IDSA Monograph Series
No. 65 October 2019

THE ROAD TO 5G

TECHNOLOGY, POLITICS AND BEYOND

MUNISH SHARMA

IDSA Monograph Series
No. 65 October 2019

The Road to 5G
Technology, Politics and Beyond

Munish Sharma

INSTITUTE FOR DEFENCE
STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

ISBN: 978-93-82169-88-8

Disclaimer: The views expressed in this Monograph are those of the author and do not necessarily reflect those of the Institute or the Government of India.

First Published: October 2019

Price: Rs. /-

Published by: Institute for Defence Studies and Analyses
No.1, Development Enclave, Rao Tula Ram Marg, Delhi Cantt., New Delhi - 110 010
Tel. (91-11) 2671-7983
Fax.(91-11) 2615 4191
E-mail: contactus@idsa.in
Website: http://www.idsa.in

Layout & Cover by: Vaijayanti Patankar

Printed at: KW Publishers Pvt Ltd
4676/21, First Floor, Ansari Road
Daryaganj, New Delhi 110002, India
Mobile: +91-9873113145
Phone: +91 11 2326 3498 / 4352 8107
www.kwpub.com

Contents

Chapter 1

Introduction

The 2018 PyeongChang Winter Olympic Games gave a sneak peek into the future of a hyper connected world. Audiences got first-hand experiences of augmented reality based navigation, immersive virtual reality and autonomous vehicles, along with a spectacular light show put together by 1218 drones. As a showcase of Korean technology prowess, and a 5G testbed, the Olympics witnessed many record breaking performances — both in sports as well as in the 5G technology domain. Propelled by an ever increasing appetite of human and connected devices for data and bandwidth, cellular mobile telephony is at the cusp of 5th Generation (5G), promising data speed of the order of 20 Gbps and use cases nothing short of fiction. For instance, Ultra-Reliable Low-Latency Communications pave the way for autonomous vehicles plying on roads, robots performing remote surgeries, or an orchestra of thousands of drones. Enhanced Mobile Broadband — as part of 5G — can enable virtual reality, which has applications as disparate as immersive media experience and pain management.

Cellular mobile telephony has come of age. More than 5 billion people across the globe have access to mobile telephones, and out of them, 3.6 billion have an Internet connection on their mobile devices.[1] The quest for faster and reliable services breaks new grounds every decade in the form of new technology solutions, with improved data speed unveiling new functions, applications, businesses, and markets. Mobile service providers thereafter invest heavily to expand network capacity and coverage to provide faster and more reliable services. Over the last three decades, digital cellular networks have not just transformed

---

[1] GSMA Intelligence, "Global Market Infographic", at https://www.gsmaintelligence.com/research/?file=5a33fb6782bc75def8b6dc66af5da976&download, accessed May 08, 2019.

traditional sectors of the likes of banking, transportation and governance, but diminished geographical distances with real time voice, video and text messaging, and media platforms for social interactions. Personal hand-held devices — in the shape and form of Smartphones now — perform a multitude of functions, in addition to voice calling, gaming, banking, video streaming, shopping and utility payments; they can even host artificial intelligence powered virtual assistants communicating in natural languages to send texts, make voice calls, order food, find routes, or book a cab.

Every generation of cellular mobile telephony has drastically increased data speed. As the next generation of mobile standards — being defined by the International Telecommunications Union[2] (ITU) — 5G promises improved end-user experience through new applications and services, leveraging gigabit speeds and significant improvements in network performance and reliability.[3] Along with high data rate, 5G will also reduce latency, save energy, and enable massive device connectivity, paving the way for next-generation applications such as autonomous vehicles, smart homes, telemedicine etc. for consumers, and massive machine-to-machine communications for industries. For governments, 5G could be the cornerstone of socioeconomic transformation, with improvised governance, transportation, energy distribution in the form of smart cities and smart grids, while yielding a whole new category of jobs, business models and markets. 5G — also heralded as a game-changer in mobile telecommunications — will be ready for full-scale commercial deployment by 2020,[4] as per the requirements laid down by the International Mobile Telecommunications-2020 (IMT-2020) Standard.

---

[2] ITU is a specialized agency of the United Nations for information and communication technologies responsible for allocation of global radio spectrum and development of technical standards.

[3] International Telecommunication Union, "Setting the Scene for 5G: Opportunities & Challenges", 2018, at https://www.itu.int/en/ITU-D/Documents/ITU_5G_REPORT-2018.pdf, p. 1.

[4] International Telecommunication Union, "ITU's Approach to 5G", October 15, 2018, at https://news.itu.int/5g-fifth-generation-mobile-technologies/, accessed May 08, 2019.

Why 5G?

Ever since Guglielmo Marconi made a successful experiment to transmit the Morse code over radio waves in 1895, wireless technology has made tremendous strides. Though radio waves were initially used for telegraphy, advances in its underlying technology expanded their use to audio broadcasting, telephony, and later, to multimedia transmission. Their utility subsequently extended from military and marine communications to wider public use in the form of entertainment, ham radio, and telephones for interpersonal communication. In the late 1970s and early 1980s, the Advanced Mobile Phone System in North America, Total Access Communication System (TACS) in the UK, Nordic Mobile Telephone System in Nordic countries and Eastern Europe, and Nippon Telephone and Telegraph (NTT) in Japan, as well as a few others formed the first generation (1G) of mobile cell phone systems. These were based on analogue communication, and had limitations such as poor audio quality, inefficient use of radio spectrum, low capacity, and the lack of interoperability and security.

As the technology related to wireless access, digital signal processing and integrated circuits progressed further, second generation (2G) of mobile communication standards leveraged it to introduce circuit-switched digital communications, and to overcome a few of the limitations of 1G. For instance, digital coding improved the voice clarity and reduced noise in 2G, and cellular phones needed less power. Following gradual improvements in bandwidth to the GSM Standard, 2.5G (GPRS) and 2.75G (EDGE) began supporting data transmission for web browsing, email access, and multimedia. With growing usage of mobile phones, the demand for data services also increased. Taking advantage of wideband wireless networks, the third generation (3G) of mobile communication standards enabled Internet, multimedia, and streaming services on mobile phones, with increased spectral efficiency and bandwidth. The fourth generation (4G) — with packet switching — introduced IP telephony, ultra-broadband Internet access, and high definition multimedia content streaming. Table 1.1 summarizes the key features, advantages and limitations of the subsequent generations of mobile communication standards.

Table 1.1: Generations of Mobile Telecommunication Standards

Generation	Standard/Technology	Data Rate	Switching	Key Features	Advantages	Limitations
1G	Advanced Mobile Phone System (AMPS) Nordic Mobile Phone System (NMTS) European Total Access Communication System (ETACS)	2.4 Kbps	Analogue and Circuit Switching	Voice calls	Mobility in comparison to Fixed line telephone services	Voice quality, Efficiency, Security, Limited mobility
2G	Global System for Mobile Communications (GSM)	14.4 to 64 Kbps	Digital and Circuit Switching	Voice calls and text messaging	Roaming, encrypted voice transmission, Internet access, Email services	Limited data rates, Less features on mobile devices
2.5G-2.75G	General Packet Radio Service (GPRS) Enhanced Data Rate for GSM Evolution (EDGE)	56–114 and up to 200 Kbps	Digital and Circuit/Packet Switching			
3G	Universal Mobile Telecommunication Systems (UMTS) International Mobile Telecommunications (IMT) 2020 Code Division Multiple Access (CDMA) 2000	384 Kbps	Digital and Packet Switching	Voice calls, text messaging, video calling and broadband data	High data rates, video streaming, maps and location services	Higher bandwidth requirements to support higher data rate, Costly spectrum and higher costs of infrastructure
3.5G-3.75G	High Speed Downlink/Uplink Packet access (HSDPA/HSUPA) Evolution Data Optimized (EVDO)	5-30 Mbps and 100-300 Mbps	Digital and Packet Switching			
4G	Long Term Evolution Long Term Evolution Advanced International Mobile Telecommunications-Advanced	100 Mbps to 1Gbps	Digital and Packet Switching	IP Services for voice and text messaging, broadband data	Reduced latency, High Definition multimedia streaming	Costly spectrum and higher costs of infrastructure
5G	International Mobile Telecommunications-2020	up to 10Gbps	Digital and Packet Switching	Broadband data, Internet of Things, Autonomous Vehicles, Critical Industry Applications	Low latency for mission critical applications, efficient usage of spectrum, reliability, energy efficiency	

Source: Compiled by the author

The hyper connected world of smart devices, smart homes, smart factories, and smart cities is data hungry. By 2022, the number of IP connected devices will be more than three times the global population. Three key factors are driving this unprecedented demand for data and the need to improve the existing 4G wireless networks. The first reason is the shift from wired to wireless devices, elevating data consumption on mobile platforms, such as smart phones and tablets. The double digit growth in IP video traffic, video surveillance, gaming traffic, and video-on-demand has shot up the global demand for mobile data traffic which, in turn, is expected to increase seven fold from 2017 to 2022.[5] The existing networks fall short in maintaining the Quality of Service for such an explosive demand, both in terms of bandwidth and speed. Consumers experience slow speeds, unstable connections, delays, or even loss of service during periods of heavy use or in crowded areas.

The second reason is the spike in number of IP connected devices. Sensors, actuators, control systems, data acquisition systems, and telemetry devices are some of the industrial equipment increasingly being connected to facilitate monitoring, safety, security, and maintenance functions. A Cisco White Paper estimates them to be around 28.5 billion by 2022, half of which will be Machine to Machine connections.[6] The heavy emphasis of industries on IP connected devices in operations, coupled with traction for smart consumer devices such as watches, televisions, speakers, refrigerators, cameras, and meters etc., is driving this segment of demand. Also termed as the Internet of Things, these devices are capable of collecting physical data, and transmitting it over the Internet for further processing, representation or decision making.

The third reason is the technology breakthroughs in the fields of robotics, Artificial Intelligence and cloud computing, which have opened up next-generation applications such as autonomous vehicles and robotic tele-surgery. Such mission-critical applications warrant high-bandwidth,

---

5 Cisco, "Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper", February 27, 2019, at https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html, accessed May 08, 2019.

6 Ibid.

persistent connectivity, and ultra-low levels of latency across the network. In addition to these requirements, the coordinated system of GPS, cameras, sensors, and radar in the case of an autonomous vehicle for instance, needs a reliable network which can function under all weather or geographical conditions. Likewise, visualisation, high-definition video streaming, and the transmission of sensory data to remote locations, etc. require high performance networks in terms of latency, jitter, and packet loss. In essence, it is not a single factor but a combination of factors which are driving cutting-edge research in all the aspects of 5G technology, paving the way for high-capacity low-latency ultra-reliable super-fast networks.

Nevertheless, technology — whether in research or actual deployment — will come at a cost. Operators and mobile service providers, catering to the needs of millions of users and connected devices, will need to bring down the cost per GB for the end users. The business and economic prospects of 5G are equally promising as the 5G use cases. High cost of 5G deployment will be offset by improved efficiency and economies of scale, as the projections for revenue and 5G user base over the next five years are actually quite optimistic.

The Economics of 5G

Mobile technologies have witnessed a sustained growth ever since they were introduced, driving both social prosperity and economic development. With each passing day they continue to connect more people and, lately, things and machines of personal use, household items, and industrial functions. As of 2018, there were 5.1 billion mobile services subscribers worldwide, and the numbers will continue to increase, with vast potential for penetration in developing and under-developed economies. A number of studies and reports related to mobile growth, IoT, data usage, and 5G connections, etc. make varying forecasts and projections. Cisco, for instance, projects 8 billion personal mobile devices and 4 billion IoT connections by 2022.[7] Ericsson

[7] Cisco, "Global Mobile Networks Will Support More Than 12 Billion Mobile Devices and IoT Connections by 2022", February 19, 2019, at https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1967403&utm_source=newsroom.cisco.com&utm_campaign=Release_1967403&utm_medium=RSS, accessed May 10, 2019.

estimates mobile data traffic to rise at a compound annual growth rate (CAGR) of around 45 per cent till 2022.[8] Once 5G witnesses a commercial launch in 2020, it is slated to carry 12 per cent of the global mobile data traffic by 2022[9], which will increase to 25 percent by 2024 (Figure 1.1).[10] By 2024, the global mobile broadband subscriptions — at 8.4 billion — will account for close to 95 per cent of all mobile subscriptions, and 5G will reach more than 40 per cent of the global population.[11] That will also elevate average data consumption on a smart phone to 21 GB per month. Table 1.2 breaks down the projections of mobile data consumption on a smart phone according to different traffic categories.

5G technologies are expected to contribute USD 2.2 trillion to the global economy over the next 15 years.[12] In a study commissioned by the Cellular Telecommunications and Internet Association (CTIA), IHS Markit estimated that 5G could produce up to USD 12.3 trillion in global sales across multiple industries by 2035.[13]

---

8 Ericsson, "Future mobile data usage and traffic growth", at https://www.ericsson.com/en/mobility-report/future-mobile-data-usage-and-traffic-growth, accessed May 10, 2019.

9 n. 7.

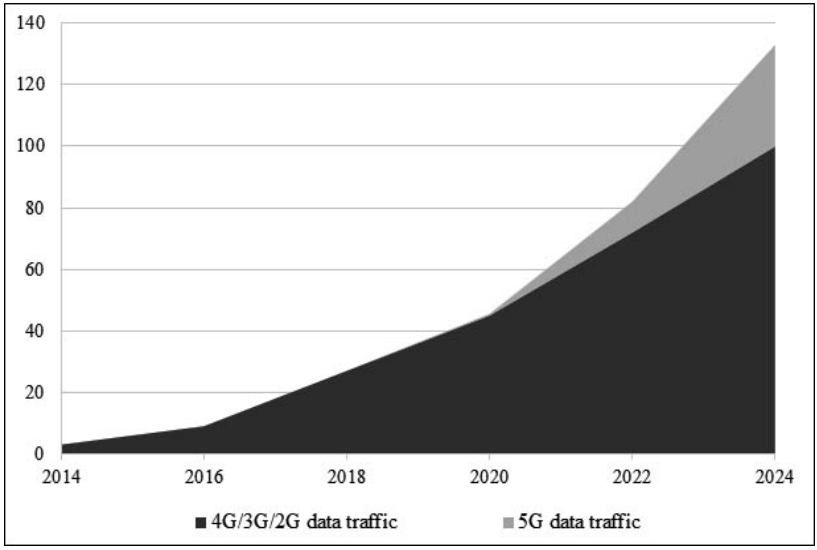
10 Ericsson, "Ericsson Mobility Report", November 2018, at https://www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-november-2018.pdf, p. 16.

