struck to

---

266 "SE Asia remains open to Huawei 5G", *The Phnom Penh Post*, August 8, 2019, https://www.phnompenhpost.com/business/se-asia-remains-open-huawei-5g.

267 "Insights on Digitalization of Thailand Industry: Digital Roadmap for Aging Society", White Paper by the Government of Thailand, February 2017,

Agriculture, and Tourism https://www-file.huawei.com/-/media/corporate/pdf/market-trends/thailand_digitalization_whitepaper_en_new.pdf?la=en-us.

268 Big Bang 2019, Digital Thailand, accessed March 26, 2020, http://www.digitalthailandbigbang.com/.

269 Zachary Abuza, "America should be realistic about its alliance with Thailand", *War on the Rocks,* January 2, 2020, https://warontherocks.com/2020/01/america-should-be-realistic-about-its-alliance-with-thailand/.

270 Richard Javad Heydarian, "Ignoring the US, Philippines goes with Huawei", *Asia Times,* July 18, 2019, https://asiatimes.com/2019/07/ignoring-the-us-philippines-goes-with-huawei/.

introduce China Telecom–a major Chinese telecom operator–to begin providing mobile and broadband services in the country.[271] However, not all within the government are happy with this decision. In September 2019, Risa Hontiveros a senator in Philippines moved a resolution to question the presence of Chinese telecom providers' facilities and equipment in Philippines military base and installation, arguing that it would undermine the nation's national security.[272]

In October 2019, Huawei officially become a hardware supplier for ***Malaysia's*** Maxis for its 5G network rollout.[273] Previously, in May 2019, former Malaysian Prime Minister Mahathir Mohamad said that his country tries to use Huawei technology "as much as possible," and criticised the US for actions he described as seeking confrontation with China in both trade and security.[274] Mohamad recognised that Malaysia is caught between the ongoing trade war between US and China, but is also aware of the limitations that Malaysia faces in taking China head on. With respect to Malaysia's inclination to participate in BRI projects and seeking Chinese loans, he has said that "...we all realise that we have to deal with China jointly, because that gives us more strength" and that "...we are not really strong enough to tell the Chinese, 'No, you should not do this kind of thing, it is the international law...'".[275] In February 2020, however, Malaysia's communications minister adopted a cautious stand saying they were aware of "concerns that have been expressed around the world", and they will implement security standards that will dictate which companies take part in the 5G rollout.[276]

In ***Brunei Darussalam***, DST communications—the largest telecom leader in the country—launched 4G with Huawei's help in 2016, and in February 2019, Huawei technologies publicly stated that it is keen to work with telecommunication companies and authorities to set up a 5G network.[277]

So far, higher officials in the ***Kingdom of Cambodia*** have come out with statements in support of using Chinese technology. In March 2019, Digital Cambodia was organised in Phnom Penh, celebrating 20 years for Huawei in Cambodia. In the event, Huawei won the title of "Best Technology Vendor of the Year 2019". In April 2019, a Memorandum of Understanding was signed between Huawei and Cambodia to build Cambodia's 5G Networks.[278] In August 2019, Telecommunication Regulator of Cambodia (TRC) spokesperson Im Vutha said that since Cambodia is a free market, firms are not barred from working together.[279] Smart Axiata, a major telecom operator, has said it will use Huawei equipment for its network, while Cellcard, a telco owned by Cambodian conglomerate Royal Group will choose ZTE. Metfone, another major mobile

---

271 "Mislatel signs deal with China Telecom for third telco", *CNN,* April 29, 2019, https://cnnphilippines.com/business/2019/4/29/Mislatel-China-Telecom.html.

272 "Resolution calling for an investigation in aid of legislation into whether or not the presence of a foreign telecommunications provider's facilities and equipment in Philippine Military bases and installations undermines National Security", Introduced by Senator Risa Hontiveros, Eighteenth Congress of the Republic of Philippines, https://www.senate.gov.ph/lisdata/3155228402!.pdf.

273 P Prem Kumar, "Huawei officially lands role in Malaysia's 5G rollout", *Nikkei Asian Review,* October 3, 2019, https://asia.nikkei.com/Spotlight/5G-networks/Huawei-officially-lands-role-in-Malaysia-s-5G-rollout.

274 Kelly Olsen, "Malaysia's Mahathir: We try to use Huawei technology 'as much as possible'", *CNBC,* May 30, 2019, https://www.cnbc.com/2019/05/30/mahathir-we-try-to-use-huawei-technology-as-much-as-possible.html.

275 Marrian Zhou, "Mahathir: ''We have to go to the Chinese'' for infrastructure", *Nikkei Asian Review,* September 27, 2019, https://asia.nikkei.com/Politics/International-relations/Mahathir-We-have-to-go-to-the-Chinese-for-infrastructure2.

276 Joseph Sipalan and Krishna N Das, "Malaysia to choose 5G partners based on own security standards", *Reuters,* February 17, 2020, https://www.reuters.com/article/us-telecoms-5g-malaysia-huawei/malaysia-to-choose-5g-partners-based-on-own-security-standards-idUSKBN20B0TV.

277 "Huawei wants to develop 5G network with Brunei", *The Bruneian,* thebruneian.news/huawei-wants-to-develop-5g-network-with-brunei/.

278 "Government and Huawei ink MoU on 5G network", *The Phnom Penh Post,* April 29, 2019, https://www.phnompenhpost.com/business/government-and-huawei-ink-mou-5g-network.

279 Thou Vireak, "Metfone to use Huawei's 5G technology for network", *The Phnom Penh Post,* August 27, 2019, https://www.phnompenhpost.com/business/metfone-use-huaweis-5g-technology-network.

operator in Cambodia has also confirmed that it plans to use Huawei technologies in its 5G rollout.[280]

In Cambodia, US foreign assistance—which has totalled over US$77.6 million by 2014—has been critical for programmes in health, education, governance, economic growth, and demining of unexploded ordnance.[281] Here, the US dollar and Cambodian currency riel is used in the country interchangeably. But Phnom Penh has moved closer to Beijing, with more than $2 billion of approved investment coming from China in 2018 alone, according to the World Bank.[282] Cambodia's current Prime Minister Hun Sen has moved closer to Beijing because Washington's focus on democratic institutions and human rights was not faring well with his authoritarian style of governance. Given these factors, Phnom Penh will not ban Chinese technology companies in the region.

In ***Indonesia***, no government position has been expressed yet to exclude Chinese equipment suppliers from the country. In October 2019, it was reported that Indonesia's communications ministry officials were in "no rush" to adopt the next-gen wireless technology. Some of the reasons cited by the Communications Minister Rudiantara are the lack of available frequency spectrum for 5G use and a price sensitive market, where consumers may not be willing to pay the high fees for 5G services.[283]

Currently, most telecom vendors in Indonesia are following a multi-vendor model when it comes to 5G deployment. Telkomsel and XL Axiata signed a contract with Ericsson for core network upgrades to prepare for 5G, but also conducted trials with Huawei during the Asian Games 2018 in Jakarta. In 2019, Telekom Indonesia and Huawei signed an MoU on 5G; they agreed to conduct a 5G Joint Innovation Program and collaborate in providing public cloud services in the Indonesian market.[284] ZTE, on the other hands, has announced its partnership with Smartfren and Telkom. No Indonesian officials or telecom companies have ruled out partnering with Huawei.

Bangladesh has one of the lowest internet penetration levels in the region and faces a significant digital divide: only one in five Bangladeshis subscribed to mobile internet services in 2017, despite 3G networks covering in excess of 90 percent of the population. Given the ground reality in Bangladesh, early adoption of 5G at this stage is a distant dream; in fact, the President of the Bangladesh Mobile Phone Consumers' Association (BMPCA) in September 2019 said that the current status and quality of telecom network in Bangladesh is below expected levels, and that state run mobile operator Teletalk is yet to provide its own 4G network. [285]

Nonetheless, Huawei along with Bangladesh Government's Posts & Telecommunications Division and Robi, demonstrated 5G technology for the first time in Bangladesh.[286] In November 2019, Chinese news agency Xinhua reported that

---

280 *Ibid.*

281 "U.S. Relations With Cambodia", Bureau of East Asian and Pacific Affairs, US Department of State, August 15, 2018, https://www.state.gov/u-s-relations-with-cambodia/.

282 "Cambodia Economic Update", *World Bank Group,* May 2019, 23, http://documents.worldbank.org/curated/en/843251556908260855/pdf/Cambodia-Economic-Update-Recent-Economic-Developments-and-Outlook.pdf; Ten Soksreinith, "Experts Say US-Cambodia Relationship at "Crisis Point"", *Voice of America*, August 27, 2019, https://www.voacambodia.com/a/experts-say-us-Cambodia-relationship-at-crisis-point/5058503.html.

283 Erwida Maulia, "Mixed signals: as Indonesia''s 5G race heats up, government says 'no rush'", *Nikkei Asian Review,* October 2, 2019, https://asia.nikkei.com/Spotlight/5G-networks/Mixed-signals-as-Indonesia-s-5G-race-heats-up-government-says-no-rush.

284 "Telkom and Huawei Tied Agreement on 5G and Cloud Joint Innov", *Huawei Cloud,* November 12, 2019, https://www.huaweicloud.com/intl/en-us/news/20191112161435303.html.

285 "BMPCA: 5G launch will deceive mobile phone subscribers", *Dhaka Tribune,* September 3, 2019, https://www.dhakatribune.com/bangladesh/dhaka/2019/09/03/bmpca-5g-launch-will-deceive-mobile-phone-subscribers.

286 Zhang Shasha, "Huawei Demonstrates 5G Technology in Bangladesh", *Beijing Review,* July 25, 2018, http://www.bjreview.com/Business/201807/t20180726_800136580.html.

Huawei is all set to facilitate Bangladesh with technical support in the implementation of 5G networks.[287] The Chinese telecom giant has also been a part of development initiatives in Bangladesh, such as digital buses.[288]

5G is currently a distant reality for Dhaka. However, its ongoing initiatives in partnership with Huawei, and affordable equipment make it a lucrative option for Bangladesh's future 5G networks.

In ***Sri Lanka***, Western diplomats reportedly raised concerns regarding Huawei to former telecom minister Harin Fernando. However, Huawei has been operational in Sri Lanka for 20 years and is a major part of the country's commercial 4G and 4G-LTE build-up. In response, Fernando noted that concerns regarding Huawei were not concrete enough to act upon. Sri Lankan carriers, namely Dialog Axiata, Mobitel and Sri Lanka Telecom conducted trials with Huawei and Ericsson[289]. Sri Lanka Telecom–signed an MoU with Huawei to facilitate the digital transformation of Sri Lanka via the implementation of a range of digital initiatives, including the "Digital Sri Lanka initiative".[290]

Both US and India, are keen on containing China's footprint in Sri Lanka in order to establish a free and open Indo-Pacific. However, there has been a large inflow of Chinese investments and loans in the region, in the aftermath of the Sri Lankan civil war. This happened at a time when Colombo was facing increasing criticism for its human rights violations and found itself diplomatically and economically isolated. This created space for Beijing to come to Sri Lanka's aid by providing financial loans, military equipment, as well as infrastructure financing. Various infrastructure development initiatives, such as the Hambantota port and the Mattala Rajapaksa International Airport have vastly increased the debt that Sri Lanka owed to China.[291] Given Colombo's economic imperatives and its large debt to Beijing, it is unlikely that Huawei will be banned in the country.