11 Ibid., p. 7.

12 GSMA Intelligence, "The Mobile Economy 2019", at https://www.gsmaintelligence.com/research/?file=b9a6e6202ee1d5f787cfebb95d3639c5&download, p. 4.

13 Karen Campbell, et al., "The 5G Economy: How 5G Technology Will Contribute to the Global Economy," *IHS Markit*, January 2017, at https://cdn.ihs.com/www/pdf/IHS-Technology-5G-Economic-Impact-Study.pdf, p. 16.

Figure 1.1: Global Mobile Data Traffic (in Exabyte per month)



One Exabyte is equivalent to one billion Gigabytes

Table 1.2: Projection of Average Data Consumption on a Smart Phone.[14]

Traffic Category	World Average Data Consumption (GB per month)	
	2018	**2024**
Downloads	0.6	1.2
Messaging	0.5	0.9
App Traffic	1	2.1
Audio Streaming	0.1	0.4
Video Streaming	3.4	16.3
Total	**5.6**	**20.9**

Source: www.ericsson.com

[14] n. 10, p. 24.

As the demand for 5G deployment picks traction across the globe, it will be an attractive business case and a strong revenue stream for equipment manufacturers, network integrators and, subsequently, mobile service providers. AT&T estimates the deployment costs to be between USD 20,000 to USD 50,000 per site, assuming fibre backhaul for sites, while Nokia estimates the same to be between USD 40,000 to USD 50,000 for a site that requires trenching and power connection. As per an ITU estimate, a small cell 5G network deployment could cost around USD 6.8 million for a small city to USD 55.5 million for a large, dense city.[15] The total cost of 5G deployment across the 28 Member States of the European Union could be somewhere around EUR 56 billion, as per an European Commission estimate.[16] The cost of the deployment includes installation of Radio Access Network (antenna, base station electronics), site upgrade costs (permits costs and civil works), optical fibre network (provision of new ducts and laying down optical fibre), etc. in addition to the switching equipment. The capital expenditures, however, will depend upon factors such as population, population density, proposed coverage area, spectrum license fee, optical fibre penetration, and real estate costs.

Previous market trends and analysis shows that frontrunners or early adopters of mobile telephony grow faster than the late adaptors or laggards as they capture the economic benefits of the new technology. Frontrunners are able to convert their advantage into revenue with better offerings in their respective markets. Operators or mobile service providers, therefore, continuously upgrade their technology, and try to stay ahead of the competition. An Ericsson study of 2017 found that 62 frontrunners (out of 195 mobile service providers) of 4G could achieve compounded annual yearly revenue growth of above 10 per

---

[15] n. 3.

[16] European Commission, "5G deployment could bring millions of jobs and billions of euros benefits, study finds", September 30, 2016, at https://ec.europa.eu/digital-single-market/en/news/5g-deployment-could-bring-millions-jobs-and-billions-euros-benefits-study-finds, accessed May 15, 2019.

cent between 2013 and 2017.[17] A Congressional Research Service report found that US companies were in the leadership position in new technologies development, industry standards development, products, etc. during the deployment of 4G networks. It added around USD 100 billion to the US economy.[18]

Beyond the estimated economic and business incentives, the 5G rollout has its own set of challenges, relating to the cost of building network and infrastructure, the availability of the desired spectrum, handset compatibility, and technical complexities,[19] to name a few. Given the enormous economic potential, the race to 5G has become extremely competitive. Technology companies in the foray, such as network equipment manufacturers, chipset makers, smart phone manufacturers, and software companies want to be the first in their respective segments. Telecom or mobile services providers across the globe have begun investing or committed investments into 5G infrastructure to gain an upper hand in their domestic markets. Many have partnered with equipment manufacturers to run 5G pilot projects. The governments are openly supporting 5G efforts to ensure that their companies are the first to deploy 5G products and roll-out services.

Concomitantly, competition among the globally established telecommunication equipment and networking gear makers, like Cisco, Samsung, Ericsson, Nokia, Fujitsu and Huawei, is heating up, all vying for first-mover advantage and industry leadership. It has not left geopolitics untouched either, instigating a race among nation states towards 5G, whether it is related to research publications, trial runs, facilitating industry, speeding up spectrum allocation, or influencing standards development. On top of that, an all-out American campaign

---

[17] Ericsson, "What makes a mobile operator successful?", at https://www.ericsson.com/en/networks/trending/insights-and-reports/growth-codes, accessed May 15, 2019.

[18] CTIA-The Wireless Association, "The Race to 5G," at https://www.ctia.org/the-wireless-industry/the-race-to-5g, accessed May 15, 2019.

[19] EY, "China is poised to win the 5G race", 2018, at https://www.ey.com/Publication/vwLUAssets/ey-china-is-poised-to-win-the-5g-race-en/$FILE/ey-china-is-poised-to-win-the-5g-race-en.pdf, p. 27.

to ban Chinese telecommunication equipment makers from global markets has spiralled into diplomatic turmoil, compelling countries to walk a political tightrope. India is carefully working out the options, not just on the question of allowing Chinese telecommunication equipment manufacturers to supply 5G gear, but also pertaining to spectrum allocation, infrastructure, and building a domestic 5G ecosystem — anticipating a trickle-down effect on the economy. The race to 5G, in essence, is to gain the first mover's advantage, and monetise the immense business opportunity it holds — but technology is the true differentiator between innovators and adaptors.

Chapter 2

Enabling 5G: Technology and Requisites

Wireless technology made it possible to transmit voice over microwaves, overcoming the mobility limitations of wired telephones. All wireless technologies use electromagnetic spectrum — which is limited and heavily regulated as different services and applications share it to meet their specific needs. With mobility in telecommunication services and their wide adaptation in business, personal use, and entertainment, the demand for spectrum has increased over the years in line with the exponential rise in mobile data traffic. Beyond a level, even 4G cannot meet the traffic requirements, even if the available spectrum is fully utilized. There are just two ways to meet the growing demand: one is to exploit unharnessed frequency bands of the electromagnetic spectrum and the other is to use the available spectrum efficiently. 5G intends to do both. Advancing research in technologies which improve spectrum efficiency and harness millimeter waves (mmWaves) from a higher-band spectrum is one of the key drivers of 5G. High-band spectrum can provide greater bandwidth and speed. However, it is susceptible to blockage and suffers from higher path loss. With mmWaves the major drawback is that their coverage is limited as these waves cannot penetrate objects or travel long distance — unlike microwaves used in 3G or 4G. Capitalizing the strengths of this spectrum is relatively easy; but the technological challenge is to overcome its shortcomings. The technology empowering 5G is simultaneously going to address the shortfalls in the existing network architecture to unleash a whole new set of applications, and use cases for both businesses and consumers.

With promising speed and bandwidth, 5G networks will support communication needs across industries, businesses, and consumers. In addition to increased speed and capacity, 5G networks will also deliver stable low-latency services with incredibly high reliability — all of which

are essential for time-critical applications, such as self-driving cars.[1] In the previous generations, mobile communication standards were set and adopted under the auspices of the International Telecommunication Union — a specialised UN body responsible for the allocation of global radio spectrum and the development of technical standards. In the case of 5G, "International Mobile Telecommunication 2020 standards" (IMT-2020) of the ITU will set the macro level requirements. However, alongside, the industry driven standardization body 3GPP (3rd Generation Partnership Project) — which has developed technical specifications for mobile technologies since 1998 — continues to do so for 5G networks, based on the ITU requirements. Besides being an arduous effort in terms of technology development and standardization, 5G deployment has its own set of challenges in the form of spectrum allocation, infrastructure and security.

What is 5G? : The Technology behind IT

The technology empowering 5G intends to achieve spectral efficiency, energy efficiency, and infrastructure utilization. Spectral efficiency aims to optimize different frequencies to provision higher bandwidth. Energy efficiency intends to reduce power consumption in both the transmitter and processing segments. The sharing of physical infrastructure — Radio Access Network (RAN) infrastructure, transmission, and core networks — among service categories as well as service providers will lead to the optimum utilization of the infrastructure. Over and above, the deployment of 5G networks is going to harness advances in technologies which enable millimetric band utilization, Network Function Virtualization, Network Slicing, massive MIMO, and Software Defined Networks for efficiency and flexibility. Collectively, these technologies are a major architectural shift from the present deployment of 3G or 4G/LTE networks.

In different bands, electromagnetic waves demonstrate distinct abilities and propagation characteristics, whether it is hop, spread, penetration, or path loss. Using New Radio interface, 5G banks on transmission at

---

[1] International Telecommunication Union, "ITU's Approach to 5G", October 15, 2018, at https://news.itu.int/5g-fifth-generation-mobile-technologies/, accessed May 08, 2019.

mmWave bands, which was not feasible until now. This band was not considered for mobile communications earlier because the waves could not travel far, could not penetrate walls, and atmospheric features such as rain, fog, and moisture led to high signal attenuation. The mmWaves can utilise frequencies in the band of spectrum between 30 GHz and 300 GHz, which was previously thought unsuitable for mobile communications. Small cells, which are an integral part of 5G deployment, solve this problem. In addition to increased speed and bandwidth, 5G can support a larger number of devices in a given coverage area, which could be of the order of 1 million devices per square kilo meter, compared to just 4000 in the case of 4G. Along with communications technology, software engineering has also made strides which find applications in 5G. Softwarization is a true value proposition for 5G, as it can help mobile service providers to virtualize their network functions and make them programmable. Previous generations — 4G and earlier — used the same mobile network architecture to host multiple services such as voice, messaging, and mobile broad band.[2] With softwarization, 5G can build dedicated logical networks for respective services.

Software-Defined Networking (SDN) technology changes the way network routing is managed, by separating the control function of a routing device from its forwarding function. SDN allows dynamic reconfiguration of network elements (switches or routers of the network) in real time — which means that networks could be controlled by software rather than hardware through application programming interfaces using a centralized control plane.[3] With SDN, 5G networks can manage and automate network redundancy from a centralized control plane and determine optimal data flow. This significantly improves resilience, performance, and quality of service for the 5G networks.

---

2 5GPPP Architecture Working Group, "View on 5G Architecture", December 2017, at https://5g-ppp.eu/wp-content/uploads/2018/01/5G-PPP-5G-Architecture-White-Paper-Jan-2018-v2.0.pdf, p. 17.

3 Nathan Cranford, "The role of NFV and SDN in 5G", *RCR Wireless News*, December 04, 2017, at https://www.rcrwireless.com/20171204/fundamentals/the-role-of-nfv-and-sdn-in-5g-tag27-tag99, accessed May 08, 2019.

Network Functional Virtualization (NFV) replaces network functions on dedicated appliances such as routers, load balancers, and firewalls, with virtualized instances to improve the utilization of hardware resources. It allows multiple network configurations and network scaling based on demand. NFV in 5G will be a major breakaway from the prevalent network management practices in the existing mobile networks, where network hardware cannot be shared, and additional hardware is required to increase capacity.[4] NFV allows operators to manage and expand their network, load-balance, scale up or down, and move functions based on the demand, using virtual, software based applications — also reducing the cost of network changes and upgrades substantially.

Network sharing is already one of the successful operating models for mobile network operators to reduce capital and operational expenditures. A step ahead, network slicing permits a physical network to be partitioned into multiple virtual networks that can support different Radio Access Networks or types of services. Network slices are logical segments, and they reduce network construction costs by using communication channels more efficiently, and by sharing physical infrastructure.[5] Network slicing enables multiple virtual networks to operate over a single, yet shared physical infrastructure (Figure 2.1). In addition to sharing capital-intensive network infrastructure, network slicing, as part of 5G deployment, will allow operators to scale their network as per the demand[6] — catering to both flexibility and efficiency in the network.

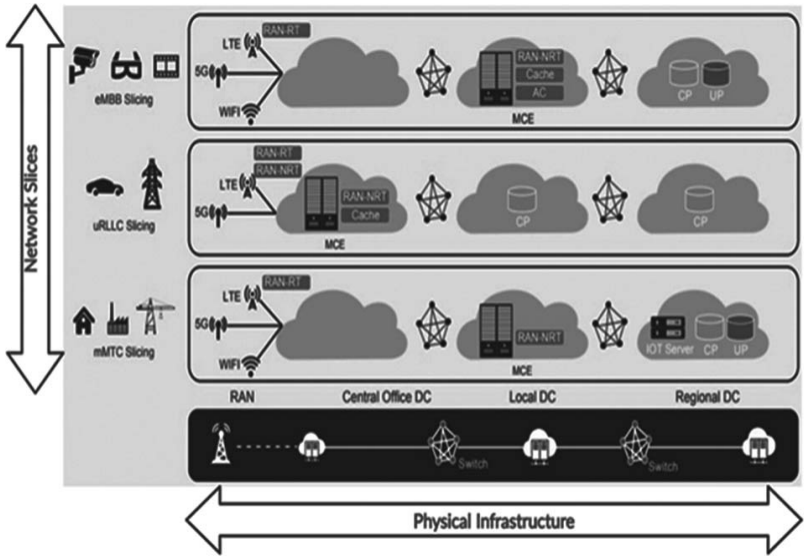
---

4 GSM Association, "Migration from Physical to Virtual Network Functions – Best Practices and Lessons Learned", October 2018, at https://www.gsma.com/futurenetworks/5g/migration-from-physical-to-virtual-network-functions-best-practices-and-lessons-learned/, accessed May 10, 2019.

5 International Telecommunication Union, "Setting the Scene for 5G: Opportunities & Challenges", 2018, at https://www.itu.int/en/ITU-D/Documents/ITU_5G_REPORT-2018.pdf, p. 12.

6 Ericsson, "Network Slicing", at https://www.ericsson.com/en/digital-services/trending/network-slicing, accessed May 10, 2019.

Figure 2.1: Network Slicing in 5G



Source: www.huawei.com

A typical mobile network is divided into cells, and each cell has a radio base station to provide the coverage. Mobile devices in a cellular network communicate with the nearest base station for both voice and data. The signal is then transmitted to the core network through cables or radio links. The base station site and equipment are capital intensive from the point of view of deployment and maintenance. For operators, the cost of land/space acquisition, civil works, network provisioning, and equipment installation on the site attract significant portions of the capital expenditure.

Due to the frequency band at which 5G services will operate, 5G deployment will require a massive number of base stations as compared to existing networks. Capitalizing on matured cloud computing technology, 5G will use Cloud Radio Access Network (C-RAN) to improve efficiency. The Radio Access Networks of earlier generations were placed close to the base stations. Hence, the bulk of the deployment cost pertained to the vast number of distributed base

station sites and last-mile transport network links.[7] By replacing distributed signal processing units at mobile base stations with a centralised cloud based radio access network, C-RAN allows operators to pool resources, reuse infrastructure, simplify network operations and management and simultaneously reduce energy consumption, and lower their capital and operational expenditures.[8] Shared physical infrastructure also encompasses space, electricity, and cooling systems.

The above technology segments are the key differentiators of 5G, in addition to the likes of Massive MIMO, Beamforming, and small cells. The success of 5G architecture is credited to the persistent cutting edge research in the science and engineering of communications. It is also building an entirely new ecosystem of technological and enterprise innovations to improve network performance and reduce costs. Leveraging these technologies, 5G is targeting three consolidated service categories (Figure 2.2) which have completely different performance requirements and traffic patterns. The three service categories are:

- **Enhanced Mobile Broadband (eMBB)**, which can enable high user mobility, especially under the scenarios requiring high data rates across a wide coverage area or ultra-high speed connection, such as on high-speed trains or in densely populated areas. This is planned to be achieved with mmWave antennas.

  eMBB use cases: Virtual Reality and Augmented Reality services, live sporting events.

  eMBB requirements: Stable connections with very high peak data rates. According to ITU guidelines, 5G network speeds should have a peak data rate of 20 Gbps for the downlink, and 10 Gbps for the uplink.

---

[7] Telefónica, "Cloud RAN Architecture for 5G", at http://www.tid.es/sites/526e527928a32d6a7400007f/content_entry5321ef0928a32d08900000ac/578f4eda1146dde411001d0e/files/WhitePaper_C-RAN_for_5G_-_In_collab_with_Ericsson_SC_-_quotes_-_FINAL.PDF, p. 2.

[8] Michael, "5G, C-RAN, and the Required Technology Breakthrough", *Medium*, June 21, 2018, at https://medium.com/@miccowang/5g-c-ran-and-the-required-technology-breakthrough-a1b2babf774, accessed May 10, 2019.

- **Massive Machine Type Communications (mMTC)**, for a very large number of connected devices, with varying requirements of the quality of service and located in a small area such as an industry or a production facility. Machine-type communications are characterized by fully automatic data generation, exchange, processing, and actuation among intelligent machines,[9] transmitting at irregular intervals low or large volumes of delay-sensitive information.

  mMTC use cases: Internet of Things (IoT), smart cities, smart power grids, and smart industries, utilities and manufacturing.

  eMBB requirements: Active intermittently at low and fixed transmission rate. mMTC enables high density of connectivity, which is around 1 million connections/Km^2.

- **Ultra Reliable Low Latency Communications (URLLC)**, which lays down stringent requirements for network latency as low as one millisecond (compared to 50 milliseconds for 4G) and reliability in terms of packet loss to be better than one in 10,000 packets. This service category enables communications in mission critical applications where bandwidth is not quite as important as speed. For instance, relay protection in power transmission requires latency less than 5 milliseconds.

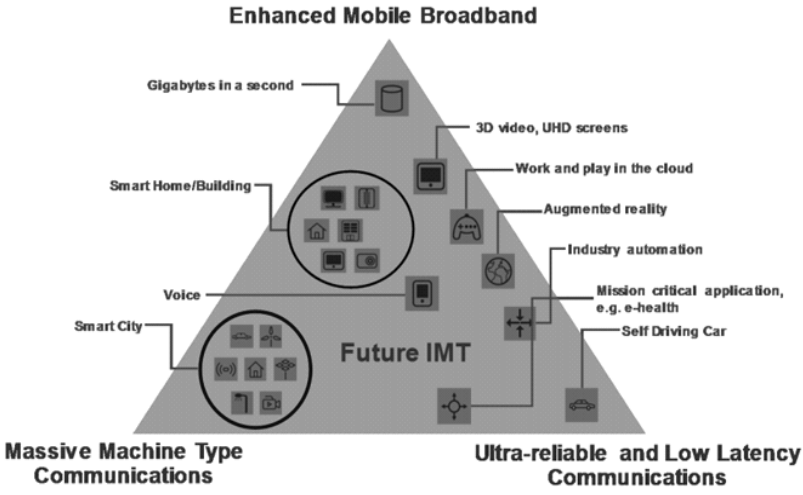
  URLLC use cases: Robotics, autonomous vehicles, and remote surgeries.

  URLLC Requirements: Latency in a 5G network could get as low as 4 milliseconds in a mobile scenario, and can be as low as 1 millisecond in URLLC scenarios.

---

[9] Eryk Dutkiewicz et al., "Massive Machine-Type Communications", *IEEE Network*, Vol. 31, No. 6, November 2017, pp. 6-7, at https://ieeexplore.ieee.org/document/8120237.

Figure 2.2: 5G Service Categories



Source: www.itu.int

The primary improvements 5G makes over 4G mobile networks include high bandwidth, broader coverage, and ultra-low latency, combined with enhanced power efficiency, cost optimization, massive IoT connection density, and the dynamic allocation of resources based on real time awareness of content, user, and location.[10] The three service categories, discussed above, are the prime benchmarks for network performance in 5G use cases. The 5G trials and pilot projects aspire to meet these requirements and specifications. In addition to these stringent technical requirements, successful and timely deployment of 5G needs to meet the challenge of spectrum availability and infrastructure provisioning.

---

[10] Cisco, "Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper", February 27, 2019, at https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html, accessed, May 08, 2019.

Spectrum and Infrastructure Requirements for 5G

Mobile networks use microwaves from the electromagnetic spectrum to provide wireless connectivity to end users. The electromagnetic spectrum extends from gamma radiation at the short-wavelength (high frequency) end to high-wavelength radio waves. In between, there are infra-red, visible light, ultra violet, and X-rays, which find applications in remote controls, radio broadcasts, television broadcasts, air traffic controls, satellite communications, wireless networks, and medical diagnosis. Microwaves, used by mobile networks, occupy a frequency range from 300 MHz (wavelength of 1 m) to 300 GHz (wavelength of 1 mm). As a waveform property, low frequency waves can travel longer distances, and can penetrate objects, such as buildings and walls and, therefore, they are used for wider coverage applications. On the flip side, their capacity to carry information or data is low. On the other hand, high frequency waves have limited coverage as they cannot penetrate through objects; but they have a higher capacity. For usability and distribution between different users, microwave spectrum is further divided into frequency bands which are then allocated or assigned to a specific service provider over a period of time. The wider the frequency bands, the more information they can carry. Wider or broader frequency bands are also referred to as 'broadband'.

Since a wide range of services, both military and civilian, rely on electromagnetic spectrum which already is a constrained resource, regulatory bodies of national governments manage the spectrum to balance social and economic benefits with security needs. Governments work with the ITU to allocate specific frequency bands to certain services on a global or regional basis. The international framework to do so is the Radio Regulations of the International Telecommunication Union[11], ratified by the Member States of the ITU. The framework allows countries to manage spectrum in their national boundaries, and it is set out through a National Frequency Allocation Table, assigning frequency bands to the specific services under designated conditions. This helps

---

[11] International Telecommunication Union, "Radio Regulations", 2016, at http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/1.43.48.en.101.pdf.

tremendously to limit interference, and allows interoperability of devices across countries. In the case of mobile services, this facilitates international roaming, allowing subscribers to use their mobile telephones across different countries. Furthermore, spectrum could either be managed through a spectrum licence, or it is unlicensed (license exempt), depending upon its characteristics and usability. The frequency bands ideal for satellite communication, for instance, are licensed, while the frequency bands at which Wi-Fi and Bluetooth services work are unlicensed.

In order to harness the benefits from different bands, 5G implementation will rely on multiple bands in the spectrum to maximise coverage and bandwidth. These include low-band (below 1 GHz), mid-band (1 GHz-6 GHz), and high-band from the mmWave spectrum (30 GHz and 300 GHz). All the three bands, or frequency ranges, have different characteristics. The low-band can support widespread coverage in urban and suburban scenarios, within buildings (indoor), and allows operators to support IoT devices and services over a wide area. Mid-band can augment capacity and coverage, while the mmWave band, which has large spectrum availability, can support high speed broadband applications in high-density areas through the deployment of small cells. Low-band and Mid-band spectrum is currently being used for 2G, 3G and 4G services; but spectrum from the mmWave band is anticipated to support the stringent requirements of data speed, capacity, quality of service, and low latency under 5G standards. 5G intends to harness the performance characteristics of each band to improve the capacity and efficiency of the network. The low-band spectrum will, therefore, comprise the coverage layer of 5G; the mid-band will form the coverage and capacity layer; and the mmWave band will be the layer providing high data rates — balancing optimal coverage, capacity, and performance.

Surpassing the technology challenges in harnessing electromagnetic spectrum, the timely roll out of 5G services will also depend upon governments and regulatory bodies to provide affordable and predictable access to the right amount and type of spectrum. At present, there are several spectrum bands under consideration. However, 5G will need harmonised spectrum for global compatibility. The GSM Association, the trade body representing mobile network operators

worldwide, recommends the 26 GHz, 40 GHz, and 66-71 GHz bands, and new mobile bands including spectrum in the 3.5 GHz range.[12] China and Japan, for instance, are considering the 3.8-4.2 GHz range, while some countries plan to use spectrum in the 4.5-5 GHz range. Countries are likely to reach an agreement on the 5G spectrum at the World Radiocommunication Conference, scheduled from 28 October to 22 November 2019, under Agenda Item 1.13.

Although spectrum allocation for mobile standards is internationally coordinated, the approach to release and assign the spectrum varies from country to country. Timely availability and affordability of the desired spectrum will be key to the success of 5G deployment. Given the vast numbers and economic opportunity, most governments will tend to monetise this opportunity and raise revenue from spectrum licensing, most probably through auction. The formidable challenge, however, is to avoid over-pricing of the spectrum as the staggeringly high competition is likely to drive the prices up. Over-pricing could be detrimental as it results in substantial amounts of spectrum being left unsold.[13] This was seen in the case of spectrum auction in India between 2012 and 2016, where sub-1 GHz bands were left unsold owing to exceptionally high reserve prices.[14] High spectrum prices could also lower the returns on investment for mobile service providers, which may incidentally drive the costs up for consumers. However, there is an alternate argument also: that mobile service providers may not necessarily pass on the spectrum prices to consumers, and that they would rather factor in future growth and profitability while buying the

---

[12] "5G Spectrum GSMA Public Policy Position", GSMA Intelligence, July 2019, at https://www.gsma.com/spectrum/wp-content/uploads/2018/11/5G-Spectrum-Positions.pdf, p. 2.

[13] "Effective Spectrum Pricing: Supporting better quality and more affordable mobile services", GSMA Intelligence, February 2017, at https://www.gsma.com/spectrum/wp-content/uploads/2018/12/Effective-Spectrum-Pricing-Full-Web.pdf, p. 40.

[14] The October 2016 auction witnessed only 41 percent of the spectrum sold, and 700 MHz band received no bids, reportedly due to the high reserve prices.

spectrum.[15] Governments have the authority to influence the prices of the spectrum, either through directly setting high final prices, or setting high reserve prices, or even by constricting the supply of the spectrum itself. Along with that, ambiguities over long-term spectrum plan or a roadmap and the lack of transparency in award rules can also lead to uncertainties, further driving up spectrum prices. In addition to spectrum, a 5G mobile network would also need physical infrastructure to provision cell sites and a transport network to carry volumes of data between the core network and the radio units installed at geographically dispersed cell sites.

A mobile network is built up of cells, whose size or coverage radius depends on the frequency — differentiating between macro cells and small cells. The higher the frequency, the smaller is the cell size. 5G will lead to a dense network of small cell sites, with a coverage radius measured in meters as compared to kilometres in the case of macro sites,[16] also known as microcells, picocells, and femtocells. Such deployment will need heavy investment in spectrum procurement or licensing, new radio interfaces, macro-cellular equipment, small cell deployment, and fronthaul and backhaul infrastructure.[17] In a mobile network, mobile backhaul is a term commonly used to describe the transport network that provides connectivity between the core network and the Radio Access Network.[18] It is the network that transports

---

[15] "Spectrum pricing in developing countries: Evidence to support better and more affordable mobile services", GSMA Intelligence, July 2018, at https://www.gsma.com/spectrum/wp-content/uploads/2018/12/2018-07-17-5a8f746015d3c1f72e5c8257e4a9829a.pdf, p. 7.

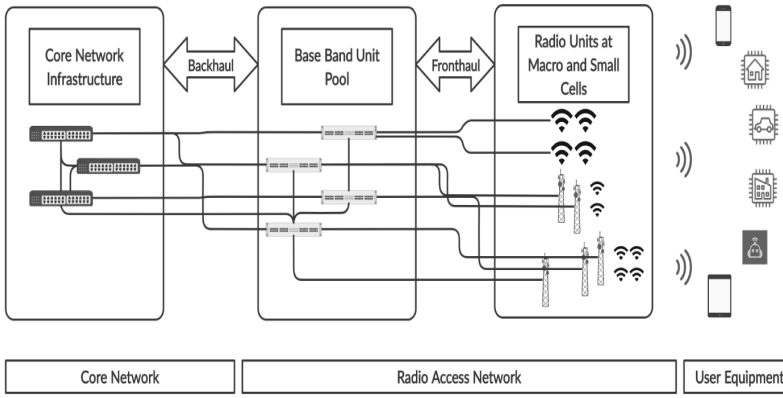
[16] Deloitte, "Communications infrastructure upgrade the need for deep fiber", July 2017, at https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-5GReady-the-need-for-deep-fiber-pov.pdf, p. 4.

[17] "Technical Preparation needed for 5G Infrastructure Deployments", April 2018, Wireless Infrastructure Association, at https://wia.org/wp-content/uploads/WIA-White-Paper-5G-Technical-Prep.pdf, p. 3.

[18] "Technology Digest", *Telecom Regulatory Authority of India*, Issue 1, July 2011, at https://main.trai.gov.in/sites/default/files/201112190518470327500Tech_times_18_July.pdf, p. 1.

cellular traffic between base stations and the nearest traffic switching centre of the service provider.[19] The concept of fronthaul is new. In the new cellular architecture, Remote Radio Heads take the radio elements of a base station and separate them from the baseband controller. Therefore, fronthaul is used to describe the connection between the centralized Baseband Unit (BBU) and the Remote Radio Head (RRH) installed at cell sites (Figure 2.3).

Figure 2.3: Fronthaul and Backhaul in a 5G Mobile Network



Mobile service providers use a mix of fixed-line (optical fibre or copper-line) and wireless components to backhaul cellular traffic under varied environments such as urban and rural, office and residential complexes, or crowded public areas. Table 2.1 outlines the different approaches to backhaul cellular traffic to and from macro and small cell base stations.

---

[19] "The Disruptive Impact of 5G on Optical Network Architecture", Tejas Networks, March 05, 2019, at https://www.tejasnetworks.com/articles/-5g-on-optical-network-architecture, accessed May 20, 2019.