For ***Pakistan***, Minister for Science and Technology, Fawad Chaudhary has said that Huawei will soon launch Pakistan's 5G network.[292] Huawei has also participated in various development initiatives and partnerships with Islamabad over the years (Table 21). Courtesy investments through the China-Pakistan economic corridor and Beijing's support to Islamabad in international forums, Huawei is likely to be part of future 5G network.

---

287 "Huawei all set for 5G technical support in Bangladesh", *Xinhua News Agency,* November 9, 2019, http://www.xinhuanet.com/english/2019-11/09/c_138541799.htm.

288 "Robi Axiata, Huawei, launch ICT training buses for women in Bangladesh", *Disruptive Asia,* October 24, 2016, https://disruptive.asia/robi-axiata-huawei-ict-training-women/.

289 "Dialog Axiata Trials 5G for the First Time in South Asia", *Dialog,* August 22, 2017, https://www.dialog.lk/dialog-axiata-trials-5g-for-the-first-time-in-south-asia/; "Mobitel 5G Becomes the First and Fastest in South Asia!", *Mobitel,* June 2019, https://www.mobitel.lk/press-releases/mobitel-5g-becomes-the-first-and-fastest-in-south-asia; "SLT Becomes the First Telco to Successfully Field Test Pre-5G LTE Advanced Pro Technology in South Asia", *Sri Lanka Telecom,* accessed March 26, 2020, https://www.slt.lk/en/content/slt-becomes-first-telco-successfully-field-test-pre-5g-lte-advanced-pro-technology-south.

290 "SLT & Huawei sign MoU to support "Digital Sri Lanka Initiatives"", *Sri Lanka Telecom,* accessed March 26, 2020, https://www.slt.lk/en/content/slt-huawei-sign-mou-support-%E2%80%9Cdigital-sri-lanka-initiatives%E2%80%9D.

291 Matt Ferchen And Anarkalee Perera, "Why Unsustainable Chinese Infrastructure Deals Are a Two-Way Street", *Carnegia-Tsinghua Centre for Global Policy,* July 2019, https://carnegieendowment.org/files/7-15-19_Ferchen_Debt_Trap.pdf.

292 https://www.techjuice.pk/huawei-5g-launch-date-in-pakistan-fawad-ch/

Table 21. Huawei's soft power initiatives in Asia and Indo-Pacific

Country	Name and Description of Initiative
Thailand	Huawei aims to build its leading cloud data centre in Southeast Asia in Thailand's Eastern Economic Corridor (EEC) with an initial budget of $10 million.[293] It has also launched a 5G test bed in Chonburi, which is a part of the EEC. MoU with Thailand government on public-private collaboration to develop the government's big data ecosystem, train talented people working in information and communications technology (ICT) and facilitate the growth of local SMEs and startups. Huawei's OpenLab in Bangkok created with a total investment of $15 million and provides industry solutions for the IOT, Big Data, and cloud computing.
Cambodia	Memorandum of Understanding signed between Huawei and Cambodia to build Cambodia's 5G Networks. Cambodian students also participated in Huawei's Seeds for the future program.[294]
Philippines	Huawei and Polytechnic University of the Philippines (PUP) entered into a Memorandum of Agreement for the development of the Huawei Digital Academy, ICT Research Projects and to also conduct a joint study on improving Internet connectivity in the PUP main campus and its branches.[295]
Singapore	Huawei launched a $10 million, 5G-powered AI Lab to serve as a space for governments, universities and educational institutes to test, trial and train on technologies.
South Korea	Huawei unveiled an open lab for next generation 5G wireless network in South Korea in May 2019, with plans to invest about $5 million in the venture.[296]
Pakistan	MoU with Special Communications Organization (a public sector organisation operated by Ministry of Information Technology and Telecommunication and maintained by the Pakistan Army) to further strengthen cooperation in Pakistan.[297] Askari Bank signed an MoU, to further economic cooperation.[298] MoU to build a cloud data centre in Pakistan.

293 "Huawei to build cloud data centre in eastern corridor", *Bangkok Post,* November 18, 2017, https://www.bangkokpost.com/business/1362463/huawei-to-build-cloud-data-centre-in-eastern-corridor.

294 "Top 11 Cambodian Students visited Huawei HQ under 'Seeds for the Future Program'", *Khmer Times,* December 17, 2016, https://www.khmertimeskh.com/63118/top-11-cambodian-students-visited-huawei-hq-under-seeds-for-the-future-program/.

295 Li Xia, "China's Huawei, Philippine university ink agreement on cooperation", *Xinhua News Agency,* July 24, 2019, http://www.xinhuanet.com/english/2019-07/24/c_138254729.htm.

296 "Huawei launches 5G lab in South Korea, but keeps event low-key after US ban", *CNBC,* May 29, 2019, https://www.cnbc.com/2019/05/30/huawei-launches-5g-lab-in-south-korea-keeps-it-low-key-after-us-ban.html.

297 "Huawei and Pakistan' Special Communications Organization Sign MoU at MWC", *Pro Pakistani,* accessed March 27, 2020, https://propakistani.pk/2019/02/26/huawei-and-pakistan-special-communications-organization-sign-mou-at-mwc/.

298 "Askari Bank signs MoU with Huawei", *Pakistan Observer,* November 28, 2019, https://pakobserver.net/askari-bank-signs-mou-with-huawei/.

Country	Name and Description of Initiative
Malaysia	MoU with Maxis to develop 5G TechCity in Malaysia, to build 5G target network, incubate of new services with new business models.[299] MoUs with state government of Terengganu, CyberSecurity Malaysia, SME Corp Malaysia, and Universiti Malaysia Sabah (UMS), to work on research, development and digital transformation. Cybersecurity Malaysia (agency under the Ministry of Science, Technology and Innovation) will establish a steering committee with Huawei to discuss technical standards, technology innovation, and develop approaches to manage cyber threats.[300] Construction of OpenLab, which will serve as an open, flexible and secure platform for joint innovation with local partners. Huawei unveiled the Customer Solution Innovation & Integration Experience Centre (CSIC) in Kuala Lumpur to serve as ICT innovation hub and centre of excellence to drive industry open ecosystem and accelerate digital economy transformation in Malaysia.

Myanmar's telecom operator Mytel—reportedly controlled by Myanmar's military—conducted the first 5G test in the country with Huawei's equipment.[301] Smart Axiata, another leading telecom operator, has also conducted trials with Huawei.[302] In December 2018, Myanmar Posts and Telecommunications Department, in cooperation with Huawei, hosted the "Myanmar 5G Forum 2018" for stakeholders to discuss the future of Myanmar's 4G/5G market and its National Broadband White Paper 2019, for a successful migration towards 5G technology from 4G.[303]

Myanmar has strong relations with China, with Beijing having supplied economic support and military equipment to the erstwhile military junta to keep the army in power. In 2010, the military junta launched democratic reforms and welcomed two visits from US leaders.[304] However, following the Rohingya crisis in the Rakhine region in Myanmar, the region has grown closer to Beijing–given how it is willing to overlook human rights violations in its bilateral engagements.

In ***Nepal***, Communications Minister Gokul Prasad Baskota said that both 4G and 5G will be introduced in the country in a phased manner.[305] Later in 2019, *Bloomberg* reported that the affluent Binod Chaudhury–Nepal's first and only billionaire–has decided to partner with Huawei to build the nations 5G networks.[306] Presently, the region's three

299 "Maxis and Huawei collaborate on Malaysia's First Techcity", *Digital News Asia,* January 14, 2020, https://www.digitalnewsasia.com/digital-economy/maxis-and-huawei-collaborate-malaysias-first-techcity.

300 Corinne Reichert, "Huawei to underpin Malaysian tech roadmap and cybersecurity agenda", *ZD Net,* November 9, 2017, https://www.zdnet.com/article/huawei-to-underpin-malaysian-tech-roadmap-and-cybersecurity-agenda/.

301 Moe Myint, "Military-Backed Mytel Announces Successful Test of 5G Service", *The Irrawaddy,* August 5, 2019, https://www.irrawaddy.com/business/military-backed-mytel-announces-successful-test-5g-service.html.

302 "Smart Axiata, Huawei work on 5G network for Kingdom", *Eleven Myanmar,* January 20, 2020, https://eleven-myanmar.com/news/smart-axiata-huawei-work-on-5g-network-for-kingdom.

303 "Myanmar 5G Forum 2018", *Huawei,* December 20, 2018, https://www.huawei.com/mm/press-events/news/mm/2018/myanmar-5g-forum-eng.

304 Marvin C. Ott, "Myanmar in China's Embrace", *Foreign Policy Research Institute,* January 24, 2020, https://www.fpri.org/article/2020/01/myanmar-in-chinas-embrace/.

305 Speech of H.E. Gokul Prasad Baskota, Ministry of Communication and Information Technology (Nepal) at the Plenipotentiary Conference of International Telecommunication Union, October 31, 2018, https://www.itu.int/web/pp-18/en/speech/122.

306 Blake Schmidt, "Billionaire on Top of the World Chooses China's Huawei to Expand", *Bloomberg,* October 3, 2019, https://www.bloomberg.com/news/articles/2019-10-02/billionaire-on-top-of-the-world-chooses-china-s-huawei-to-expand?sref=NDAgb47j.

major telecoms—Nepal Telecom, Ncell and Smartcell—already use Huawei and ZTE equipment in their existing telecom infrastructure.[307]

Nepal's relations with China have witnessed an upswing in the past year. In October 2019, Xi Jinping became the first Chinese leader to visit Nepal in more than 20 years. On this occasion, 20 deals were signed and nearly $500 million in financial aid was pledged to Kathmandu.[308] In 2017, Nepal joined China's BRI project, while separate deals to build two railway links have also been concluded.[309] Though New Delhi has been Nepal's traditional ally, Beijing's ability to finance the region's infrastructure projects–minus a controversial "big brother" approach–make a positive case for the entry of Huawei in its 5G network.

The above discussion demonstrates that China's economic and military might in the region will play a persuasive role in national decisions on Huawei's entry in 5G networks. The importance of trade and investment ties, infrastructure projects, military partnerships and China's readiness to overlook human rights violations in bilateral relations contrasts with US' approach and establishes it as a preferred partner. Further, Huawei's existing initiatives and agreements with countries in Asia and the Indo-Pacific have enabled it to build strong ties with both public and private stakeholders, such as in Cambodia, Thailand and Malaysia. On the other hand, the importance of Washington's partnership is limited to a few countries for specific reasons, such as Japan for strategic considerations, and Vietnam for containing Chinese aggression in the South China Sea. As a result, the US' clarion call to ban Huawei has not been heeded by most. New Zealand, of course, is representative of an outlier in this section of the study, whose economic advancement, strong commitment to cybersecurity, membership of the Five eyes alliance and its physical distance from continental Asia, diminishes the full force of Chinese influence on the nation.

307 Arun Budhathoki, "Huawei gives China a technological edge in Nepal", *Asia Times,* July 26, 2019, https://asia-times.com/2019/07/huawei-gives-china-a-technological-edge-in-nepal/.

308 "China, Nepal sign trade, infrastructure and security deals", *Al Jazeera,* October 31, 2019, https://www.aljazeera.com/news/2019/10/china-nepal-sign-trade-infrastructure-security-deals-191013074901324.html.

309 *Ibid.*

CHAPTER 4.