Table 2.1: Mobile Backhaul Technology Trade-Offs

Segment	Microwave (7-40 Ghz)	V-Band (60 Ghz)	E-Band (70/80 Ghz)	Optical Fibre	Copper (Bonded)	Satellite
Future-Proof Available Bandwidth	Medium	High	High	High	Very Low	Low
Deployment Cost	Low	Low	Low	Medium	Medium/ High	High
Suitability for Heterogeneous Networks	Outdoor Cell-Site/ Access Network	Outdoor Cell-Site/ Access Network	Outdoor Cell-Site/ Access Network	Outdoor Cell-Site/ Access Network	Indoor Access Network	Rural Only
Interference Immunity	Medium	High	High	Very High	Very High	Medium
Time to Deploy	Weeks	Days	Days	Months	Months	Months
License Required	Yes	Light Licensed/ Unlicensed	Licensed/ Light Licensed	No	No	No

Source: ABI Research

Wireless backhaul takes place in the sub-6 GHz (licensed and unlicensed), microwave (6 GHz to 40 GHz), V-band (60 GHz), and E-band (70/80 GHz band). Although the wireless backhaul option is cheap, quick, and easy to deploy as compared to wired backhaul (especially optical fibre), it has bandwidth limitations and is prone to interference. Mobile service providers rely heavily on microwave (7 GHz to 40 GHz), V-band (60 GHz) and E-band (70/80 GHz) backhaul options. V-band or the E-band options are also suitable to support 5G as they can deliver throughput from 10 Gbps to 25 Gbps. However, due to higher frequency, these bands are subject to attenuation from atmospheric effects, which limit their range. Limited range and high throughput of E-band also works in the favour of 5G, as it could be used to achieve high bandwidth over short distance, which is ideal for small cell deployment.[20]

---

[20] "Mobile backhaul options: Spectrum analysis and recommendations", GSMA Intelligence, September 2018, at https://www.gsma.com/spectrum/wp-content/uploads/2019/04/Mobile-Backhaul-Options.pdf, p. 13.

Traditionally, 2G and 3G mobile networks relied on microwave backhaul to connect cell sites with the nearest switching centre. To cater to the increased data flow, 4G introduced IP-based connectivity by replacing copper-based or microwave-based cell sites with optical fibre, which further accelerated the demand for Fibre to the Tower (FTTT). The ability of the 5G networks to carry the anticipated amount of data will essentially depend upon the capacity, reliability, and availability of mobile backhaul networks. As a major shift from the previous generations of mobile technology, 5G will have a dense network of small cells in CRAN architecture. It will integrate fronthaul and backhaul in a single transport network, whose functioning is dependent on a strong mobile backhaul to transport data between the core network and edge subnetworks.

In order to meet the capacity and latency requirements under 5G, optical fibre connectivity is utmost important to support small cell deployment and increased mobile backhaul traffic.[21] An ABI Research of 2017 estimates that the majority share, around 56 percent, of backhaul was supported by traditional microwave (7 GHz to 40 GHz) backhaul equipment. But the higher bandwidth requirements of 4G and LTE are driving the adoption of optical fibre, which will grow from 26.2 per cent in 2017 to 40.2 per cent by 2025 globally, reducing microwave backhaul (7 GHz to 40 GHz) to 38.2 per cent for macrocell sites.[22] At present optical fibre is the predominant backhaul method for small cells with 43.2 per cent, followed by microwave (7 GHz to 40 GHz), and by 2025, the percentage of small cells supported by optical fibre will grow to 56.1 per cent.[23]

5G will capitalize on the recent advances in optical signal processing, such as dense lightwave multiplexing, optical amplification, and reconfigurable optical add-drop multiplexing, which can deliver 100G/200G/400G bit rates per wavelength over thousands of kilometres,

---

[21] EY, "China is poised to win the 5G race", 2018, at https://www.ey.com/Publication/vwLUAssets/ey-china-is-poised-to-win-the-5g-race-en/$FILE/ey-china-is-poised-to-win-the-5g-race-en.pdf, p. 33.

[22] n. 20, p. 3.

[23] n. 20, p. 19.

at the lowest cost per bit for the core network.[24] Considering the requirements of 5G, optical fibre is a future-proof and scalable medium, which is also operationally cost-effective in the long term.[25] Though optical fibre offers tremendous capacity, it has its own limitations in terms of costs and the logistics of deployment. Laying down optical fibre is also time consuming, which involves trenching, ducting and permits. When mobile service providers are looking at the quick provisioning of sites, laying down new optical fibre is a costly option, as compared to wireless backhaul.

In the run-up to 5G, countries faring badly in optical fibre network are gearing up to quickly lay down optical fibre cables on a nationwide scale. The UK, for instance, has earmarked GBP 6.85 billion for 5G infrastructure upgrades by 2021, which includes increasing fibre penetration. A Deloitte Consulting analysis estimates that the USA requires an investment of USD 130–150 billion to build optical fibre infrastructure over the next five to seven years.[26] India and China also have vast plans to increase the penetration of optical fibre to urban areas, and extend the reach to rural areas. In 2017, China added 7.05 million km of optical fibre cable.[27] India, in the same year, laid 1,55,000 km of optical fibre cable under the BharatNet project,[28] and the aim is

---

24 n. 19.

25 Digital Gipfel, "Optical fiber expansion and 5G: Correlations and Synergies", June 2017, at http://www-file.huawei.com/-/media/CORPORATE/PDF/white%20paper/white_paper_fiber_5g_digital-summit_en.pdf, p. 5.

26 "Deep deployment of fiber optics is a national imperative", Deloitte, July 2017, at https://www2.deloitte.com/us/en/pages/consulting/articles/communications-infrastructure-upgrade-deep-fiber-imperative.html, accessed May 20, 2019.

27 "Digital China adds data, kilometers of high-speed cables", *China Daily*, April 20, 2018, at http://www.chinadaily.com.cn/a/201804/20/WS5ad922f2a3105cdcf6519642.html, accessed May 20, 2019.

28 Rajesh Kurup, "OFC of 1,55,000 km laid under BharatNet project", *Business Line*, January 12, 2018, at https://www.thehindubusinessline.com/info-tech/ofc-of-155000-km-laid-under-bharatnet-project/article9514537.ece, accessed May 20, 2019.

to increase the network to 2.5 million km by 2022.[29] Similar efforts are underway across the globe to prepare the underlying infrastructure for the early and swift roll-out of 5G services as soon as the standardization process is over. Access to harmonized spectrum, robust infrastructure, and standardized technology is essential to develop a competitive and efficient global 5G ecosystem.

The Standardization of 5G Technology

One of the prime reasons for the unparalleled success of the telecommunications industry, in terms of global reach, scale, and integration with global research and technology development supply chains, has been the persistent focus on Standardization. Standards are essential for the wide adoption of new technologies in global markets.[30] Information and Communication Technologies (ICT) have global significance and relevance for every nation and, therefore, global standards are fundamental to building ubiquitous connectivity. In telecommunications, standards are vital for interconnection and interoperability when the technology developers, integrators, and service providers are scattered all across the globe —in a truly multi-vendor, multi-network, and multi-service environment. Standards also ensure safety, reliability, and quality, and therefore allow suppliers to benefit from the economies of scale in the open global market.[31]

Standardization wholly depends on the concerted efforts of all the stakeholders, be it the global regulatory bodies, standardization bodies,

---

[29] Bhuma Shrivastava, "India to roll out 5G by 2022, increase fiber backbone to 2.5 mn kilometers", *Business Standard*, August 07, 2018, at https://www.business-standard.com/article/technology/india-to-roll-out-5g-by-2022-increase-fiber-backbone-to-2-5-mn-kilometers-118080700356_1.html, accessed May 20, 2019.

[30] "Standards and Patents", World Intellectual Property Organization, at https://www.wipo.int/patent-law/en/developments/standards.html, accessed May 25, 2019.

[31] "Why Standards", European Telecommunications Standards Institute, at https://www.etsi.org/standards/why-standards, accessed May 25, 2019.

industry associations, equipment manufacturers, or the mobile services providers. The process itself is complex and highly innovative, drawing on contributions in pioneering research and early collaborations between academia and other industries.[32] Technology developers or the equipment manufacturers conduct trials with the service providers, and their findings contribute to the standardization process thereof. Many communications equipment manufacturers, chip makers, and communications carriers or service providers from across the globe have pushed forward the very process of determining 5G standards. The wireless technologies and the intellectual property in the form of patents they have developed are the result of long-term persistent research and development, which ultimately benefits the vision of 5G. The whole endeavour of standardization is spearheaded by three primary bodies: the International Telecommunication Union (ITU), the 3rd Generation Partnership Project (3GPP), and the Internet Engineering Task Force (IETF).

ITU: The Geneva-based United Nations specialized agency for ICTs focuses on international connectivity in communication networks. It allocates global radio spectrum and satellite orbits, develops the technical standards, and works incessantly to improve worldwide access to ICTs. ITU's contribution to the development and adoption of standards in telecommunications has been seminal. The role of ITU in building the 5G ecosystem has already been discussed in this chapter, and includes the setting up of the vision for 5G, identifying spectrum bands, refining the criteria for 5G radio interface technologies, or conducting numerous preliminary studies culminating in the standards necessary to meet 5G's performance targets.

3GPP: The 3rd Generation Partnership Project is comprised of seven telecommunications standard development organizations (ARIB[33],

---

[32] "5G standardization", Ericsson, at https://www.ericsson.com/en/future-technologies/standardization/5g-standardization, accessed May 25, 2019.

[33] Association of Radio Industries and Business (ARIB) – Japan, at https://www.arib.or.jp/english/.

ATIS[34], CCSA[35], ETSI[36], TSDSI[37], TTA[38], and TTC[39]). They are known as "Organizational Partners", and provide their member companies with a stable environment to produce the reports and specifications that define 3GPP technologies.[40] The 3GPP provides complete system specifications for network technologies, including radio access, the core transport network, and service capabilities. The member companies contribute to the specifications and studies through Working Groups under three Technical Specification Groups (TSG): Radio Access Networks, Services & Systems Aspects, and Core Network & Terminals. With more than 370 members from leading telecommunication providers (for example, AT&T, China Mobile, SK Telecom), technology companies (for example, Intel, Qualcomm, Samsung, Ericsson, Huawei, ZTE), and government agencies, 3GPP builds consensus on technical specifications for mobile communications through an open and contribution-driven process. The contributions undergo iterations before they take the shape of technical specifications, which ultimately are transposed into Standards.

IETF: The Internet Engineering Task Force is the premier Internet Standards body. It is a large, open international community of network designers, operators, vendors, and researchers working towards the evolution of the Internet architecture and the smooth operations of

---

34 Alliance for Telecommunications Industry Solutions (ATIS) – U.S., at https://www.atis.org/.

35 China Communications Standards Association (CCSA) – China, at http://www.ccsa.org.cn/english/.

36 European Telecommunications Standards Institute (ETSI) – European Union, at https://www.etsi.org/.

37 Telecommunications Standards Development Society (TSDSI) – India, at https://tsdsi.in/.

38 Telecommunications Technology Association (TTA) – Korea, at https://www.tta.or.kr/English/.

39 Telecommunication Technology Committee (TTC) – Japan, at https://www.ttc.or.jp/e.

40 3GPP, "About 3GPP", at https://www.3gpp.org/about-3gpp/about-3gpp, accessed May 25, 2019.

the Internet.[41] IETF is working with 3GPP on specifications for virtualization functions, traffic engineering, abstractions, and network management, which have impact on key 5G technology differentiators, such as Network Function Virtualization and low latency communication. IETF's routing-related work on service chaining, source routing, distributed networking, segment routing, path computation etc. is vital for traffic management in 5G networks.[42]

The technology in the telecommunications sector is fast paced, and every decade witnesses a new generation of mobile Standards, all the way from 2G in the 1990s, through 3G in 2000s, to 4G in 2009. In early 2012, the ITU embarked on a programme to develop "IMT for 2020 and beyond", setting the stage for 5G research activities and establishing the high-level requirements and vision for 5G. In September 2015, at the World Radiocommunication Conference, the ITU's vision for 5G was finalized, and it established the key requirements that 5G had to meet under three prime usage scenarios or service categories: enhanced Mobile BroadBand (eMBB), ultra-Reliable and Low Latency Communications (uRLLC), and massive Machine Type Communications (mMTC). The 2017 ITU report titled Minimum Requirements Related to Technical Performance for IMT-2020 Radio Interface(s), laid down the following technical performance indicators for 5G use cases[43].

---

41 "About", Internet Engineering Task Force, at https://www.ietf.org/about/, accessed May 25, 2019.

42 Jari Arkko and Jeff Tantsura, "5G and Internet Technology", *Internet Engineering Task Force*, June 16, 2017, at https://www.ietf.org/blog/5g-and-internet-technology/, accessed May 25, 2019.

43 "Minimum requirements related to technical performance for IMT-2020 radio interface(s)", International Telecommunication Union, ITU-R M.2410-0, November 2017, at https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2410-2017-PDF-E.pdf, pp. 2-9.

Table 2.2: Technical Performance Indicators for 5G Use Cases

Parameter	Requirement	Purpose of evaluation
Peak Data Rate[44]	Downlink: 20 Gbit/s Uplink: 10 Gbit/s	eMBB usage scenario
Peak Spectral Efficiency[45]	Downlink: 30 bit/s/Hz Uplink: 15 bit/s/Hz	eMBB usage scenario
User Plane Latency[46] (a single user, for small IP packets)	4 ms for eMBB 1 ms for URLLC	eMBB and URLLC usage scenarios
Control Plane Latency[47] (Device To Core)	20 ms	eMBB and URLLC usage scenarios
Connection Density[48]	1 million devices per km^2	mMTC usage scenario
Energy Efficiency[49]	>90 percent improvement over LTE	eMBB usage scenario
Mobility[50]	0 to 500 km/h (covering stationary, pedestrian, vehicular and high speed vehicular classes)	eMBB usage scenario
Mobility Interruption Time[51]	0 ms	eMBB and URLLC usage scenarios

Source: ITU, www.itu.int

---

[44] Peak data rate is the maximum achievable data rate under ideal conditions (in bit/s), defined for a single mobile station.

[45] Peak spectral efficiency is the maximum data rate under ideal conditions normalised by channel bandwidth (in bit/s/Hz).

[46] User plane latency is the contribution of the radio network to the time from when the source sends a packet to when the destination receives it (in milliseconds).

[47] Control plane latency refers to the transition time from a most "battery efficient" state (e.g. idle state) to the start of continuous data transfer (for example, Active state).

[48] Connection density is the total number of devices fulfilling a specific quality of service (QoS) per unit area (per km^2).