The Situation in Other Regions

A. Middle East

As of February 2020, 10 telecom operators in economically advanced Gulf Cooperation Council (GCC) countries, namely Bahrain, Kuwait, Qatar, Saudi Arabia and the United Arab Emirates have commercially launched 5G.[310] Between May and June 2018, Etisalat (UAE), Ooredoo (Qatar), STC (Saudi Arabia) and Zain (Kuwait) launched 5G in their home markets, with various vendors including Huawei and ZTE.[311] No Middle Eastern country has come forth to ban Huawei and the region, in fact, has been one of the first to deploy 5G networks using Chinese telecom equipment.

Table 22 details mobile operators that have used Huawei and/or ZTE in their respective networks.

Table 22. 5G Commercial Launches in the Middle East with Huawei and ZTE equipment

Country	Telecom Operator
Bahrain	Viva (Bahrain), with Huawei
Kuwait	Viva (Kuwait Telecom Company), with Huawei
Qatar	Vodafone Qatar, with Huawei
Saudi Arabia	Saudi Telecom Company (STC), with Huawei, Ericsson, and Nokia
	Zain Saudi Arabia, with Huawei and Nokia
UAE	Du (Emirates Integrated Telecommunication Company, EITC), with Huawei and Nokia
	Etisalat UAE, with ZTE & Ericsson

Source: News reports and company websites.

These countries have been at the forefront of deploying 5G services; factors such as a sound policy framework, roadmaps, and an advanced market for 5G deployment have helped.[312] *Firstly*, state-led initiatives to support the development of 5G proved crucial in ensuring its early deployment. Government efforts to create a suitable regulatory environment, with a strong top down approach, driven by local governments have facilitated the adoption of the networks.[313] In Saudi Arabia, the government established the National 5G Task Force in early 2018 to prepare the necessary administrative foundation for supporting 5G deployment,[314] and complement Riyadh's "Vision 2030"

310 "5G and LTE Deployments", *5G Americas*, last updated March 17, 2020, https://www.5gamericas.org/wp-content/uploads/2020/01/MiddleEast.pdf.

311 John Calabrese, "The Huawei Wars and the 5G Revolution in the Gulf", *Middle East Institute,* July 30, 2019, https://www.mei.edu/publications/huawei-wars-and-5g-revolution-gulf.

312 "5G in the Middle East and Africa", *OVUM*, 2018, 3, https://www.omdia.com/~/media/informa-shop-window/tmt/whitepapers-and-pr/5g-in-the-middle-east-and-africa-pdf.pdf.

313 Samuel Abraham, "5G implementation: How the GCC nations leapfrogged the world", *International Finance,* November 13, 2019, https://internationalfinance.com/5g-implementation-how-the-gcc-nations-leapfrogged-the-world/.

314 "How Saudi Arabia is paving the way to be a regional leader in 5G", *International Telecommunications Union,* March 24, 2019, https://news.itu.int/how-saudi-arabia-is-paving-the-way-to-be-a-regional-leader-in-5g/.

plan, which aims to build a modern economy.[315] Other initiatives to harness the full potential of 5G technologies include the establishment of NEOM, the city of the future, to be built in the North-Western part of the Kingdom.[316] With an initial investment of $500 billion, the futuristic mega-city will be 33-times the size of New York, and will integrate next generation futuristic technologies, such as flying taxis, robot cleaners and artificial rain.[317] Here, mobile operator Zain KSA launched its 5G network at the Neom Bay Airport—an area regarded as Saudi Arabia's futuristic gateway.[318] Similarly, the UAE established the National 5G Committee, while other countries like Bahrain and Kuwait have adopted broader digital strategies–namely, the Vision 2030 and the Vision 2035–to promote information and communication technology development.[319]

Secondly, the GCC member countries are one of the richest countries in the Middle East and have a high GDP per capita, averaging at US$ 26,700.[320] This region has consumers with high purchasing power, thereby making it a big market for not only 5G services, but also 5G enabled smartphones.

Thirdly, GCC members have a substantially high subscriber penetration rate, which is indicative of a mature market that is ready to adopt advanced digital communications technology. Here, mobile subscribers comprise 76 percent of the population, with Bahrain, Kuwait and UAE having a subscriber penetration rate of 90 percent or above.[321] This is in contrast with other Arab states, where the average subscriber rate is at 46 percent. Constraints such as infrastructure, disruptions due to civil war, and high cost of phone data services (such as in Lebanon[322]) make it difficult to foresee an early and ubiquitous deployment of 5G commercial services in these areas.

This is not to say that other Middle Eastern countries have not made efforts towards adopting 5G technologies. Though countries like Lebanon, Jordan, Syria and Oman are yet to deploy 5G commercial services, they have succeeded on commencing trials, demonstrations of use cases and 5G spectrum allocations. In Libya, *touch*—a leading mobile operator—performed the first 5G trial in the nation with Huawei,[323] while Oman's Omantel has launched commercial 5G broadband services for residential customers.[324]

Lastly, the GCC has also made efforts to setup collaborations between stakeholders to streamline the adoption of 5G. For instance, in 2016 *du* (UAE) established a consortium of academic experts and global telecom vendors known as the 5G Innovation Gate

---

315 "Vision 2030", Kingdom of Saudi Arabia, 2017, https://vision2030.gov.sa/sites/default/files/report/Saudi_Vision2030_EN_2017.pdf.

316 How Saudi Arabia is paving the way to be a regional leader in 5G", *op. cit.*

317 Bill Bostock, "Everything we know about Neom, a 'mega-city' project in Saudi Arabia with plans for flying cars and robot dinosaurs", *Business Insider,* September 21, 2019, https://www.businessinsider.in/Everything-we-know-about-Neom-a-mega-city-project-in-Saudi-Arabia-with-plans-for-flying-cars-and-robot-dinosaurs/People-will-get-about-using-flying-taxis-Saudi-officials-say-/slideshow/71232428.cms.

318 "5G implementation: How the GCC nations leapfrogged the world", *op. cit.*

319 Turhan Muluk, "Enabling Policies for 5G and IoT", *International Telecommunications Union,* August 2019, https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2019/ETDubai/Intel%20-%20Enabling%20Policies%20for%205G%20and%20IoT.pdf.

320 "GDP Per capita", Statistical Centre for the Cooperation Council for the Arab Countries of the Gulf ("GCC-Stat"), accessed March 26, 2020, https://www.gccstat.org/en/.

321 "Middle East Mobile Operators Will Be 5G Early Adopters, According To New GSMA Report", *GSMA Intelligence,* March 26, 2020, https://www.gsma.com/mena/resources/middle-east-mobile-operators-will-5g-early-adopters-according-new-gsma-report.

322 "Freedom on the Net 2018 – Lebanon", *Freedom House*, November 1, 2018, https://freedomhouse.org/report/freedom-net/2018/lebanon.

323 "Huawei Brings state-of-the-art 5G to Lebanon", *Huawei,* November 6, 2018, https://www.huawei.com/en/press-events/news/2018/11/huawei-state-of-the-art-5g-lebanon.

324 Vinod Nair, "High speed internet: 5G network launched in Oman", *Oman Observer,* December 11, 2019, https://www.omanobserver.om/gear-up-for-high-speed-internet-with-5g-launch/.

(U5GIG) to "bridge the gap between telecom industry and academia in UAE".[325]

As mentioned previously, none of the Middle Eastern countries have come forth to ban Huawei or any other Chinese telecom companies from their 5G build-up. For instance, in a 2019 interview, Saudi technology minister Abdullah bin Amer Al-Sawaha said that Riyadh is open to anyone, including Chinese telecom giant Huawei, as long as regulatory and security requirements are complied with.[326] Head of Oman's Shura Council's Economy Committee, Sulayem Alhakmani, cleared Huawei to supply equipment in its market, and said that Oman is an "independent country" and does not see any "problem" with Chinese technology.[327] Further, Huawei's ongoing collaborations, research partnerships and technology initiatives represent a strong case for continuing the company's services (Table 23).

Table 23. Huawei and its collaboration with the Middle East

Country	Initiative
Saudi Arabia	The King Abdulaziz City for Science and Technology (KACST) a scientific government institution that works on scientific applied research, is creating a joint research centre with Huawei for future communications technologies.[328] 2016 Memorandum of Understanding between Huawei and the Royal Commission for Jubail and Yanbu (autonomous organisation under the Saudi Arabian government) on smart city technology development.
UAE	Huawei and Dubai municipality signed an MoU to establish a framework to collaborate on the Smart Dubai initiative. UAE's Telecom Regulatory Authority launched 5G and IoT Joint OpenLab at Dubai with Huawei to boost services, innovation and collaboration across markets and further ICT development in the country.
Kuwait	Joint Innovation Center with Zain (telecom operator in Kuwait), which will be a research hub to advance mobile broadband technologies and applications for Zain mobile customers locally and regionally.[329]
Qatar	Qatar's Ooredoo and China's Huawei partnered to set up an Innovations Lab in Qatar that will be a research hub for network technology, such as 5G, 4K video capabilities and the Internet of Things (IoT).
Middle East (general)	Announcement of 5G OpenLab at GITEX 2019, which will boost 5G services throughout the Middle East region, prompting innovation and collaboration across markets with the intention of creating an open ecosystem to further develop ICT across the region.[330]

In September 2019, the US FCC Chair Ajit Pai warned its Gulf allies—Saudi Arabia,

325 "The Huawei Wars and the 5G Revolution in the Gulf", *op. cit.*

326 "Saudi Arabia open to Huawei, says Communications Minister", *Al Arabiya,* February 28, 2019, http://english.alarabiya.net/en/business/technology/2019/02/28/Saudi-Arabia-open-to-Huawei-so-long-as-security-requirements-are-complied-with-.html.

327 James Barton, "Huawei gets the green light for 5G in Oman", *Developing Telecoms,* February 26, 2020, https://www.developingtelecoms.com/telecom-business/vendor-news/9249-huawei-gets-the-green-light-for-5g-in-oman.html.

328 "Creating a joint research center for future communications by KACST & Huawei, the leading global information and communications technology", King Abdulaziz City for Science and Technology (KACST), accessed March 26, 2020, https://www.kacst.edu.sa/eng/about/news/Pages/news755.aspx.

329 "Zain and Huawei Unveil First of Its Kind Joint Innovation Center in Middle East", *Zain,* June 9, 2018, https://www.zain.com/en/press/zain-and-huawei-unveil-first-of-its-kind-joint-inn/.

330 "Huawei Announces 5G OpenLab in the Middle East at GITEX 2019", *Huawei,* October 14, 2019, https://www.huawei.com/en/press-events/news/2019/10/huawei-announces-plan-5g-openlab-middleeast.

the United Arab Emirates, and Bahrain—regarding the security risks associated with Chinese equipment.[331] The US' concerns also come in the backdrop of Washington's strategic and military cooperation in the region. Washington's policy in the region initially focused on the containment of the Soviet Union and securing energy supplies, and then progressed to combating terrorism and isolating Iran. As a result, the Middle East has a large US military presence, with Table 24 below mapping American military bases and facilities in the region. Former US navy officials have indicated that China's foray in the region increases the likelihood of information and electronic surveillance, and may jeopardise US information and cybersecurity.[332]

Table 24. US bases in Middle East

Country	Name of U.S. bases and details of military agreements
Bahrain	United States Naval Forces Central Command and Headquarters of the US 5th Fleet. Shaikh Isa Air Base and Muharraq Air Base (Navy) *Bahrain also has a Defense Cooperation Agreement signed in 1991.*
Iraq	Al Asad Air Base
Israel	Dimona Radar Facility Mashabim Air Base / Bisl'a Aerial Defense School
Jordan	Muwaffaq Salti Air Base (Azraq)
Kuwait	Ali Al Salem Air Base Camp Arifjan: US HQ in Kuwait Camp Buehring Camp Patriot *Also has Defense Cooperation Agreement with Kuwait since 1991*
Oman	RAFO Masirah Muscat International Airport RAFO Thumrait Al-Musannah Air Base Port of Duqm Port of Salalah
Qatar	Al Udeid Air Base Camp As Sayliyah
Saudi Arabia	Eskan Village
Turkey	Incirlik Air Base Izmir Air Station NATO Member
United Arab Emirates	Al Dhafra Air Base Port of Jebel Ali: Busiest US Navy port of call Fujairah Naval Base

Source: U.S. Military Bases and Facilities in the Middle East, American Security Project, June 2018, https://www.americansecurityproject.org/wp-content/uploads/2018/06/Ref-0213-US-Military-Bases-and-Facilities-Middle-East.pdf.

331 Alexander Cornwell, "U.S. flags Huawei 5G network security concerns to Gulf allies", *Reuters,* September 12, 2019, https://www.reuters.com/article/us-huawei-security-usa-gulf/u-s-flags-huawei-5g-network-security-concerns-to-gulf-allies-idUSKCN1VX241.

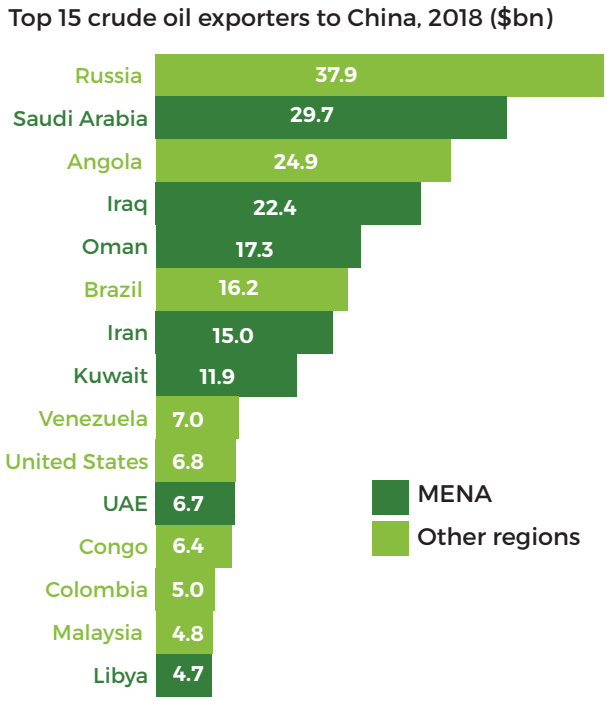
332 David Brennan, "Chinese Deal To Take Over Key Israeli Port May Threaten U.S. Naval Operations, Critics Say", *Newsweek,* September 14, 2019, https://www.newsweek.com/chinese-deal-take-over-key-israeli-port-may-threaten-us-naval-operations-1121780

The Trump administration, however called for US retrenchment from the region, given its aim to re-orient priorities from regional contingencies to great power competition vis-à-vis China.[333] Nonetheless, US military footprint in the Middle East continues to be fairly consistent.[334] In this regard, Huawei and ZTE's equipment in 5G networks–with their possibility to be used for espionage and cyberattacks–would be a major concern for the Washington.

Beijing's presence in the region has also increased—it has become the biggest trade partner and external investor in the region. This has been supported by China's 2016 Arab Policy Paper,[335] which aims to anchor future China-Arab diplomatic ties by establishing a "1+2+3" cooperation pattern, with energy cooperation at the core, and infrastructure construction and trade and investment facilitation as the two wings. Analysts also argue that China's authoritarian capitalism is more attractive to Middle Eastern regimes, who view it as a better alternative to US' development aid and investment, which are often tied up with pressure to pursue governance reforms and human rights accountability.[336]

In 2015, Beijing also became the largest global importer of crude oil, with almost half its supply coming from the Middle East (Fig. 7). Further, Middle East is also important

Fig 7. China's crude oil exports from the MENA (Middle East and North Africa) region 2018



Crude oil imports: "China's great game in the Middle East", European Council on Foreign Relations, October 21, 2019, https://www.ecfr.eu/publications/summary/china_great_game_middle_east.

333 "Summary of the 2018 National Defense Strategy of United States of America", *U.S. Department of Defense*, 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

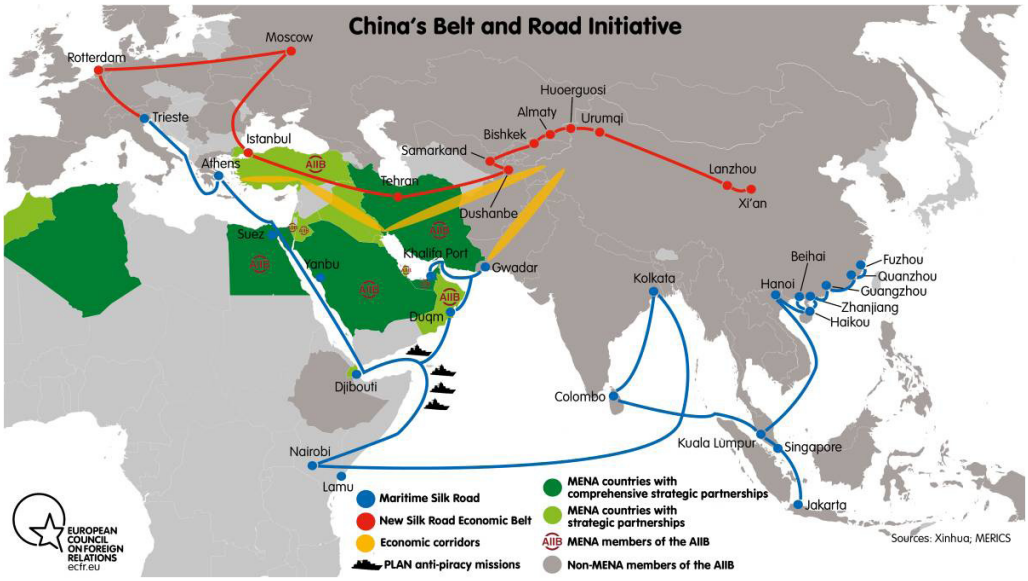
334 Daniel Benaim and Michael Wahid Hanna, "The Enduring American Presence in the Middle East", *Foreign Affairs,* August 7, 2019, https://www.foreignaffairs.com/articles/middle-east/2019-08-07/enduring-american-presence-middle-east.

335 "China's Arab Policy Paper", The State Council, People's Republic of China, January 2016 http://english.www.gov.cn/archive/publications/2016/01/13/content_281475271412746.htm.

336 Camille Lons, "China's Evolving Role In The Middle East" in *China's great game in the Middle East*, European Council on Foreign Relations, Policy Brief, October 2019, https://www.ecfr.eu/publications/summary/china_great_game_middle_east.

to China's 2013 Belt and Road Initiative, since sea routes and trade routes such as Bab el-Mandeb, Strait of Hormuz and Suez Canal constitute important sea-lanes of communication for China (Fig. 8).

Fig. 8. China's Belt and Road Initiative (BRI) in the Middle East



Source: "China's great game in the Middle East", European Council on Foreign Relations, October 21, 2019, https://www.ecfr.eu/publications/summary/china_great_game_middle_east.

Israel, on the other hand, presents an interesting case study. Washington is an important strategic ally for Israel, while Israel is US' most reliable partner in the Middle East.[337] Receiving over $3 billion in US Foreign Military financing annually, the two nations enjoy a robust strategic partnership involving joint military exercises, military research, and weapons development. Politically, Washington's support to Israel is crucial for the Palestine issue, where US policies such as recognising Jerusalem as its capital in 2017, and its 2020 West Asia peace plan to recognise the illegal West Bank settlements have been supported by Prime Minister Benjamin Netanyahu.

However, there has been a growing divergence between the two countries over Israel's expanding relations with China, which is currently Israel's third largest trading partner. There has been an increase in China's investments in Israel's advanced technologies and critical infrastructure, a development that complements Israel's interests in expanding diplomatic ties with the world's fastest growing economy.[338] This may put a strain in US-Israel relations, given Washington's concerns with Beijing's increasing economic and political presence in the region.

337 "U.S. Relations With Israel", U.S. Department of State, May 14, 2018, https://www.state.gov/u-s-relations-with-israel/.

338 Shira Efron, Howard J. Shatz, et. al., *The Evolving Israel-China relationship*, (California: RAND Corporation, 2019), 86-99, https://www.rand.org/pubs/research_reports/RR2641.html.

All levels of American leadership—from Trump to Pompeo—have raised concerns about Israel's partnership with China, including participation of Chinese tech companies in 5G bidding.[339] Here too, the US has threatened to reduce US–Israel intelligence-sharing should Israel's engagement with Beijing continue.[340]

While Israel published a tender for 5G networks in July 2019,[341] its Communication Ministry has not issued any official comment on the participation of Chinese tech companies. Israeli intelligence officials, such as Nadav Argaman, head of Shin Bet, Israel's internal security service, and former head of Mossad, Efraim Halevy, have voiced concerns regarding Chinese infiltration in telecom infrastructure. On the other hand, some fear that by ousting Huawei, China may retaliate by potentially increasing military and intelligence assistance to Iran.[342]

The Huawei conundrum will require Israel to perform a fine balancing act, given its close ties with the US and need to ensure Washington's continued cooperation on political, military and strategic areas. On the other hand, for the remaining countries in the Gulf region, the answer to the Huawei dilemma has been fairly clear. For this region, the benefits of a fast and early deployment of 5G outweigh the purported security risks, because of which it has decided against banning Chinese telecom companies from building their 5G infrastructure.

B. Latin America

In Latin America, majority of the countries have been absent from the discourse on Huawei and the 5G dilemma, save for Brazil. Constraints such as the present status of telecommunications networks, poor infrastructure and high economic volatility mean that 5G is still a distant reality for the region, thereby marking a lack of debate on Huawei and 5G. However, for these very reasons, China's investments, trade and markets, and above all Huawei's capacity to provide affordable equipment, indicate that Latin American countries have little to gain from banning Chinese suppliers.

According to GSMA's 2019 report on Latin America, the region will be in the bottom three for regional 5G adoption rates (Fig 9). It is expected that Latin American countries will focus on 4G adoption–estimated to reach 67 percent by 2025–while 5G adoption will only reach seven percent by 2025. Here, mobile operators, will build or invest in 4G networks, before investing in emerging technologies like 5G. Nonetheless, as of today, 18 5G trials[343] have been ongoing in this region, with Uruguay's Antel and Peurto Rico's T-Mobile having launched commercial 5G services with Nokia.[344]

However, major countries such as Brazil and Argentina–where some conversations on Huawei and 5G have taken place–have been resistant to US pressure to ban the Chinese company. A primary reason is that since economic growth is faltering in the

339 Omri Nahmias, "Trump aims to prevent Chinese companies from building 5G network in U.S.", *The Jerusalem Post,* May 18, 2019, https://www.jpost.com/American-Politics/Trump-aims-to-prevent-Chinese-companies-from-building-5G-network-in-US-589930.