[49] Network energy efficiency is the capability to minimize the radio access network energy consumption in relation to the traffic capacity provided.

[50] Mobility is the maximum mobile station speed at which a defined QoS can be achieved (in km/h).

[51] Mobility interruption time is the shortest time duration supported by the system during which a user terminal cannot exchange user plane packets with any base station during transitions.

In 2016, 3GPP began its work on 5G Standards for a new radio access technology — 5G New Radio (5G NR) — and a next-generation network architecture — 5G NextGen. By mid-2017, the 3GPP Technical Specifications Groups agreed on a detailed work plan for Release 15 — the first release of 5G specifications for enhanced mobile broadband, ultra-reliability and low latency, frequency ranges, and radio design. The development of 5G Standard is a two pronged approach. The first is to improve the existing 4G LTE technology in terms of network capacity and performance. The second one follows a completely new design for network structures and wireless technologies, which will pave the way for the next generation mobile communication network — the 5G NR. The deployment of 5G NR will require massive infrastructure upgrade and a large numbers of new cell sites for small cell deployment. Small cells, together with the advent of mobile-edge computing, cloud-based technologies, new spectrum, etc. also make security a formidable challenge for technology underpinning 5G deployment.

Security in 5G

Telecommunication services are now widely recognized as a critical infrastructure, whose protection is largely a national security concern. Seamless functioning of all the critical infrastructure sectors is essential for the economic and social well-being of modern nation states. Governments, businesses, armed forces, and even individuals, are dependent alike on the telecommunications sector for their need to share data or information. The technology and services provided by the telecommunications sector also form the backbone for various other industries, some of whom are part of the critical infrastructure. Exploitation of vulnerabilities in network devices and the Distributed Denial of Service (DDoS) attacks can degrade the performance of the telecommunication networks, or even disrupt services. Vulnerabilities in consumer devices, in their operating systems or in the applications, along with the sensitivity of information collected by mobile service providers have drawn attention to the aspects of privacy and data protection. Until 5G, telecommunication networks were catering to the communication needs of human beings.

The implementation of 5G will unveil whole new set of machine-to-machine communications for cases like autonomous vehicles, industrial

IoT, or robotics. In the medium to long term, 5G networks will be a critical infrastructure, also supporting industrial automation, robotic surgeries in healthcare, autonomous vehicles in the transportation segment, in addition to the legacy functions of telecommunication networks. Over and above, 5G architecture has dissolved the boundaries between hardware and software, between the RAN and the 'core' network, and also between switching and transport layers. There is also a shift in computing power from the core to the edge of the network in order to reduce user plane latency. These architectural changes necessitate higher standards of network security for 5G, their strict implementation by the manufacturers, and the methodical configuration and management by the service providers.

The onset of 5G as the next generation of mobile standards has also renewed apprehensions relating to backdoors in the telecommunication infrastructure, the role of foreign technology providers, and surveillance by foreign governments. This is largely analysed and assessed under the purview of national security. The risk to telecommunication infrastructure primarily originates from the possibilities of backdoors in either the core network, or RAN at strategic locations or high value establishments which could be used by the adversary for interception or exfiltration of data, or to disrupt infrastructure in times of conflict through radio jamming or redirecting traffic.[52] Given the complexity of the design, development, and deployment of underlying technology, and the vast expanse of platforms and vendors involved, it is extremely hard to detect malicious code, or backdoors, or even to ensure the sanctity of supply chains. Major threats include data theft, data interception, unauthorized data modification, malware, and Denial of Service attacks against the network infrastructure.

---

[52] Nicolas Botton and Hosuk Lee-Makiyama, "5G and National Security: After Australia's Telecom Sector Security Review", European Centre for International Political Economy, No. 8, 2018, at https://ecipe.org/wp-content/uploads/2018/10/TSSR-final.pdf, p. 4.

5G Security Objectives

Security for 5G aims to build technology and procedures for network access, the network thereof, and the domains encompassing the user and the applications.[53] The broader objectives of these security features are:

- Authentication and Key Agreement, and Identity Management to prevent any unauthorised access to the network, or to the communication between a subscriber and a serving network, including both signalling messages and user plane data. The 5G authentication and key agreement (5G AKA) protocol and the extensible authentication protocol (EAP) framework provide the much needed flexibility in authentication protocols and credential types for subscribers and connected devices.[54]
- The confidentiality and integrity of the communication channel between the user interface and the radio access network. Confidentiality also extends to user identity, location, user data and signalling data (signalling in both the access network and the core network).
- Privacy protection of the user as sensitive data (user and signalling) traverses over mobile networks. Since mobile operators collect, store, and process personal data, privacy protection also extends to regulatory compliance with the emerging rules and regulations, such as the *General Data Protection Regulation* of the European Union.
- Secure industrial operations for the safety and security of critical infrastructure control systems implemented, or to be implemented, in the form of IoT.

---

[53] Qiuming Liu, He Xiao, Xiaohong Qiu, Li Yu, "Impact of Social Interaction on the Capacity of Hybrid Wireless Networks", *Access IEEE*, Vol. 6 , pp. 46683-46694, 2018.

[54] Ericsson, "5G security — enabling a trustworthy 5G system", March 28, 2018, at https://www.ericsson.com/en/white-papers/5g-security—enabling-a-trustworthy-5g-system, accessed September 12, 2019.

- The availability of the services by balancing the requirements of network performance with key security considerations, and the early detection and mitigation of DDoS attacks.
- Trusted supply chains for the radio equipment, integrated circuits, core networking equipment, and the end user equipment,[55] which will be sourced from various suppliers or vendors. This may include the strengthening of the existing tools, such as trusted third party certification schemes for security evaluation of the software, firmware, and hardware. This will also help in identifying potentially non-secure products and suppliers, so that they could be kept out of sensitive functions, or even from the core networks.[56]

Why is 5G different?

A typical telecommunication network has four logical segments: radio access network, core network, transport network, and interconnect network. Each of these segments comprises three planes: the control plane carries signalling traffic; the user plane carries actual traffic such as voice and data; and the management plane carries the administrative traffic. The three planes have different security risks. Signalling traffic could be tempered with to re-route calls, interception, eavesdropping, or for denial of service. Likewise, the management plane could be used to disrupt network traffic.[57] Besides the susceptibility of 5G networks to air interface attacks — such as Man in the Middle attack, Jamming, Rogue Nodes — security risks arise out of API

---

[55] Laura A. Odell et al., "Implications and Considerations of 5th Generation Mobile Networks (5G) for the US Department of Defense", Institute for Defense Analyses, April 2019, at https://www.ida.org/-/media/3aa2167e34314398972eb3f18402b84e.ashx, p. 7.

[56] Lorenzo Pupillo, "5G and National Security", Centre for European Policy Studies, June 21, 2019, at https://www.ceps.eu/5g-and-national-security/, accessed September 12, 2019.

[57] "A guide to 5G network security", Ericsson, at https://www.ericsson.com/en/security/a-guide-to-5g-network-security, accessed September 12, 2019.

vulnerabilities, IoT Core integration, App server vulnerabilities, to name a few.[58]

Compared to the previous generations of mobile standards, the challenges for the security of the network and the privacy of the users in 5G are different. 5G use cases in industries, homes, healthcare, and automobiles, etc., have diverse requirements for performance and, therefore, their security levels vary too. An IoT network slice in a 5G deployment will have different attributes of security algorithms, key negotiation, and security, as compared to a mobile broadband slice. Availability and integrity would prevail in the case of IoT, especially for mission critical applications, while confidentiality would be a priority for the mobile broadband slice. The security of IoT itself is one of the key concerns, whose numbers with the introduction of 5G are slated to rise.

Virtualization is the cornerstone of 5G deployment. This also means that there will be an increase in the number of players — the vendors supplying different segments of hardware and software, virtual infrastructure providers, virtual network service operators, and virtual application vendors. Small cell deployment and the use of mobile-edge computing for enabling 5G services means that a lot of security features which were restricted to the core, will spread all across the network, thus broadening and widening the scope of security standards. New technologies in the 5G RAN such as massive MIMO, mmWave, and device to device communications have brought new challenges to network access security. Owing to these, and a multitude of other factors, 5G networking technologies are being designed to be more secure than the previous generations of mobile standards. 3GPP is defining 5G standards to secure the core network, radio and user equipment, with a strong emphasis on privacy and identity management.

---

[58] Michael Geller and Pramod Nair, "5G Security Innovation with Cisco", Cisco Whitepaper, 2018, at https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/service-provider-security-solutions/5g-security-innovation-with-cisco-wp.pdf, p. 14.

5G in Security/Military

Along with advancement in mobile technology, 5G is also a significant development in communications technology — both for the civilian as well as the military domain. The advent of technology for harnessing new spectrum can pave the way for some very specific yet important needs of military communications. Due to inherent characteristics, communication in the extremely high frequency (mmWave, for instance) band has Low-Probability-of-Interception (LPI), Low-Probability-of-Detection (LPD), and Low-Probability-of-Jamming (LPJ).[59] These characteristics make it suitable for deployment in some distinct topographies or forward areas. High bandwidth and extremely low latency can enable high-speed data sharing in different formations of the armed forces, which could be in the form of imagery, videos, maps, or simulations for enhanced situational awareness.

With the growing use of unmanned aerial and ground vehicles in military operations, 5G networks can enable the transmission of high-definition (4K video) content in the real-time to mobile units and static command centres simultaneously. Melded with Virtual Reality/Augmented Reality, high-definition content from reconnaissance missions or geospatial data can be shared across the chain of command for meticulous operational planning, or to get the soldiers acquainted with the topography or surroundings of the battlefield they are entering in. As armed forces across the world are on the verge of embracing Artificial Intelligence, 5G networks can truly underpin their need for ultra-fast data transmission.

5G can connect cameras and sensors without the need of laying down cables. This could be leveraged in perimeter security, drastically cutting down deployment time and quite useful for temporary military installations. Beyond transforming the battlefield for network centric warfare, 5G can also find path breaking applications in monitoring the

---

[59] "Defense Applications of 5G Network Technology", US Department of Defense, Defense Science Board Task Force, June 2019, at https://www.acq.osd.mil/dsb/reports/2010s/5G_Executive_Summary_2019.pdf, p. 6.

health and body parameters of soldiers. With the real-time monitoring of heart-rate, blood pressure, and other vital parameters, 5G connected wearable devices can also help geo-locating soldiers who need immediate medical attention. Robotic surgeries — one of the most discussed applications of 5G — could be live-saver at field hospitals and forward deployment positions where the availability of doctors and surgeons with the right expertise is limited. Standards are just going to lay down the technical specifications of 5G technology, but the true potential and extent of its applications is still unknown. Pilot projects and 5G technology demonstrations are a precursor to the unfolding future of a hyper connected world.

3GPP released 'Non-Stand-Alone' (NSA) NR new radio specifications for 5G by the end of 2017, which is pivotal to large-scale trials and early deployments of standardized commercial 5G networks. Release 15 — the first full set of 5G standards towards IMT-2020 — will form the first phase of 5G deployments. The first full-scale commercial deployments for 5G are expected shortly, after IMT-2020 specifications are finalized in early 2020. Regulators across the world are already auctioning licenses to operate 5G networks in the frequency bands identified for IMT-2020.[60] Governmental bodies, ministries, and operators have announced 5G test-beds and deployment target dates, as countries want to position themselves at the forefront of 5G adoption. Pilot projects, such as the 2018 PyeongChang Winter Olympics, are being developed to showcase 5G technology. These deployments, however, are not 5G implementations in the real sense, as they have come up ahead of finalized 5G specifications, and they probably may not meet the specifications.

A race to be the first one to demonstrate a 5G network is already on among leading companies, and the same has triggered competition between governments to facilitate and enable early deployment. All put together, the race is about patenting the underlying technology, allocating spectrum for trials and roll out at the earliest, influencing the

---

[60] n. 1.

international standard-setting platforms, and to provision the enabling infrastructure by the time IMT-2020 requirements are finalised at the ITU. Apart from the science and technology, the case of 5G is different from the previous generations of mobile standards. None of the previous generations attracted such media and public attention. 5G has been in the news as Chinese companies associated with the development of technology for 5G were caught in the storm of the trade war between the USA and China. Another reason is the rise of China as a leader in 5G technologies, who was an adopter earlier with a negligible contribution at the international standard-setting platforms. The next chapter examines this rise of China, and presents a brief account of the manufacturing of telecommunication equipment in China, analyses China's ascent to the standard-setting platforms, and delves into the curious case of Huawei.

Chapter 3

Tracing China's Journey to 5G

China is the world's largest user base for telecommunications, and the equipment it produces rivals that from developed economies. Chinese telecom equipment manufacturers and their products have been subject to intense scrutiny in a few countries on security grounds. Their ties with the government and the military have been the primary source of concern. In addition to these, a provision (Article 7) in the 2017 National Intelligence Law requiring organizations to "support, assist and cooperate with the state intelligence work" adds to these apprehensions. With 5G implementation on the horizon, the security debates have again picked up pace, amidst the ongoing US-China trade war. The telecommunications sector in China has evolved from underdevelopment to such a stage where Chinese vendors can directly compete with their Western counterparts, and make significant contributions to the standards development process.

It is worthwhile to look at the evolution of telecommunications equipment manufacturing in the People's Republic of China — from absolute dependence on foreign technology to import substitution with local manufacturing, and then to a global exporter. By and large, it has been driven by investments from government or state-owned enterprises, and the quest for innovation in private-owned enterprises, which were strongly backed by a conducive industrial policy led by specialised ministries.

Backgrounder

The first effort to build telecommunication infrastructure in China dates back to 1877, which was a telegraph line in Taiwan,[1] during the rule of

---

[1] Eric Harwit, "China's Telecommunications Industry: Development Patterns and Policies", *Pacific Affairs*, Vol. 71, No. 2, 1998, pp. 175–193.

the Qing dynasty. The Qing government had created the Ministry of Posts and Communications to supervise telegraphs, posts, and railways in 1906.[2] After centuries of dynast rule and decades of civil war, the People's Republic of China came into existence in 1949. By then, telephone density in China was a meagre 0.05, supported by just 300,000 telephone lines.[3] The newly formed government raised a Ministry of Posts and Telecommunication (MPT) in November 1949, which had the dual responsibilities of a regulator and an operator of telecommunication services,[4] through its operational arm, China Telecom. MPT oversaw the civilian telephone network and communications, and it had complete monopoly in the telecommunications sector.

Initially, the sector was completely dependent on government investments. Although, private players and foreign vendors were allowed to supply telecommunication equipment later; but they were debarred from providing telecom services. Foreign direct investment was also banned in telecom services and network operations.[5] From 1949 till about 1977, when the economic reforms began, telecommunications as a sector developed slowly — probably because its role in the national economy was not recognized correctly.[6] This phase of China's industrial development was also military driven. High technology sectors, such as electronics and aerospace, relied completely on military investment

---

2 John Bowman and John Stewart Bowman, *Columbia Chronologies of Asian History and Culture*, New York: Columbia University Press, 2000, p. 58.

3 Liang Xiongjian, Zhang Xueyuan, and Yang Xu, "The Development of Telecommunications in China", *IEEE Communications Magazine*, November 1998, pp. 54-58, at https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=733474.

4 "Annual Report 1998", China Telecom Limited, at https://www.chinamobileltd.com/en/ir/reports/ar1998/1998a13_en.pdf, p. 73.

5 n. 3, p. 55.

6 Liang Xiongjian and Zhang Jing, "Development and Regulatory System Reform of the Telecommunications Industry in China", *Global Communications Newsletter*, at http://www.comsoc.org/pubs/gcn/gcnll03.html, accessed June 05, 2019.

and the expertise residing in military research institutions.[7] Telecommunications attracted the attention of the government at the very beginning of the economic reforms, and the sector was often mentioned as closely linked to China's economic growth.[8] In 1979, Deng Xiaoping noted that telecommunications, along with energy and transportation, needed public investment as they were the foundation for infrastructure construction.[9] The report of the 12th National Congress of the Communist Party of China (1982) underscored the need for expanding postal and telecommunications services to ensure a fair rate of growth in the national economy.[10]

Akin to the situation in other parts of the world, urban areas in China witnessed faster growth of telecommunication networks, owing to increase in demand for both personal and business communications. Since the beginning, specialized ministries have overseen the expansion of the telecommunications sector, under heavy regulation. Along with the import of foreign networking equipment, the government continued to invest in and support domestic manufacturing, which ultimately reduced dependence on imports, and met the surging demand for equipment at lower costs. Following the admission of the People's Republic of China to the UN in 1971, the ITU also resumed its representation in the Union in 1972.[11]

---

7 Evan A. Feigenbaum, *China's Techno-warriors*, Stanford: Stanford University Press, 2003, p. 2.

8 n. 1, p. 183.

9 Yun Wen, "The Rise of Chinese Transnational ICT Corporations: The Case of Huawei", Dissertation Submitted in Partial Fulfilment of the Requirements for the Degree of Doctor of Philosophy in the School of Communication Faculty of Communication, Art and Technology, Simon Fraser University, 2017, p. 57.

10 Hu Yaobang, "Report to the 12th National Congress of the Communist Party of China", September 12, 1982, at http://www.bjreview.com.cn/90th/2011-04/12/content_357550_9.htm, accessed May 30, 2019.

11 "1970-1979 Telecommunication Development Events", China Telecom, at http://www.chinatelecom.com.cn/news/06/hh60n/60nlsjc/t20090911_53999.html, accessed May 30, 2019.

The manufacturing of telecommunications equipment actually began under the Chinese Ministry of Machine Building in 1957, with Russian assistance. It began with the production of automated telephone switches.[12] After building a production base in Shanghai during the1950s–1960s, China had around 27 equipment manufacturing facilities under the MPT by 1970, and another 100 were functioning under provincial telecom bureaus.[13] As a part of the reforms in the telecommunications sector, and its opening up for free market planning and to attract foreign investors, the MPT created the China Posts and Telecommunications Industry Corporation (PTIC) in 1980, absorbing the production capacity of 27 factories. This decision paved the way for foreign investment, innovation, research, competition, and fostering close relations with foreign telecommunications technology providers. The decade of the 1980s witnessed structural changes in China's telecommunications policy, both related to equipment and services, which made the state-owned enterprises independent in the planning and marketing of products, R&D, and even profit retention.

In 1982, the then MPT Minister, Wen Minsheng, announced that the telecommunication system would be a priority for developing China's economy.[14] In 1984, Vice Premier Li Peng took control of the Leading Group for the Revitalization of the Electronics Industry, which identified telecommunications as one of the priority areas, in addition to integrated circuits, computers, and software.[15] This phase saw an increase in

---

[12] Eric Harwit, "Building China's Telecommunications Network: Industrial Policy and the Role of Chinese State-Owned, Foreign and Private Domestic Enterprises." *The China Quarterly*, No. 190, 2007, pp. 311–332.

[13] Ibid.

[14] "China accelerates development of telecommunications", *Xinhua General Overseas News Service*, February 22, 1982 [Appeared in Eric Harwit, "Building China's Telecommunications Network: Industrial Policy and the Role of Chinese State-Owned, Foreign and Private Domestic Enterprises." *The China Quarterly*, No. 190, 2007, pp. 311–332]

[15] Milton Mueller amd Zixiang Tan, *China in the Information Age: Telecommunications and the Dilemmas of Reform*, Center for Strategic and International Studies, Westport: Praeger Publishers, 1997, p. 56.

telecommunication equipment imports, including digital switching and transmission systems,[16] which was an advanced technology at the time. The preferential treatment also included a waiver of 90 per cent of central government loans extended to telecommunication enterprises.

In a bid to attract foreign capital and gain access to modern technology, the government reduced tariffs on telecommunication equipment imports in the year 1986, which lasted for a decade, until 1996. This phase also witnessed a rise in generous foreign loans for equipment procurement, although Chinese operators were required to buy products from the vendors of the countries issuing credit for procurement.[17] Canada, for instance, extended a 20 year soft loan to China in 1988 which assisted Nortel's exports to China.[18] This also led to a decline in domestic production, and an influx of foreign players: Japan's NEC and Fujitsu, Lucent from the USA, Canada's Nortel, Sweden's Ericsson, Germany's Siemens, BTM from Belgium, and France's Alcatel — then termed as "seven countries and eight systems", drawing parallels with the Eight-Nation Alliance, the international military coalition set up in 1900 in response to the Boxer Rebellion during Qing rule.

Simultaneously, China took the joint ventures route to spur domestic production of the equipment, with the caveat that the Chinese side holds majority ownership. The first such joint venture was Shanghai Bell; it was between PTIC and the Belgian subsidiary of ITT

---

[16] "Posts and telecommunications in China", *Xinhua General Overseas News Service*, August 20, 1984 [Appeared in Eric Harwit, "Building China's Telecommunications Network: Industrial Policy and the Role of Chinese State-Owned, Foreign and Private Domestic Enterprises." *The China Quarterly*, No. 190, 2007, pp. 311–332].

[17] Yu Hong, Francois Bar and Zheng An, "Chinese telecommunications on the threshold of convergence: Contexts, possibilities, and limitations of forging a domestic demand-based growth model", *Telecommunications Policy*, No. 36, 2012, pp. 914–928.

[18] "The story of the rise of 200 million households: the history of Chinese switches", *Sina*, September 11, 2002, at http://tech.sina.com.cn/it/t/2002-09-11/1020137952.shtml, accessed June 10, 2019. [Translated using Google Translator]

Corporation, in 1983. Shanghai Bell began production in 1985. Germany's Siemens AG also entered into a joint venture with the Ministry of Electronics Industry for a stake in the Beijing International Switching Company, by 1985. Joint ventures essentially served two strategic purposes: to reduce the reliance on imports at the one end, and built domestic capacity to mass manufacture low-cost components for telecommunication equipment with the absorbed technology at the other end. Towards the mid-1990s, domestic manufacturing picked up market share and began reducing the need for imports. The preferential import policies also came to an end by 1996, and the subsequent import-substitution policy significantly benefited indigenous equipment manufacturers. The joint-ventures, many in number by then, actually served the interests of both the foreign and the domestic partners. The foreign partners got access to low-cost equipment production facilities, and the Chinese government saved foreign exchange on account of reduced imports.

In 1994, the Directorate General of Telecommunications was separated from the MPT to be the national system operator (later known as China Telecom), leaving MPT with regulatory powers. The monopoly of the MPT as a carrier also came to an end in 1994 when a consortium, led by the Ministry of Electronics Industry, the Ministry of Railways, and the Ministry of Electric Power, formed China Unicom as the second carrier.[19] This was also the beginning of an open and competitive market ahead. As the world was ushered into the era of digital and mobile communications in the 1990s, the defining phase of reforms in China's telecommunications sector also came to an end, in March 1998, following the merger of the MPT with the Ministry of Electronics Industry, and the network management functions of the Ministry of Radio, Film and Television to form the Ministry of Information Industry (MII).[20]

---

[19] James Mulvenon and Thomas J. Bickford, "The PLA and the Telecommunications Industry in China", in James C. Mulvenon and Richard H. Yang (eds.), *The People's Liberation Army in the Information Age*, RAND Corporation, CF-145-CAPP/AF, 1999, at https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF145/CF145.chap12.pdf.

[20] Ibid., p. 247.

China acceded to the World Trade Organization in December 2001 and, as part of the negotiations, it agreed to open up the telecommunications sector (equipment and services) for foreign investment. Prior to China's accession to the WTO, protectionist policies were in place to favour the telecommunication services and domestic industry. Only foreign equipment manufacturers were allowed to invest in China, under strict controls of ownership and conditions on technology transfer. As a member of the Basic Telecommunications Agreement, China had to ensure fair competition and the interconnection of carriers. Also, it had to allow up to 49 per cent ownership by foreign investors in the basic telecommunications services in the first two years after accession, to be increased to 50 per cent at the end of two years.[21] In accordance with the Information Technology Agreement, China had a commitment to eliminate import duties on high technology products, including computers, semiconductors, software, and telecommunication equipment.[22] Now, China had to implement an impartial and pro-competitive regulatory policy in the telecommunications sector, which also meant that China had to end preferential treatment to domestic enterprises. As a result, advanced mobile communications technology from foreign vendors made an influx into the Chinese telecommunications market. However, China's integration with the world also opened the doors for Chinese companies to go global, with their products as well as to harness talent available in different parts of the world.

China has selectively used foreign technology and private sector expertise in telecommunications to its advantage. It has comfortably kept both at bay from operating telecommunication networks, while foreign vendors and domestic manufacturers have been restricted to equipment

---

[21] James Shen, "The impact of China's entry into the WTO on the Chinese telecommunications industry", *Cambridge Review of International Affairs*, Vol. 13, No. 2, pp. 121-135, at https://www.tandfonline.com/doi/pdf/10.1080/09557570008400304.

[22] "Information Technology Agreement — an explanation", World Trade Organization, at https://www.wto.org/english/tratop_e/inftec_e/itaintro_e.htm, accessed June 08, 2019.

supplies and technology integration. Chinese private sector companies, though with the support of the government, have gone global, carving a market share in both developing and developed economies. Their rising influence in defining telecommunication standards also reflects their technical prowess, the foundations of which were laid down in the mid 1990s. Chinese telecommunication equipment manufacturers have also succeeded in shedding their identity as low-end component suppliers or Original Equipment Manufacturers, through sustained investment in world-class R&D facilities and human resources, spread all across the globe. Their rise has, of course, remained controversial, with apprehensions over their links to the government or military, security risks from their equipment, and allegations of Intellectual Property infringements.

China's Rapid Ascent in Standardization Bodies

As discussed briefly earlier, high technology R&D and industrialization in China had a heavy influence of the military in the pre-reform era. Even during the reforms, the People's Liberation Army (PLA) continued to invest resources in the telecommunications sector. In a first of its kind in China, the Zhengzhou Institute of Information Engineering of the PLA and the PTIC jointly developed an indigenous 30,000 line digital program-controlled switch, the HJD-04, in the year 1991,[23] under the auspices of the Great Dragon Group which had begun research in 1989. This breakthrough opened the floodgates for indigenous R&D and innovation in China. The Great Dragon Information Technology (GDT) was subsequently founded in 1994 as a state-owned enterprise to commercialise HJD-04 switch. Huawei also started the development of digital switches in 1992, and success came in the form of C&C08 in 1994. The Datang Telecom Technology Co. Ltd. (DTT) was founded in 1998 by the China Academy of Telecommunications Technology (CATT), which went on to play a leading role in the development of China's 3G mobile communication standard. The Ministry of Aerospace Industry founded Zhongxing Semiconductor

---

[23] Xiaobai Shen, "HJD-04: The Chinese-Developed System", *The Chinese Road to High Technology*, London: Palgrave Macmillan, 1999.

Co. Ltd. in 1985, which was later renamed Zhongxin Technology Corporation (ZTE) in 1993. As state-owned enterprises, GDT, DTT, and ZTE received ample financial assistance from the government, even for Research and Development. With the onset of domestic technology suppliers and the end of preferential import policies by 1996, the MII thereafter encouraged Chinese telecommunication network operators to purchase equipment from home-grown manufactures. GDT, DTT, ZTE, and Huawei have been the face of China's rise as a global telecommunication equipment manufacturer. However, Huawei and ZTE clearly stand out in the present time.

Beginning with fixed line telephone technology, Chinese companies remained a follower in GSM technology (2G), but kept pace with the global developments in the 3G era. ZTE established a research and development institute in Shanghai for wireless and access products in 1994.[24] Huawei's research and development endeavour for GSM and CDMA began in 1995, and it was able to develop wireless GSM-based solutions and WCDMA products independently by 1997–1998, with a team of more than 500 scientists, researchers, and engineers. Amongst the Chinese companies, Huawei has always stood apart for its investments in R&D — both independent and joint. As early as 2002, it was investing 18.8 per cent of its revenue in R&D — higher than any other domestic company or foreign companies in China.[25]

Europe has contributed significantly to Huawei's R&D endeavour, beginning with a center in Sweden in 2000. From 1998 to 2002, it invested heavily in the WCDMA (around RMB 3 billion), and increased staff at R&D centres across China, USA, Sweden, and India to 3500.[26]

---

[24] Huang Guo, "20 Years History of ZTE Corporation", ZTE Corporation, at https://www.zte.com.cn/global/about/magazine/zte-communications/2005/2/en_49/162340, accessed June 08 2019.

[25] Peilei Fan, "Catching up through developing innovation capability: evidence from China's telecom-equipment industry", *Technovation*, No. 26, 2006, pp. 359–368.

[26] Ibid., p. 364, and Xudong Gao, "A latecomer's strategy to promote a technology standard: The case of Datang and TD-SCDMA", *Research Policy*, No. 43, 2014, pp. 597–607.

At present, Huawei has 18 R&D facilities across eight European countries, managed through its European Research Institute at Brussels, set up in 2015.[27] The same year, it partnered with the University of Surrey (UK) and other leading technology companies and mobile service providers to found the 5G Innovation Centre.[28] Since 1986, ZTE has built 13 R&D facilities within and outside China.[29] Chinese telecommunication equipment manufacturers have effectively leveraged global expertise in the science and technology of mobile communications. They have followed a two pronged approach: used aggressive in-house R&D, and supplemented it with external alliances with universities and leading technology developers. Joint laboratories and collaborative research with technologically advanced partners and academic institutions have gone a long way in elevating their in-house innovation capacity and technology competence.