340 Dan Arbell and David Gordon, "What do Israel's China ties mean for its relationship with the US?", *International Institute for Strategic Studies*, May 8, 2019, https://www.iiss.org/blogs/analysis/2019/05/israel-china.

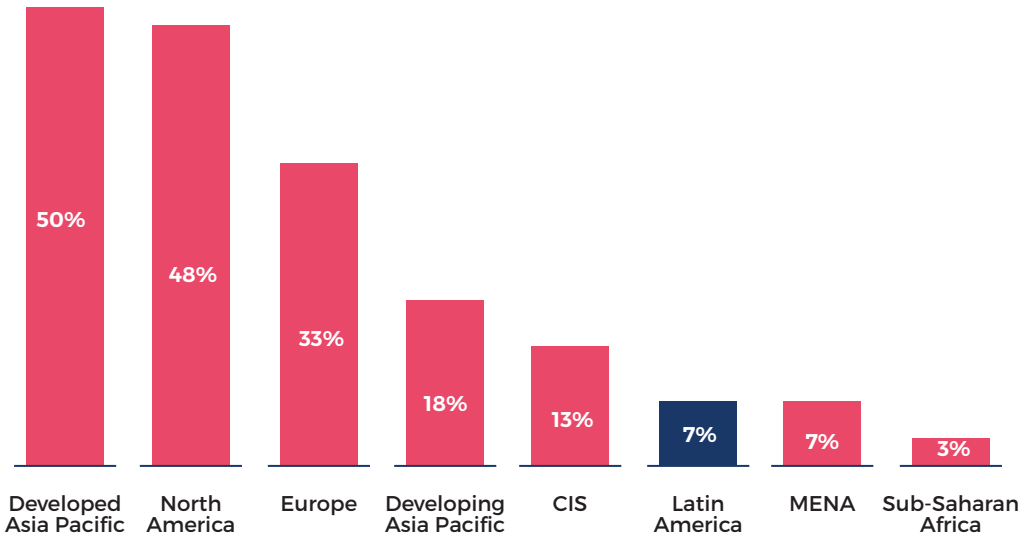
341 Shoshanna Solomon, "Tender launched for 5G next-gen mobile networks, to provide higher speeds", *The Times of Israel,* July 14, 2019, https://www.timesofisrael.com/tender-launched-for-5g-next-gen-mobile-networks-to-provide-higher-speeds/.

342 "What do Israel's China ties mean for its relationship with the US?", *op. cit.*

343 GSMA Intelligence, "Intelligence Brief: What will make 5G take off in LatAm?", *Mobile World Live,* August 28, 2019, https://www.mobileworldlive.com/blog/intelligence-brief-what-will-make-5g-take-off-in-latin-america/.

344 "Uruguay: ANTEL, Nokia Complete First 5G Commercial Network in Latin America", *Merco Press,* April 11, 2019, https://en.mercopress.com/2019/04/11/uruguay-antel-nokia-complete-first-5g-commercial-network-in-latin-america; "One Step Closer to Nationwide 5G: T-Mobile Marks a World's First on the Road to 5G", *T-Mobile,* November 20, 2018, https://www.t-mobile.com/news/first-600mhz-5g-test.

Fig 9. Latin America is in the bottom three for regional 5G adoption rates



Source: The Mobile Economy: Latin America, GSMA intelligence, 2019, 27, https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_LATAM_Eng.pdf.

region, there is a strong imperative to attract Chinese investment. Brazil is facing a strong recession and registered an annual GDP growth rate of 1.1 percent in 2018[345]; Argentina's inflation rate hit 53.9 percent in 2019[346]; while in Venezuela hyperinflation is at 10 million percent[347].

For Brazil, which currently features one of the lowest levels of infrastructure investment (2.1 percent of GDP), 5G infrastructure investments, such as fibre backhaul has suffered. Things are much worse in Venezuela, where the nation's economic crisis marked by five years of recession and two years of hyperinflation, has hindered the country's telecommunications infrastructure and the quality of internet access. This has affected investments, replacement and repair of existing infrastructure, and the citizen's purchasing power and appetite for costlier services such as 5G stands affected.[348] Because of this, it will not only be premature, but even difficult to ban Huawei from the region.

The debate on 5G, Huawei and China, has been particularly robust in Brazil, where there is a strong inclination to attract Chinese investments and financing. Taking Beijing's side is an unexpected choice for current President Jair Bolsonaro, given his political and ideological congruence with Trump. For instance, during his campaign Bolsonaro sharply criticised communist regimes and warned that China was "rapacious predator" out to exploit Brazil.[349] During Bolsonaro's March 2019 visit the White House, Trump

345 GDP growth (annual %) - Brazil, *The World Bank,* accessed March 26, 2020, https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?locations=BR.

346 Benedict Mander, "Argentina's inflation nears highest level in three decades", *Financial Times,* January 16, 2020, https://www.ft.com/content/e6f5c436-37d2-11ea-a6d3-9a26f8c3cba4.

347 Valentina Sanchez, "Venezuela hyperinflation hits 10 million percent. 'Shock therapy' may be only chance to undo the economic damage", *CNBC,* August 3, 2019, https://www.cnbc.com/2019/08/02/venezuela-inflation-at-10-million-percent-its-time-for-shock-therapy.html.

348 "Freedom On The Net 2019: Venezuela", *Freedom House,* accessed March 26, 2020, https://www.freedomonthenet.org/country/venezuela/freedom-on-the-net/2019.

349 Paulo Trevisani, "Brazil Deepens China Ties in About-Face", *The Wall Street Journal,* November 15, 2019, https://www.wsj.com/articles/brazil-deepens-china-ties-in-about-face-11573772734.

emphasised that Brazil must curb the spread of Huawei technology in the region, and will need to become a trusted ally to limit Chinese influence in Latin America.[350]

However, Brazil's poor economic growth means that China's partnership is important to it because of Beijing's appetite to consume Brasilia's commodities, in addition to the scope for increasing bilateral trade and investment ties. China is Brazil's largest trade partner and export market, and according to China's Ministry of Commerce, bilateral trade increased to $110 billion in 2018.[351] Further, Brazil is a focal point for Huawei's deployment of 4G networks[352], thereby strengthening the cause for continuing old partnerships in 5G networks. Another possible reason for not obliging Washington's demands could be the 2013 revelation that the US National Security Agency monitored former president Dilma Rousseff's phone calls and spied on Brazil's state oil corporation, thus limiting the credibility of Washington's warnings.[353]

With these factors, it seems unlikely that Brazil will ban Huawei; however, the matter is yet to be decided. Members of the government and other stakeholders have diverging views on the Huawei question, as demonstrated by statements in Table 25. Presently, Brazil's auction of 5G spectrum–initially scheduled for March 2019–has been delayed to late 2020-early 2021. This provides Brasilia with more time to evaluate the costs and benefits of permitting Huawei to build its 5G networks, and also gives the US the opportunity to find and promote an attractive alternative to Huawei.[354] However, there are concerns that the delay will hurt Brazil's economic competitiveness, with an Ericsson study estimating a cost of about R$25bn ($6bn) in lost tax revenues[355].

350 Oliver Stuenkel, "Huawei Heads South", *Foreign Affairs,* May 10, 2019, https://www.foreignaffairs.com/articles/brazil/2019-05-10/huawei-heads-south.

351 May Zhou and Kong Wenzheng, "China's relations with Brazil have grown for 45 years", *China Daily,* November 13, 2019, https://www.chinadaily.com.cn/a/201911/13/WS5dcaebfca310cf3e35576eaf.html.

352 R. Evan Ellis, "China on the Ground in Latin America: Challenges for the Chinese and Impacts on the Region", (New York: Palgrave Macmillan, 2014), 106.

353 Margaret Myers, "Latin America and 5G: Five Things to Know", *The Dialogue,* December 14, 2019, https://www.thedialogue.org/analysis/latin-america-and-5g-five-things-to-know/.

354 Oliver Stuenkel, "Brazilian 5G: The Next Battleground in the U.S.-China Standoff", *Americas Quarterly,* January 16, 2020, https://www.americasquarterly.org/content/brazils-5g-next-battleground-us-china-stand.

355 Bryan Harris and Andres Schipani, "Brazil 5G auction delay dents country's tech ambitions", *Financial Times,* January 13, 2020, https://www.ft.com/content/b54a11aa-2001-11ea-b8a1-584213ee7b2b.

Table 25. Overview of statements made by stakeholders in Brazil on Huawei and 5G

Date	Name	Designation	Statement
January 2020	Marcos Pontes	Minister for science, technology, innovation and communications	Brazil will not accept any pressure from the US over whether to allow the Chinese company Huawei to bid for its 5G network
July 2019	Hamilton Mourão	Vice President	Brazil's ties with its biggest trade partner cannot be disregarded and there is no veto against Huawei in Brazil.[356]
February 2020	Eduardo Bolsonaro	Brazilian president's son, lawmaker	Huawei's involvement in building the 5G network could affect military cooperation between Brazil and the United States.[357]
February 2020	Anatal	Brazil's telecom regulator	Any decisions on security risks of using Chinese technology will be taken by the national security chief.[358]

Source: News reports.

What further weighs in favour of Huawei and ZTE is their large footprint in the region due to their contribution to building existing telecommunications infrastructure and investing in partnerships and research collaborations (Table 26).[359] In 2014, Huawei had a corporate presence in 14 countries in Latin America, with a total of 4,500 employees in 19 regional offices, software research and development centres, and training centres.[360] With specific reference to 5G, Huawei has reportedly signed contracts with seven telecom operators in Latin America, while its smartphone sales grew by 50 percent in the region.[361] There have also been 5G trials with Huawei's equipment in Brazil, Colombia, Peru, Chile, Ecuador and Argentina. Since taking on the Chinese company will be expensive, endanger jobs and jeopardise trade ties, these factors make Huawei an attractive regional partner.[362]

356 "Brazil's vice-president Hamilton Mourao says no restrictions on Huawei", *The Straits Times,* July 16, 2019, https://www.straitstimes.com/world/brazils-vice-president-says-no-restrictions-on-huawei.

357 Anthony Boadle, "Huawei role in Brazil 5G up to national security chief: regulator", *Reuters,* February 18, 2020, https://www.reuters.com/article/us-brazil-telecoms/huawei-role-in-brazil-5g-up-to-national-security-chief-regulator-idUSKBN20C1U1.

358 *Ibid.*

359 Miguel Pérez Ludeña, "Chinese Investments in Latin America: Opportunities for growth and diversification", United Nations Economic Commission for Latin America and the Caribbean (ECLAC) - Production Development Series No. 208, April 2017, 16, https://repositorio.cepal.org/bitstream/handle/11362/41134/S1700083_en.pdf?sequence=1&isAllowed=y.

360 "China on the Ground in Latin America: Challenges for the Chinese and Impacts on the Region", *op. cit.,*104.

361 Rodolfo Espinal, "Tecnología 5G para América Latina y mayor protección a ciberseguridad", *El Peruano,* December 17, 2019, https://elperuano.pe/noticia-tecnologia-5g-para-america-latina-y-mayor-proteccion-a-ciberseguridad-87668.aspx.