From fixed line telephones to the analogue mobile communication system and then on to 2G (GSM), China had a long term dependency on imports for the core technology. Till the time of 2G implementation, Huawei, DTT, ZTE were all adopting technology developed by European, American, or Japanese companies, who had an early mover advantage and were also controlling the standards. The 1980s policy efforts to reduce dependence on foreign technology, and promote joint ventures, essentially meant that the foreign vendor had to transfer the technology, and the Chinese partner had to absorb the imported technology to be used for independent production. Concomitantly, local manufacturers were able to supply as much as 98 per cent of the newly inducted switching equipment for fixed local networks by 1998,

---

[27] Huawei, "Huawei Launches New European Research Institute to Gear up European Digitization Progress and Achieve Win-Win Outcomes", May 14, 2015, at https://www.huawei.com/en/press-events/news/2015/05/hw_427623, accessed June 12, 2019.

[28] "About 5G Innovation Centre", University of Surrey, at https://www.surrey.ac.uk/5gic/about, accessed June 12, 2019.

[29] "Introduction to ZTE", Embassy of the People's Republic of China in India, at http://in.chineseembassy.org/eng/jjmy/zymywl/zzgs/t112583.htm, accessed June 12, 2019.

increasing their market share to 99 per cent by 1999.[30] However, the road to long term success was indigenous research and development capability, and not production alone.

Chinese R&D efforts for standards development started in 1992 in the form of a research project titled "Digital Mobile Communications Technology (GSM)". It was sponsored by the State Planning Commission and former MPT. The China Academy of Telecommunications Technology undertook this project, and took four years to build a prototype.[31] It could not find much traction as the European standard was already prevalent. The government's flagship National High-Technology Research and Development Plan (863 Plan) also continued to build the necessary momentum, and strategic concerns about national security gave further thrust to this endeavour.

The ITU had called for technical proposals for the new mobile telecommunications standard in April 1997, under the name IMT-2000, dubbed as the 3G standard. Keeping pace with the advancing technology in 3G wireless communications system, the China Academy of Telecommunications Technology/DTT proposed (in 1998) the Time Division-Synchronous Code Division Multiple Access[32] (TD-SCDMA) as China's 3G standard to the ITU. In 1995, a technology start-up company Cwill — set up by two Chinese researchers Chen Wei and Xu Guanha — originally began working on uplink synchronous

---

30 "3G Mobile Policy: The Case of China and Hong Kong", prepared by Xu Yan of the Hong Kong University of Science and Technology as a part of a series of Telecommunication Case Studies produced under the New Initiatives programme of the Office of the Secretary General (OSG) of the International Telecommunication Union.

31 Xu Yan and Douglas C. Pitt, *Chinese Telecommunications Policy*, Artech House Publishers, 2002, p. 132.

32 TD-SCDMA derives from SCDMA, an indigenous wireless access technology, developed by Beijing Xinwei Telecom Technology Inc, a joint venture of the China Academy of Telecom Technology and Cwill in the mid-1990s; for details see, John Whalley, Weimin Zhou and Xiaopeng An, "Chinese Experience with Global 3G Standard-Setting", CESIFO Working Paper No. 2537, February 2009, at https://www.ifo.de/DocDL/cesifo1_wp2537.pdf, p. 11.

technology, which took the shape of SCDMA (Synchronous CDMA) later.[33] A joint venture between DTT/CATT and Cwill in 1995, named Beijing Xinwei Telecom Technology Inc., undertook the development of this wireless access technology.[34] Cwill, however, quit the venture later. DTT/CATT took over the research team at Xinwei, and continued the development of TD-SCDMA so that it met the technical requirements of IMT-2000. Siemens joined the effort in 1998, augmenting the standardization and development of TD-SCDMA. It was accepted as one of the 3G mobile communications standards by the ITU in 2000, alongside the Europe-Japan led Wideband CDMA[35] and the North America-South Korea led CDMA2000.[36] The technical specifications of TD-SCDMA were accepted by 3GPP in March 2001, and included in its Release 4 in 2002.

To further promote its global adoption and spur industrialization, the TD-SCDMA Technology Forum was immediately established jointly with China Mobile, China Telecom, China Unicom, DTT, Huawei, Motorola, Nortel, and Siemens, having 420 members from across the globe.[37] A TD-SCDMA Industry Alliance was also formed in 2002 for further commercialization. The Chinese government extended generous financial support of USD 85 million (about RMB 700 million)

---

[33] Qiao Nan Lu Yi Xuan, "TD-SCDMA", www.net.cn, at http://zhuanti.cww.net.cn/zhuanti/td_scdma/default.html, assessed June 15, 2019, and Hui Yan, "The 3G Standard Setting Strategy and Indigenous Innovation Policy in China: Is T-SCDMA a Flagship?", Danish Research Unit for Industrial Dynamics Working Paper No. 07-01, at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.417.6831&rep=rep1&type=pdf, p. 8.

[34] n. 32, p. 11.

[35] WCDMA was supported by the NTT DoCoMo of Japan, and Ericsson and Nokia in Europe.

[36] CDMA 2000 was supported by Qualcomm and Motorola from the USA, Nortel Networks from Canada, and Samsung from South Korea.

[37] Jing Wang, "A Brief Introduction to the TD-SCDMA Forum", *TD-SCDMA Forum*, October 2005, at https://www.3gpp.org/ftp/Op/OP_14/DOCS/PDF/OP14_10.pdf, accessed June 15, 2019.

in 2003 to domestic companies to accentuate the industrialization of TD-SCDMA.[38]

The role of the Chinese government in this endeavour has remained debatable. It has been argued that the Chinese government has had the greatest interest in the 'Chinese indigenous standard'[39], and therefore it has extended active support to the development of TD-SCDMA. Overall, the development of the sector has also been attributed to the protectionist policies of the government. When SCDMA was selected in the "9th Five-Year" research programs, CATT received RMB 15 million from the National Key Technologies R&D Program under the Ministry of Science and Technology, and an additional RMB 10 million from the State Development Planning Commission (the predecessor of the National Development and Reform Commission) for its development.[40] Once the TD-SCDMA was accepted as a 3G standard, the National Development and Reform Commission, with the Ministry of Science and Technology, and the then MII aggressively supported the TD Industry Alliance and pushed ZTE and Huawei to join the Alliance. The financial support of USD 85 million was part of this effort.

The alternative argument has been that the Chinese government never indicated that the TD-SCDMA must be adopted as a 3G standard for nationwide implementation until 2009, when the licences were issued. Also, before the founding of the TD-SCDMA Industry Alliance in 2002, there were few companies willing to invest time and resources in

---

38 Xudong Gao, "A latecomer's strategy to promote a technology standard: The case of Datang and TD-SCDMA", *Research Policy*, No. 43, 2014, pp. 597–607.

39 James Stewart, Xiaobai Shen, Chengwei Wang and Ian Graham, "From3G to 4G: standards and the development of mobile broadband in China", *Technology Analysis & Strategic Management*, Vol. 23, No. 7, 2011, pp. 773–788.

40 n. 33, and Yan Hui, "From Self-Innovation to International Standardization: A Case Study of TD-SCDMA in China", *Seoul Journal of Economics*, Vol. 26, No. 1, 2013, p. 122.

TD-SCDMA technology, except Siemens.[41] However, later on, Ericsson, Alcatel Lucent, Qualcomm, Samsung, etc. participated in the development of equipment, terminals, and chipsets for TD-SCDMA.[42] The 2008 Beijing Olympics showcased 3G services based on TD-SCDMA, and it was commercially launched in 2009.

TD-SCDMA also succeeded in overcoming the technical limitations of Time Division Duplex (TDD), whose characteristics have advantages for massive MIMO and Adaptive-Beam Antennas — the technologies key to 5G. Shortly after having the first brush with global mobile communication standards with 3G, China set on to the next generation with TD-LTE, the long-term evolution of TD-SCDMA, to provide packet based high-data-rate service with enhanced coverage, capacity, low latency, and low cost. Unlike TD-SCDMA, the TD-LTE managed to garner more support from operators and manufacturers globally. The 3GPP RAN workshop on the long term development of 3G mobile communication systems in 2004 had set the stage for 4G. In an October 2009 ITU-R meeting, China submitted the TD-LTE-Advanced as a candidate technology, based on a study and performance evaluation by CATT/DTT and other Chinese companies on mobile broadband systems. It was accepted in November 2010.[43] More of an international effort, Chinese and foreign technology companies and operators (Qualcomm, Nokia, Ericsson, Verizon, to name a few) were a part of this process alike, which was further facilitated by the Global TD-LTE Initiative (2011) founded by China Mobile, Vodafone, Softbank, Bharti Airtel, and now supported by 218 partners.[44]

---

41 n. 38, p. 601.

42 Shanzhi Chen, Jian Zhao, And Ying Peng, "The Development of TD-SCDMA 3G to TD-LTE-Advanced 4G From 1998 To 2013", *IEEE Wireless Communications*, December 2014, pp 167–176.

43 Ibid., p. 172.

44 "Who we are", GTI, at http://www.gtigroup.org/about/, accessed June 20, 2019.

The efforts finally paid off well as China grew its influence in international technology standards and policy matters. It also elevated the profits for Chinese companies as they moved up the value chain from licensed manufacturers to innovators. Standard-setting in the previous generations was centred in North America, Europe, and Japan. With the 3G standardization process, China was able to demonstrate its indigenous innovation capacity — challenging the dominance of Western countries and their allies in mobile communication standards. Extensive engagement in R&D, and then leveraging it to make significant contributions to the standardization process underscores the position of a company in fierce global technology competition. For nation states, this is intrinsic to the geopolitics of global technology development. Techno-nationalism — the explicit connection between technology accomplishment and a related position on the global order[45] — has also been a strong driving force for China.[46] Having their own 3G standard has also saved Chinese companies exorbitant fees or royalties for using patented technologies or IPR in their products. Holding IPR has also meant that Chinese companies could negotiate better terms through cross-licensing agreements with foreign IPR holders.

With an aggressive push from the industry, and facilitation by the government, the market share of domestic companies, including Huawei, ZTE and DTT, increased from under 20 per cent in the 2G era to close to 70 per cent with the implementation of 3G, displacing foreign companies in the domestic market. Amongst all the Chinese players, Huawei's sudden rise has rattled the global telecommunications market. The company has also been at the centre stage of controversies, as many questions have been raised on its ability to develop Intellectual

---

[45] n. 7, p. 37.

[46] Richard P. Suttmeier, "A new Techno-nationalism? China and the development of technical standards", *Communications of the ACM*, Vol. 48, No. 4, 2005.

Property, its alleged links with the government, and the potential use of its equipment for surveillance.

The Rise of Huawei

The private sector has been an integral part of China's telecommunication growth, initially through joint ventures with foreign entities and, later, through home-grown companies. Before Chinese telecommunication companies could match up to global standards and the demand of mobile communications, major global players, like Motorola, Alcatel (Alcatel, a French company took over BTM in 1987), Siemens, NEC, and Ericsson, had a wide presence in the Chinese telecommunications market. As early as 1995, AT&T was supplying terminals and modems, Motorola had presence in switching systems, and Siemens and Ericsson were installing base stations for mobile networks.[47] The transfer of technology to local companies had sown the seeds of China's present day telecommunications manufacturing capability. From the 1980s through the 1990s, China was producing low-end routers and switches. It was serving as an ideal manufacturing hub for foreign companies, with ease of access to the burgeoning telecommunications markets in the Asia Pacific.[48] Chinese companies at that time were export oriented, and engaged in labour-intensive production; but they were severely lacking in-house innovation or R&D expertise.

Government support to R&D and innovation initiatives in seven strategic sectors came in the form of the Chinese National High-Technology Research and Development Plan in 1986, better known as the "863 Plan". Policy support and preferential treatment by the central and provincial governments have played a vital role in the development of telecommunications manufacturing in China. The Shenzhen Municipal

---

[47] William R. Boulton, "Hong Kong-South China Electronics Industry", in Michael Kelly and William R. Boulton, *Electronics Manufacturing in the Pacific Rim*, World Technology Evaluation Center, May 1997, at http://www.wtec.org/loyola/em/03_04.htm, accessed June 20, 2019.

[48] Brian Low, "The evolution of China's telecommunications equipment market: a contextual, analytical framework", *Journal of Business & Industrial Marketing*, Vol. 20, No. 2, 2005, pp. 99–108.

Government, way back in 1986, had extended policy support for the high technology sector in accordance with the ICT development strategy of the central government. The Shenzhen government subsequently lifted controls on private ownership in the high technology sector which allowed technologists to invest in companies, start new ventures, and build intellectual property under a favourable tax regime. As a direct beneficiary of this initiative, Huawei was formed in 1987 as a private owned enterprise in Shenzhen and, by 1998, it went on to topple Shanghai Bell as the largest manufacturer of digital automatic switches in China. Hauwei was originally a sales agent for a Hong Kong based company producing Private Branch Exchange (PBX) switches. Huawei's domestic rival, ZTE, was actually founded as Zhongxing Semiconductor Co. Ltd. in 1985 — a state-owned enterprise under the Ministry of Aerospace Industry at Shenzhen. It was registered under the present name in 1993 as a "state-owned and private-run" system of operation which was totally new in China at that time.[49]

After establishing a strong foothold in the domestic market, Huawei and ZTE went global with their affordable technology, which found traction especially in the price-sensitive developing countries. Soon after entering Russia in the late 1990s, Huawei made forays into South-East Asia, West Asia, Africa, and Latin America.[50] Using it as a stepping stone, Huawei made inroads into markets in Europe, beginning as a low-end Original Equipment Manufacturer — well known for its price advantage. In 2004, Huawei bagged its first significant contract in Europe to build a 3G network for the Dutch operator Telfort,[51] and it was shortlisted by Banverket Telenät, the state-owned Swedish Rail Administration telecom, to expand its network across Sweden.[52] These

---

49 n. 24.

50 Guan Chong, "Chinese Telecommunications Giant Huawei: Strategies to Success", Nanyang Technopreneurship Center, Singapore, S/N 88-16-013, pp. 3–4.

51 Huawei, "Milestones", at https://www.huawei.com/en/about-huawei/corporate-information/milestone, accessed June 25, 2019.