362 "Huawei heads South", *op. cit.*

Table 26. Huawei's investments and technology proposals in Latin America

Country	Initiative
Brazil	In 2017, Huawei in partnership with Brazil's National Institute of Communications opened the Centre for Competence and Innovation Development (CIDC), to jointly develop network and technology solutions for operators in Brazil. Plans to invest up to $800 million over the next three years to expand its presence in Brazil via a new manufacturing facility in São Paulo.
Chile	Opening of Huawei Cloud in 2019, to provide a full-stack cloud platform and a wide range of Artificial Intelligence (AI) services for Latin America.
Uruguay	Memorandum of understanding signed with Uruguay's government in August 2019 to deepen cooperation on 5G, industrial digitisation and training people in information and communication technology.[363]
Bolivia	September 2019 announcement by Oscar Coca, Bolivia's Minister for Public Works, that ENTEL, Bolivia's state-run telecom operator will partner with Huawei for 5G networks, and the project will involve an investment of $70 million dollars.[364]
Ecuador	Huawei and Beijing's state-controlled China National Electronics Import & Export Corporation (CEIEC) have helped build "ECU-911"—a national emergency response and video surveillance system.[365]
Peru	In 2017, Telefónica Peru chose Huawei to help transform its existing central office to build a cloud data centre.[366] Huawei has also contributed to Nextel's CDMA network and modernised Telefónica's fixed telephone system.[367]
Seeds of the future programme	In September 2019, 30 university students from Mexico, the Dominican Republic and Jamaica were in China to participate in this programme aimed at spreading knowledge, increasing awareness of and interest in information and communication technology, and encouraging broad participation in digital communities.[368]
Proposals	Huawei is considering building the first subsea cable to connect South and Central America and China.[369] Investment of $50 million to support local app development in Latin America.[370]

Source: News reports.

363 Li Xia, "China's Huawei to deepen cooperation with Uruguay on 5G technology", *Xinhua News,* August 27, 2019, http://www.xinhuanet.com/english/2019-08/27/c_138342414.htm.

364 "Huawei to help bring 5G to Bolivia", *Telesur TV,* September 26, 2019, https://www.telesurenglish.net/news/Huawei-To-Help-Bring-5G-To-Bolivia--20190926-0003.html.

365 Charles Rollet, "Ecuador's All-Seeing Eye Is Made in China", *Foreign Policy,* August 9, 2018, https://foreignpolicy.com/2018/08/09/ecuadors-all-seeing-eye-is-made-in-china/; Paul Mozur, Jonah M. Kessel and Melissa Chan, "Made in China, Exported to the World: The Surveillance State", *The New York Times,* April 24, 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

366 Linda Hardesty, "Telefónica Peru Transforms Central Office to Cloud Data Center", *SDX Central,* June 26, 2017, https://www.sdxcentral.com/articles/news/telefonica-peru-transforms-central-office-cloud-data-center/2017/06/.

367 "China on the Ground in Latin America: Challenges for the Chinese and Impacts on the Region", *op. cit.,* 110.

368 "Huawei program helps train Latin American students", *Xinhua News,* September 16, 2019, http://www.xinhua-net.com/english/2019-09/16/c_138396185.htm.

369 Chris Kelly, "Huawei considers world's first subsea link between China and Latin America", *Total Telecom,* August 30, 2019, https://www.totaltele.com/503707/Huawei-considers-worlds-first-subsea-link-between-China-and-Latin-America.

370 Jacob Atkins, "Huawei announces US$50 million for Latin American developers, plans to install lab in Mexico", *Contxto,* November 7, 2019, https://www.contxto.com/en/mexico/huawei-announces-us50-million-for-latin-american-developers-plans-to-install-lab-in-mexico/.

At present, save for the largest Latin American countries–such as Brazil–the region is expected to see a delayed rollout of 5G networks. It is also possible that governments will have an interest in focusing on getting faster speeds, instead of scrutinising the possibility of surveillance and other security risks from China.[371] Further, the importance of China's economic ties and Huawei's pre-existing partnership presents a strong case for keeping Chinese telecom companies in 5G networks. On Washington's obsession with Beijing, Latin America has expressed both indifference and bewilderment.[372] Moreover, Latin America's deep-seated concerns regarding excessive US influence–a remnant of the erstwhile Monroe doctrine–make them wary of paving the way for further US intervention in the region. As the Huawei debate unfolds, Latin American countries will focus on national priorities to develop a 5G network that is affordable and develops upon pre-existing partnerships.

C. Russia and Central Asia

With Russia, the answer to the 5G dilemma is clear-cut; the country has welcomed Huawei to build its 5G networks. Before Jinping's three-day visit to Russia in June 2019, Huawei and MTS–one of Russia's largest telecom operators–signed a deal to develop 5G technology in Russia.[373] Moscow's other major mobile operators, such as Beeline, MTS, VimpelCom and MegaFone have also carried out trials with Huawei, along with other vendors such as Ericsson, Nokia, Qualcomm and Samsung.[374]

Since the 2014 Ukraine sanctions against Russia, its access to Western technology has been limited. Similarly, China is also at the centre of the ongoing economic, geopolitical and technological rivalry with the US. With these shared concerns, similar governance systems, and a strong imperative to remain technologically advanced, there has been greater bonhomie and cooperation on technological initiatives between the two countries.

Kremlin declared 2020-21 as the Year of Russian-Chinese Scientific, Technical and Innovation Cooperation[375] and is planning to organise 800 events within the year, including the promotion of Russian and Chinese languages in both states. Such collaborations will help bridge the technological gap between Russia and other western nations, and support initiatives such as Moscow's Digital Economy Program,[376] which approves the use of US$1.8 billion by 2025 to address current weaknesses in its digital economy.[377]

In December 2019, at least eight top Russian universities and research institutes had announced new or expanded partnerships with Huawei, entailing plans for research collaborations in wireless communications, neural networks, machine learning, and data storage and processing.[378] Russian President Vladimir Putin even spoke up for the

---

371 "Latin America and 5G: Five Things to Know", *op. cit.*

372 "Huawei heads South", *op. cit.*

373 Andrew E. Kramer, "Huawei, Shunned by U.S. Government, Is Welcomed in Russia", *The New York Times,* June 6, 2019, https://www.nytimes.com/2019/06/06/business/huawei-russia-5g.html.

374 "Major European 5G Trials And Pilots", European 5G Observatory, accessed March 26, 2020, https://5gobservatory.eu/5g-trial/major-european-5g-trials-and-pilots/.

375 "Russia, China discussing key projects for year of scientific cooperation", *TASS Russian News Agency,* December 25, 2019, https://tass.com/science/1103515.

376 "Digital Economy of the Russian Federation", Government of the Russian Federation, No. 1632, July 2017, http://government.ru/docs/28653/.

377 "Competing in the Digital Age: Policy Implications for the Russian Federation", Russian Digital Economy Report, *World Bank Group*, September 2018, 2, http://documents.worldbank.org/curated/en/860291539115402187/pdf/Competing-in-the-Digital-Age-Policy-Implications-for-the-Russian-Federation-Russia-Digital-Economy-Report.pdf.

378 Simone McCarthy, "Shunned in the US, Huawei looks to Russia to invent an AI future", *South China Morning Post,* December 3, 2019, https://www.scmp.com/news/china/diplomacy/article/3040264/shunned-us-huawei-looks-russia-invent-ai-future.

company, saying the US was trying to "brazenly force it out of the global market" by blacklisting it, as quoted by the government-funded RT news network.[379] Nevertheless, it remains to be seen if intellectual property theft could still be a concern between Beijing and Moscow, given how Russia's state defence conglomerate Rostec accused China of copying technology from Sukhoi fighter jets to missile systems.[380]

Huawei and China have also scaled up their technology cooperation with Central Asian countries like Uzbekistan, Kazakhstan, and Tajikistan. Chinese investments and initiatives like the Digital Silk Road have been welcomed by Central Asian countries, since they are an important means to build and operate new age digital infrastructure and connectivity in the impoverished region. This position is supported by a CSIS study, which found that 42 percent of Huawei's agreements are in lower-middle-income countries, suggesting the tech is popular due to both competitive pricing and its potential to generate steady income streams for cash-strapped governments.[381] On the other hand, analysts note that such initiatives have not only ramped up debt for Central Asian countries to unsustainable levels, but is also a method to introduce authoritarian uses of technologies, such as surveillance and facial recognition–minus the protection of privacy and data protection rights.[382]

A brief overview of both Huawei and China's technology investments are provided in Table 27 below.

379 Dimitri Simes, "Huawei plays star role in new China-Russia AI partnership", *Nikkei Asian Review,* February 4, 2020, https://asia.nikkei.com/Spotlight/Asia-Insight/Huawei-plays-star-role-in-new-China-Russia-AI-partnership.

380 *Ibid.*

381 Jonathan E. Hillman & Maesea McCalpin, "Watching Huawei's 'Safe Cities'", Policy Briefs, Center for Strategic and International Studies, November 2019, https://www.csis.org/analysis/watching-huaweis-safe-cities.

382 Bradley Jardine, "China's Surveillance State Has Eyes on Central Asia", *Foreign Policy,* November 15, 2019, https://foreignpolicy.com/2019/11/15/huawei-xinjiang-kazakhstan-uzbekistan-china-surveillance-state-eyes-central-asia/.

Table 27. Illustrations of Huawei's partnerships and collaborations in Central Asia

Country	Developments
Uzbekistan	Uzbek President Shavkat Mirziyoyev visited Huawei's Innovation Center while in China for the Belt and Road Forum in April 2019.[383] In August 2019, Prime Minister of Uzbekistan, Abdulla Aripov, visited Huawei's headquarters and signed two Agreements of Cooperation to implement a "safe city" project and application of modern technologies to emergency medical services.[384] Huawei closed a $1 billion deal with Uzbekistan to build a traffic monitoring system involving 883 cameras[385]. State-backed mobile operator Ucell and Uzmobile conducted 5G trials with Huawei in September 2019.[386]
Kazakhstan	Four students from the Al-Farabi Kazakh National University to participate in the Seeds of the Future program.[387] In May 2017, Huawei opened the Huawei Authorised Information and Network Academy (HAINA) in Almaty, to train specialists in information and communication technologies (ICT) and telecommunications spheres.[388]
Tajikistan	90 percent of the country's telecommunications equipment is supplied by Huawei. The Tajik government spent $22 million to implement Huawei's "safe cities" system in Dushanbe in 2013. China owns TK mobile, one of the five telecommunication providers in Tajikistan.
Turkmenistan	In 2017, Huawei upgraded the railway communications network and provided an end-to-end Global System for Mobile Communications-Railway (GSM-R) solution to improve operational efficiency of main lines.[389]

With specific reference to 5G, analysts note that since the region shares a strong connection with Huawei, the company is unlikely to be banned.[390] Further, 5G commercial launches for Central Asian countries are estimated to take place in 2021-2024, which means it may be too early for them to decide whether to ban Huawei or not. (Fig. 10)

383 The Official Website of the President of the Republic of Uzbekistan, April 25, 2019, https://president.uz/ru/2524.

384 "Prime Minister of the Republic of Uzbekistan has visited Huawei R&D center in Shenzhen", *Huawei,* August 29, 2019, https://www.huawei.com/en/press-events/news/2019/8/uzbekistan-prime-minister-visit-huawei.

385 "China's Surveillance State Has Eyes on Central Asia", *op. cit.*

386 "Ucell, Uzmobile testing 5G in Uzbekistan", *Comms Update,* September 18, 2019, https://www.commsupdate.com/articles/2019/09/18/ucell-uzmobile-testing-5g-in-uzbekistan/.

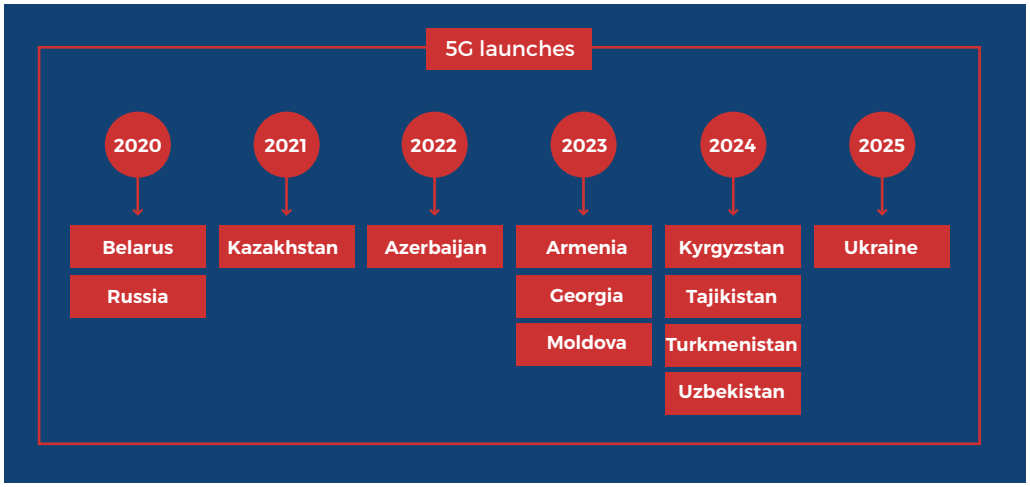
387 Aidana Yergaliyeva, "Huawei to prepare KazNU ICT professionals", *The Astana Times,* April 11, 2019, https://astanatimes.com/2019/04/huawei-to-prepare-kaznu-ict-professionals/.

388 Dana Omirgazy, "Huawei Academy opens in Almaty to support local ICT education", *The Astana Times,* May 3, 2017, https://astanatimes.com/2017/05/huawei-academy-opens-in-almaty-to-support-local-ict-education/.

389 "Huawei Helps Turkmenistan to Build Steel 'Silk Road'", *Huawei,* April 22, 2017, https://e.huawei.com/in/case-studies/global/2017/201704221441.

390 Umida Hashimova, "Before and Beyond 5G: Central Asia's Huawei Connections", February 19, 2019, *The Diplomat,* https://thediplomat.com/2020/02/before-and-beyond-5g-central-asias-huawei-connections/.

Fig 10. Estimated 5G commercial launches in Central Asian countries



Source: "The Mobile Economy: Russia & CIS 2019", GSMA Intelligence, 2019, 12, https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_RussiaCIS_Eng.pdf.

Consequently, the region also finds itself in the middle of the technological cold war between US and China. In his February 2020 visit to Kazakhstan and Uzbekistan, US Secretary of State Mike Pompeo, discussed the Chinese Communist Party's repression of Uighur Muslims, Kazakhs, and members of other minority groups in Xinjiang[391], and added that though Washington supports the region's freedom to choose to do business with whatever country, he is "confident" that they will get the "best outcome" when they partner with American companies.[392] China's embassy in Uzbekistan condemned Pompeo's statements and termed it as "malicious incitement and slander", which attempt to "sow discord" between Beijing and Central Asian countries.[393]

Central Asia is also an important component of China's Belt and Road Initiative. By 2017, China is estimated to have invested in $304.9 billion worth of contracts with its partners in the region in sectors including transport, communication, energy infrastructure, financial linkages, technology transfer and trade facilitation.[394] On the other hand, Washington's direct assistance to support peace and security, democratic reform, economic growth, and humanitarian needs amounts to $9 billion. Additionally, US led-financial institutions like the World Bank and International Monetary Fund have extended over $50 billion, and the private sector over $31 billion in commercial ventures in the region.[395] These numbers will be difficult to compete with China's large investments in the region.

The US Strategy for Central Asia 2019-2025 aims to build their resilience to short and long-term threats to their stability; strengthen their independence from malign actors; and develop political, economic, and security partnerships with the United States.[396]

---

391 "Uzbekistan resists as U.S. seeks to rally Central Asians against China", *Reuters,* February 3, 2020, https://www.reuters.com/article/us-uzbekistan-usa-china-rights/uzbekistan-resists-as-u-s-seeks-to-rally-central-asians-against-china-idUSKBN1ZX1HQ.

392 Mark Armstrong, "Mike Pompeo tours Kazakhstan with warning over Chinese investment", *Euro News,* February 2, 2020, https://www.euronews.com/2020/02/02/mike-pompeo-tours-kazakhstan-with-warning-over-chinese-investment.

393 http://uz.china-embassy.org/rus/sgxx/sgsd/t1739690.htm

394 Adil Miankhel, "Why Central Asia chooses Chinese investment", *East Asia Forum,* June 29, 2019, https://www.eastasiaforum.org/2019/06/29/why-central-asia-chooses-chinese-investment/.

395 *Ibid.*

396 "United States Strategy for Central Asia 2019-2025: Advancing Sovereignty and Economic Prosperity", Bureau Of South And Central Asian Affairs, U.S. Department of State, February 5, 2020, https://www.state.gov/united-states-strategy-for-central-asia-2019-2025-advancing-sovereignty-and-economic-prosperity/.

However, Washington has limited resources and bandwidth that it is willing to commit in the region.[397] Since Huawei is also an integral part of existing telecommunications networks, and China–with Huawei–has launched various digital infrastructure initiatives, the region is unlikely to place any ban on the company, and has not had any conversation in this regard.

D. Africa

In Africa, commercial deployment of 5G will lag behind those of other regions. North Africa has a higher subscriber penetration rate–68 percent–and is estimated to see a 5G adoption rate of six percent by 2025.[398] Sub-Saharan Africa, on the other hand, lags behind other regions in terms of 4G adoption (seven percent connections as compared to the global average of 44 percent), but studies suggest that by 2019, 3G would have replaced 2G connections.[399] Further, internet adoption rate in Africa currently stands at 28.2 percent,[400] well below the world average of 53.6 percent.

As a result, 5G networks are not imminent in most markets in the region as existing technologies are capable of supporting current demands for mobile internet connectivity.[401] Analysts also note that 5G is not yet relevant to Africa, and most mobile operators in Africa will focus on deploying 4G networks particularly with Huawei. Gaining access to the internet, and the need to build digital infrastructure and connectivity will overshadow Chinese surveillance concerns–as in the case of Latin America.

Nonetheless, some advanced countries in Africa have made efforts towards 5G deployment. In September 2019, South Africa's network operator *rain* and Huawei jointly launched Africa's first commercial 5G network.[402] ZTE has conducted 5G trials with MTN Uganda,[403] while in West Africa, Nigeria's mobile operator conducted its first 5G trials with Huawei, ZTE and Ericsson.[404] Huawei also showcased 5G technology at the 2019 Cup of African Nations with Telecom Egypt.[405] In May 2019, Huawei announced a three-year memorandum of understanding with the African Union to improve the technical expertise of the region and to cooperate on key issues related to information and communication technologies.[406]

---

397 Peter Leonard, "Perspectives | US strategy for Central Asia: An old recipe for a new situation", *Eurasian Net,* February 6, 2020, https://eurasianet.org/perspectives-us-strategy-for-central-asia-an-old-recipe-for-a-new-situation.

398 "The Mobile Economy Middle East & North Africa 2019", *GSMA Intelligence*, 2019, 6, https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_MENA_Eng.pdf.

399 "5G In Sub-Saharan Africa: Laying the Foundations", *GSMA Intelligence,* 2019, https://www.gsma.com/subsaharanafrica/resources/5g-in-sub-saharan-africa-laying-the-foundations.

400 "Measuring digital development: Facts and figures 2019", *International Telecommunications Union*, 2019, 2, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf.

401 "5G In Sub-Saharan Africa: Laying the Foundations", *op. cit.,* 5.

402 "rain and Huawei Jointly Announce the 5G Provisioning to Selected Users in South Africa", *Huawei,* September 18, 2019, https://www.huawei.com/en/press-events/news/2019/9/rain-Huawei-Provisioning-Selected-Users-South-Africa.

403 Liao Shumin, "ZTE, Uganda's MTN Team Up to Trial 5G", *Yicai Global,* January 20, 2020, https://yicaiglobal.com/news/zte-uganda-mtn-team-up-to-trial-5g.

404 Yinka Awosanya, "4 things we learnt from MTN Nigeria's 5G trial", *Techpoint Africa,* November 25, 2019, https://techpoint.africa/2019/11/25/mtn-nigeria-5g-trial-abuja/.

405 "Huawei executives met with Egyptian prime minister to promote digital ecosystem development in Egypt", *Huawei,* April 22, 2019, https://www.huawei.com/en/press-events/news/2019/4/huawei-egyptian-prime-minister-digital-ecosystem-egypt.

406 "Huawei and the African Union sign a MoU to strengthen their technical partnership on ICT", *Huawei,* May 31, 2019, https://www.huawei.com/za/press-events/news/za/2019/huawei-the-african-union-sign-a-mou.

Both Huawei and ZTE have a strong presence in the African region, having contributed to building its telecommunications infrastructure. Huawei has established itself across Africa since launching in Kenya in 1998, and now operates in 40 countries.[407] Huawei has already built 70 percent of the continent's 4G networks, and such construction is often supported by loans from Chinese state banks–which are faster, and bundled with fewer conditions.[408] ZTE, on the other hand, not only provides telecom equipment to the region, but has also attempted to expand its investments to renewable energy and palm oil through its companies ZTE Agribusiness and Zonergy.[409]

A 2017 article by Tokunbo Ojo, examined the growing internationalisation of Huawei, its business strategies and engagement with the Nigerian telecom sector. He observes that Sino-Nigerian relations exhibit a "triangular diplomacy", a term which means that bilateral negotiations are no longer limited to traditional government-to-government negotiations, but involves corporate executives and other tiers of government.[410] This means international business and international relations are intertwined 'as politicians need to boost economies through supporting entrepreneurship' while 'international entrepreneurs need politicians and government representatives to get access to foreign markets to deal with legal issues across borders'[411]. In Nigeria, as is the case with other African countries, Huawei's corporate social responsibility (CSR) activities focus on IT skill training, education and donations, which help improve the company's public opinion and enhances China's soft power and geopolitical influence in the continent.

Table 28 looks at Huawei's soft power strategies in the African continent.

407 Agence France-Presse,"Huawei strengthens foothold in Africa to offset US ban", *South China Morning Post,* June 9, 2019, https://www.scmp.com/news/world/africa/article/3013717/huawei-strengthens-foothold-africa-amid-us-ban.

408 Amy Mackinnon, "For Africa, Chinese-Built Internet Is Better Than No Internet at All", *Foreign Policy,* March 19, 2019, https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-is-better-than-no-internet-at-all/.

409 Deborah Brautigam, *Will Africa Feed China*?, (New York: Oxford University Press, 2015), 76-84.

410 Tokunbo Ojo, "Political economy of Huawei's market strategies in the Nigerian telecommunication market", *The International Communication Gazette* 79, no. 3 (2017): 323.

411 *Ibid.*

Table 28. Huawei's initiatives and research collaborations in Africa

Country	Description of initiative
Egypt	Huawei OpenLab opened in Cairo in 2017 to build ICT ecosystem in Northern Africa in response to industry digital transformation.[412] April 2019 meeting with Egyptian Prime Minister Mostafa Madbouly to discuss new capital smart city construction related technologies and practical education and training in various industry sectors.[413] In February 2020, Egyptian Higher Education Minister Khaled Abdel-Ghaffar discussed the implementation of a memorandum of understanding (MoU) signed by both sides to boost ICT talents in Egyptian universities.[414]
South Africa	In 2018, Huawei Cloud opened in the country to provide cloud services in Africa. In May 2019, Huawei partnered with the University of the Witwatersrand (Wits) and the University of Pretoria (UP) to launch a free 5G course.[415]
Nigeria	In 2016, Huawei inaugurated its Innovation and Experience Center and the Joint Open Lab in the University of Lagos (Unilag), Nigeria, to train ICT talents.[416] In 2018, Huawei donated $327,000 ICT equipment to the Digital Bridge Institute (DBI) to boost capacity building in Nigeria.[417]
Algeria	In 2018, the country chose Huawei to build e-governance initiatives in the country by digitising a large volume of official documents of various ministries.[418]
Uganda	In May 2019, Huawei signed an agreement with Uganda's Makerere University to set up an Information Communication Technology (ICT) academy at the institution.[419]
Zambia	Huawei provided components to help build Zambia's smart city solutions and support the activities of Zambia National Data Centre.[420]
Kenya	Kenya's government signed a 17.5 billion shilling (US$172 million) deal with Huawei in April to build a data centre and "smart city" services.[421]

Source: News reports

412 "Huawei Announces New OpenLab in Cairo to Build ICT Ecosystem in Northern Africa", *Huawei,* December 11, 2017, https://www.huawei.com/en/press-events/news/2017/12/Huawei-New-OpenLab-Cairo.

413 "Huawei executives met with Egyptian prime minister to promote digital ecosystem development in Egypt", *Huawei,* April 22, 2019, https://www.huawei.com/en/press-events/news/2019/4/huawei-egyptian-prime-minister-digital-ecosystem-egypt.

414 "Egypt, China's Huawei plan ICT training for talented Egyptian students", *Xinhua Net*, February 27, 2020, http://www.xinhuanet.com/english/2020-02/27/c_138821781.htm.

415 "Huawei takes the 5G war to South African universities", *University World News,* June 1, 2019, https://www.universityworldnews.com/post.php?story=20190601054424951.

416 "Huawei inaugurates Innovation and Experience Center in Nigeria", *Huawei,* October 8, 2016, https://www.huawei.com/en/press-events/news/2016/10/huawei-innovation-experience-center-nigeria.

417 "Huawei donates equipment to Nigerian Institute", *APA News,* October 4, 2018, http://apanews.net/index.php/en/news/huawei-donates-equipment-to-nigerian-institute.

418 "China's Huawei set to help build e-government for Algeria", *China Daily,* March 1, 2018, https://www.chinadaily.com.cn/a/201803/01/WS5a974fb9a3106e7dcc13ec27.html.

419 "Huawei to set up ICT academy at Uganda's top university", *New China,* May 15, 2019, http://www.xinhuanet.com/english/2019-05/15/c_138060968.htm.

420 "New ICT Helps Build Smart Zambia", *Huawei,* accessed March 26, 2020, https://e.huawei.com/topic/leading-new-ict-en/smart-zambia-case.html.

421 "Huawei strengthens foothold in Africa to offset US ban", *op. cit.*

US foreign policy objectives and statements clearly establish that one of their goals in their engagement with Africa is to contain Beijing. While unveiling the US' 2018 Africa strategy, National Security Advisor John Bolton remarked that one of the priorities of the Trump administration is to safeguard the economic independence of African states and protect US national security interests. Bolton detailed how China's foreign direct investment in the region ($6.4 billion in 2016-17) are often part of its BRI initiative and have pushed countries like Zambia and Djibouti into an unsustainable debt trap. He further emphasised that the use of bribes, opaque agreements, and debt traps can hold African countries "captive to Beijing's wishes and demands"[422]. On US concerns about China's surveillance and footprint in the region, African policymakers recognise that such concerns most likely come from US' own "vested interests" and Africa is viewed as a "pawn" in the ongoing geopolitical context.

That is not to say that Huawei has not been implicated in controversies in the region. The Chinese government, in coordination with Chinese telecommunications companies, was found to have transferred confidential data from the headquarters of the African Union to servers in Shanghai over a period of five years without prior consent.[423] Further, a 2019 *Wall Street Journal* article reports that Huawei sold security tools to the governments of Uganda and Zambia for digital surveillance and censorship, and utilised Huawei's staff to intercept encrypted communication from opposition movements.[424] The company's activities did in fact face repercussions in Algeria eight years ago. In 2012, an Algerian court found Huawei and ZTE employees guilty of a bribery scandal, following which the two companies were banned from participating in any public tenders for telecommunications equipment in Algeria for two years.[425]

While these are worrying concerns, current constraints in Africa's telecommunications infrastructure, coupled with low levels of internet penetration mean that there will be no large-scale rollout of 5G in the region. Even if they do, Huawei's affordability and strong footprint complements the region's national priority to swiftly upgrade Internet facilities, thereby making a strong case against Huawei's ban in the African continent.

422 "Remarks by National Security Advisor Ambassador John R. Bolton on the The Trump Administration's New Africa Strategy", *National Security Council,* The White House, December 13, 2018, https://www.whitehouse.gov/briefings-statements/remarks-national-security-advisor-ambassador-john-r-bolton-trump-administrations-new-africa-strategy/.

423 Joan Tilouine and Ghalia Kadiri, "A Addis-Abeba, le siège de l'Union africaine espionné par Pékin," *Le Monde*, January 26, 2018, https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.

424 Joe Parkinson, Nicholas Bariyo and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents", *The Wall Street Journal,* August 15, 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

425 Juha Saarinen, "Huawei, ZTE banned from Algeria", *IT News,* June 14, 2012, https://www.itnews.com.au/news/huawei-zte-banned-from-algeria-304858.

CONCLUSION

This analysis has illustrated how different countries, based on economic, technical and strategic considerations have responded to the ongoing debate on 5G. While countries like the US and Australia have been forthright about banning Huawei because of security risks, other countries like Japan and New Zealand–without explicitly naming the Chinese telecom giant–have done enough to indicate where they stand on the issue. The UK's solution to the 5G dilemma has been the most unique of all; it has long recognised the problems with Huawei's equipment, but is confident that it will be able to mitigate any risks based on the existing mechanism it has in place to oversee and regulate Huawei's kit. Canada–yet to tender a decision on Huawei–is keen on studying the feasibility of the UK's solution and intends to depoliticise the issue as far as possible. On the other hand, countries like Russia and Cambodia have welcomed Huawei with open arms, given their existing partnerships with China.

Three key factors influence a country's decision on this question—cost, security risks, and strategic concerns. How countries approach this decision has varied across the globe. It may have been taken by a single body (for example telecom regulatory authorities); or a combination of bodies at the administrative level (in Canada's case); or at the ministerial or cabinet level; or may involve the Parliament or other legislative committees. This in itself can indicate the parameters upon which a country is carrying out its assessment of 5G vendors and the weight assigned to the issue. The decisions of countries in some cases can be categorised as a clear "yes" or "no", however for many others, they may, by design, keep their response ambiguous or choose to not take any decision given the complexity of the matter.

Huawei's low costs will be most attractive to countries seeking an economically viable upgrade to 5G networks, or those keen on expediting a 5G launch. Though 5G is far from being a reality in Latin America, Africa and Central Asia, its economical pricing will be attractive to these countries, for they may also be willing to overlook any concern related to espionage or surveillance. With these considerations, the advanced countries of the GCC in the Middle East were one of the first in the world to commercially deploy 5G networks and have been able to do so with the help of Chinese vendors.

Security risks associated with 5G networks have dominated conversations in Europe, with the union placing measures to address cybersecurity concerns and the possibility of foreign influence by scrutinising investments, public procurement, and equipment. The EU launched a concerted approach towards 5G network security by undertaking a comprehensive risk assessment and formulating a toolbox to streamline the responses of individual member states towards network security. The EU toolbox gives sufficient leeway to countries to ban Huawei and other Chinese suppliers. EU member states have not come forth with a ban, but are establishing stringent law and policy mechanisms at the national level to ensure that their networks are safe, secure and protected against cyberattacks. Nonetheless, Washington's attempts to dissuade EU member states from using Huawei has not elicited the desired response, with countries like Germany condemning US' sharp rhetoric. Some countries, such as Poland, Czech Republic, Estonia and Romania have been the only few to explicitly side with the US on the issue.

On strategic and foreign policy considerations, China demonstrates the greatest influence in the Middle East, Central Asia, and Asia and the Indo-Pacific. The dominance of China's economic ties in the region, in terms of trade, investment, foreign aid, loans and infrastructure development, have made Beijing a welcome partner. China's size and geographical proximity in Asia and the Indo-Pacific makes it a crucial factor in policy imperatives of smaller nations in the region. Further, the prevalence of Huawei in existing networks coupled with its numerous initiatives to broaden research and technology partnerships guarantees its role as a vendor to supply 5G equipment. A few aberrations in these two regions would include countries like Israel, which have an age-old alliance with the US, or Vietnam, which has been cautious of China and its maritime aggression.

What would have been a straightforward question of choosing the most competent supplier of cutting-edge technology, has transformed into a technological cold war between the US and China. Those who are not averse to Huawei may dismiss the reactions of Washington and other nations as premature, alarmist and most likely motivated by protectionism and perceived loss of tech leadership. However, critics would argue that allowing Huawei may weaken national security and create risks for espionage and cyberattacks from China. In addition, the act alone will establish Beijing as the new global cyber power, giving it the enviable opportunity to shape the next generation of emerging technologies for years to come–much the same way as the US played a crucial role in shaping the internet.

While the US has been on a warpath against Huawei and China, few have joined it on its mission. Changes in America's approach to foreign policy, from its isolationism, protectionism and its withdrawal from multilateralism, have confounded allies and may have even contributed to its failure to fruitfully engage with the world. At the same time, China has steadily risen to be a large economic and military power and continues to do so with the help of large, transnational companies like Huawei. It is increasingly occupying the void left by the US to fill the need for aid, economic support and even multilateralism and globalisation–even if they may be on terms that are unfavourable to recipient nations. Countries are more than aware of the threats that China could pose to the global order, from possible military aggression to digital authoritarianism, but they recognise that Beijing is no longer a factor that can be ignored.

5G and its potential to power emerging technologies like AI and IoT are indispensable for the next stage of digital revolution. Countries will need to examine a host of factors to formulate a policy response that looks at economic, security and strategic aspects of 5G networks. As the geopolitical confrontation between US and China unfolds, the challenge for countries is to arrive at a choice that ushers technological advancements in their region, without forsaking the core concern of national security.

ABOUT THE AUTHOR

Aarshi Tirkey is a Junior Fellow with the Strategic Studies Programme of Observer Research Foundation. Her research focuses on international law — its relevance and application to Indian foreign policy, such as security, trade, bilateral relations and multilateral engagements. A lawyer by training, Aarshi has prior experience in litigation and non-profit work. She was a recipient of the Faculty Graduate Scholarship during her LLM from the National University of Singapore.

Ideas • Forums • Leadership • Impact

Observer Research Foundation
20 Rouse Avenue, Institutional Area,
New Delhi - 110002
India
contactus@orfonline.org
www.orfonline.org