52 Lars Anders Karlberg, "Huawei-Ryanair of the mobile system", *NyTeknik*, December 13, 2004, at https://www.nyteknik.se/digitalisering/huawei-mobilsystemens-ryanair-6443049, accessed June 25, 2019.

deals were a major breakthrough for Huawei on two counts: Huawei made inroads into Ericsson's home-turf; and the deals approved Huawei's candidature as a 3G equipment supplier in developed countries or the mainstream markets which dominated the existing standards. Huawei's international expansion also received a major push in 2004, with a USD 10 billion credit line from the state-owned China Development Bank,[53] and another USD 600 million from the Export-Import Bank of China.[54]

British Telecom picked Huawei as one of the suppliers for its network transformation project in 2005. It was labelled as the 21st Century Network.[55] In the same year, Vodafone, the largest international mobile communications operator at that time, also approved Huawei as one of the preferred telecom equipment suppliers, and signed a Global Framework Agreement after a long, all-around quality certification and evaluation process. Vodafone's list of preferred telecom equipment suppliers included global brands like Ericsson, Nokia, Siemens, and Lucent. Vodafone tested Huawei's equipment for power consumption, coverage, and transmission efficiency. Huawei claimed that its highly efficient power amplifier technology reduced the power consumption of Node B, saving 32 per cent in electricity consumption over conventional base stations annually. Huawei also contended that it successfully solved the problem of 3G high-speed coverage within a month, and became the only supplier to pass the high-speed mobility test in the industry, with over 98 per cent call success rate along the

---

53 "Huawei on a roll with 3G", *China Daily*, January 09, 2005, at http://www.chinadaily.com.cn/english/doc/2005-01/09/content_407215.htm, accessed June 25, 2019.

54 "China in Africa", *Institute of Developing Economies – Japan External Trade Organization*, at https://www.ide.go.jp/English/Data/Africa_file/Manualreport/cia_11.html, accessed June 25, 2019; and Vivien Foster et al., *Building Bridges: China's Growing Role as Infrastructure Financier for Sub-Saharan Africa*, Washington DC: The World Bank, 2009, p. 24.

55 Tony Dennis, "Marconi loses out in BT's 21CN network", *The Inquirer*, April 28, 2005, at https://www.theinquirer.net/inquirer/news/1000768/marconi-loses-out-in-bts-21cn-network, accessed June 25, 2019.

high-speed train route.[56] Thereafter, Vodafone continued to induct Huawei's equipment in its networks across Spain, Greece, Romania, Iceland, and Hungary.

Huawei made an entry into Germany when it secured a bid from O2 in 2007 to replace its existing base stations, and to construct 8,000 new GSM and UMTS transceivers,[57] vying for network capacity expansion and performance upgrade. O2's GSM and UMTS networks were previously independent of each other, ailing with high energy-consumption and maintenance costs. Huawei used its dual-mode base stations to converge GSM and UMTS networks, and deployed a single RAN combining 2G and 3G capabilities.[58] Huawei, along with Nokia Siemens Networks, was selected to build UMTS/HSPA networks for Canadian telecom operators Telus and Bell Canada, in 2008.[59] With an aggressive expansion in these markets, Huawei was able to place itself at second position in the global market share of radio access equipment by 2009. The rise of Chinese equipment manufactures is often credited to the aggressive investment in indigenous research and development, which dates back to the late 1980s.

---

56 Huawei, "Quality wins trust – Huawei selected by Vodafone to build the radio access part of its", at http://market.huawei.com/hwgg/itu2006/en/news/news1.html, accessed June 25, 2019.

57 "O2 and Huawei confirm expansion contract", *TeleGeography*, April 23, 2008, at https://www.telegeography.com/products/commsupdate/articles/2008/04/23/o2-and-huawei-confirm-expansion-contract/, accessed June 25, 2019.

58 Huawei, "O2: Fresh air and market share", December 10, 2011, at https://www.huawei.com/en/about-huawei/publications/communicate/45/HW_082710, accessed June 25, 2019.

59 Jamie Sturgeon, "Canadian telecom companies get cosy with Huawei", *Financial Post*, February 14, 2012, at https://business.financialpost.com/technology/canadian-telecom-companies-get-cozy-with-huawei, accessed June 25, 2019; and TELUS Corporation, "Annual Information Form for the year ended December 31, 2008", March 13, 2009, at https://www.sec.gov/Archives/edgar/data/868675/000110465909017585/a09-6978_1ex99d3.htm, accessed June 25, 2019.

China from 2G to 5G: Laggards to Leaders?

At the apex level, the National Medium- and Long-term Program for Science and Technology Development 2006–2020 of the State Council of China enlisted the next generation broadband mobile telecommunication as one of the most important technology development areas.[60] The 13th Five-Year Plan has identified 5G as a "strategic emerging industry",[61] and the ambitious Made in China 2025 plan outlines its goal of becoming one of the leaders in 5G international standards, technology, and industry.[62] From 3G to 5G, China has grown its influence in the standardization process. The Ministry of Industry and Information Technology (MIIT) (created in 2008, replacing MII), along with the National Development and Reform Commission, and the Ministry of Science and Technology jointly founded the IMT-2020 (5G) Promotion Group in 2013.[63] The idea was to push a cooperative mechanism with the EU, the USA, Japan, and Korea. Chinese enterprises, with Huawei as a representative, managed to include the polar code into the 3GPP standard as a part of the technological solution for 5G control channels. This was the first time that a solution

---

60 The State Council of the People's Republic of China, "The National Medium- and Long-Term Program for Science and Technology Development (2006-2020)", at https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/China_2006.pdf, p. 22.

61 "The 13th Five-Year Plan for Economic and Social Development of the People's Republic of China (2016–2020)", translated by the Compilation and Translation Bureau, Central Committee of the Communist Party of China Beijing, China, at http://en.ndrc.gov.cn/newsrelease/201612/P020161207645765233498.pdf, p. 67.

62 The United States Chamber of Commerce, "Made in China 2025: Global Ambitions Built on Local Protections", 2007, at https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf, p. 67.

63 EY, "China is poised to win the 5G race", 2018, at https://www.ey.com/Publication/vwLUAssets/ey-china-is-poised-to-win-the-5g-race-en/$FILE/ey-china-is-poised-to-win-the-5g-race-en.pdf, p. 6.

recommended by a Chinese enterprises had entered the field of the basic communications frame agreement.[64]

As per IPlytics, Chinese companies — including Huawei, ZTE, and CATT, etc. own 36 per cent of all 5G Standard Essential Patents as of February 2019.[65] Chinese companies topped the list for most 5G Standard Essential Patents applications in communication systems by the end of April 2019, accounting for 34 per cent of the world's total.[66] During the 5G standard-setting process, Huawei made 11,423 technical proposals as per data-analytics firm IPlytics and, in 2018 alone, it had filed 5,405 patent applications.[67] This is the largest for a company, and its impact reflects in the Standard Essential Patents. As of February 2019, Huawei owned 1,529 of Standard Essential Patents for 5G — the most for any company.

Beginning with fixed line telephones and early generations of mobile communication systems, foreign companies needed Chinese telecommunication equipment manufacturers to support their global expansion as low-end manufacturers. With 3G or TD-SCDMA, Chinese telecommunication equipment manufacturers became important for them to gain or sustain access to the Chinese telecommunications market, the largest in the world. Likewise, Chinese telecommunication equipment manufacturers needed foreign companies as they lacked competency in chipsets, software, and core networks. Towards 4G, and subsequently 5G, Chinese players were

---

64 Wang Huotao et al., "Who is the Leader of 5G Standard Patents?" *China Intellectual Property*, Issue 85, May 2018, at http://www.chinaipmagazine.com/en/journal-show.asp?id=1557, accessed June 26, 2019.

65 Dan Strumpf, "Where China Dominates in 5G Technology", *The Wall Street Journal*, February 26, 2019, at https://www.wsj.com/articles/where-china-dominates-in-5g-technology-11551236701, accessed June 26, 2019.

66 Yang Yang, "China leads 5G patent race", *China Daily*, May 09, 2019, at http://global.chinadaily.com.cn/a/201905/09/WS5cd3b72aa3104842260babc2.html, accessed June 26, 2019.

67 Charlie Campbell, "Inside the Controversial Company Helping China Control the Future of the Internet", *Time*, May 23, 2019, at https://time.com/5594366/5g-internet-race-huawei/, accessed June 26, 2019.

well integrated with the global technology research and production supply chains, more as partners rather than suppliers. China's rise in the global telecommunications equipment market has neither been inevitable, nor peaceful. Since the very beginning, the Chinese government has drawn severe criticism for protectionist policies and weak Intellectual Property protection regime. Chinese companies have constantly been accused of Intellectual Property theft, lack of innovation competence, and their copy-cat culture. Given the sheer economic potential of 5G technologies, they have come under the direct scrutiny of national governments; to the effect that technological competition is altering the already complex geopolitical equations in unfathomable ways.

Chapter 4

The Race to 5G: Competition, Confrontation, and Geopolitics

Well before 5G could even make its first full-scale commercial deployment,[1] it has become entangled in a global spat over alleged snooping charges which have seen Chinese telecommunications equipment manufacturers being banned from international markets. More than half a dozen countries have either called off Huawei from their 5G trials or are revisiting Huawei's role in their 5G roll-out plans. This is not a new phenomenon for Chinese telecommunications equipment manufacturers, especially Huawei and ZTE who have always been looked at with scepticism. The reasons for this scepticism are many, and range from threats of surveillance to economic considerations and technology superiority to the security of telecommunication infrastructure.

5G has also set global players — such as Cisco, Samsung, Ericsson, Qualcomm, Nokia, and Huawei — scrambling to not just secure their share of the pie, but also prove their leadership as key technology developers as well as influencers of international standards through technical contributions. The competition is not immune to politics and power play either. Governments have come up with aggressive policies to promote 5G, targeting an early deployment. The race to technology dominance is on in different arenas, be it setting the global standards for 5G mobile communication system, rolling out state-of-the-art infrastructure, or building next-generation applications, businesses, and industries. The race to 5G is indeed becoming more and more conspicuous.

---

[1] "ITU's Approach to 5G", International Telecommunication Union, October 15, 2018, at https://news.itu.int/5g-fifth-generation-mobile-technologies/, accessed July 01, 2019.

A Brief History of Scepticism

By the time Huawei began producing routers in 1999, the American major Cisco already had 80 per cent share in the Chinese market. Huawei's price wars had made a dent in Cisco's market share by 2002, setting the stage for the upcoming phase of technology rivalry. In 2003, Cisco filed a lawsuit against Huawei for copyright violations, accusing it of copying Cisco's IOS source code, the operating system for Quidway routers, and even its command line interface and manuals.[2] Later on, Huawei admitted its fault, and the lawsuit was finally settled, with Huawei promising that it would modify the command line interface, user manuals, and those portions of the source code that Cisco had issues with.[3] Huawei's woes did not end there. In 2010, Motorola also filed a lawsuit against Huawei for allegedly stealing trade secrets as well as for espionage through its employees who shared information about Motorola's transceiver and other technology.[4] This lawsuit was also withdrawn in 2011. Another lawsuit against Huawei was filed by T-Mobile in 2014. It accused Huawei of technology theft, including part of a smartphone testing robot, operating software, and design details.[5] The lawsuit ended up in T-Mobile being awarded USD

---

2 Jim Duffy, "Cisco sues Huawei over intellectual property", *Network World*, January 29, 2003, at https://www.networkworld.com/article/2339527/cisco-sues-huawei-over-intellectual-property.html, accessed July 01, 2019; and Mark Chandler, *Cisco Blogs*, October 11, 2012, at https://blogs.cisco.com/news/huawei-and-ciscos-source-code-correcting-the-record, accessed July 01, 2019.

3 John Leyden, "Cisco drops Huawei lawsuit", *The Register*, July 29, 2004, at https://www.theregister.co.uk/2004/07/29/cisco_huawei_case_ends/, accessed July 01, 2019.

4 "Motorola sues Huawei for stealing trade secrets", *China Daily*, July 22, 2010, at http://www.chinadaily.com.cn/bizchina/2010-07/22/content_11035979.htm, accessed July 01, 2019.

5 United States District Court for the Western District of Washington at Seattle, Indictment - Case 2:19-cr-00010-RSM (United States of America vs. Huawei Device Co. Ltd., and Huawei Device USA Inc.), at https://www.justice.gov/opa/press-release/file/1124996/download, p. 2.

4.8 million in damages three years later under the breach of contract allegation, and not on a trade secrets claim.[6]

Legal battles have just been the tip of a deep running technological competition and the brewing trade tensions all along. It is not just the American corporate which has been at loggerheads with Chinese telecommunication equipment manufacturers; even policy makers have been wary of their expansion in the USA, and are often at odds with the political system under which Chinese firms grew and operated. Huawei's multiple bids to acquire American technology companies have been foiled many a time in the past.

In the year 2008, Huawei wanted to acquire a minority stake of 16.5 per cent[7] in 3Com —Huawei's American partner for the manufacture of routers and switches since 2003. The bid was called off after it faced acute political opposition, and was put under the review of the Committee on Foreign Investment in the United States on security grounds.[8] Another bid by Huawei to acquire Motorola's wireless equipment business in 2010 was also blocked by the US government,[9] and Nokia Siemens acquired it subsequently. Prudent policy makers did not want American technology in the hands of Chinese firms which, for a long time, have been accused of close linkages with the government and the military. The American media as well as policy think tanks have further echoed these concerns, and lobbied hard against Chinese firms.

---

6 Rachel Lerman, "Jury awards T-Mobile $4.8M in trade-secrets case against Huawei", *The Seattle Times*, May 18, 2017, at https://www.seattletimes.com/business/technology/july-awards-t-mobile-48m-in-trade-secrets-case-against-huawei/, accessed July 01, 2019.

7 "Document Concerning Proposed Acquisition of 3Com by Affiliates of Bain Capital", Exhibit 99.1, US Securities and Exchange Commission, at https://www.sec.gov/Archives/edgar/data/738076/000095013507006113/b671148kexv99w1.htm, accessed July 01, 2019.

8 "Huawei-3Com deal finally collapses", *Financial Times*, Mar 20, 2008, at https://www.ft.com/content/c2091814-f6b5-11dc-bda1-000077b07658, accessed July 01, 2019.

9 Tian Tao, David De Cremer and Wu Chunbo, *Huawei: Leadership, Culture, and Connectivity*, SAGE Publications, 2018.

The 1999 Rand Corporation publication, *The People's Liberation Army in the Information Age*, noted that the PLA has traditionally been a key player in China's telecom modernization.[10] It has also highlighted that the PLA has commercial interests in this sector, which are advanced through the enterprise system. Besides using the lucrative 800 MHz band for commercial purposes, PLA affiliates like the China Electronic Systems Engineering Company and the Zhengzhou Institute of Information Engineering have played prominent roles in China's telecommunication industry. The 2005 Rand Corporation Monograph — a study commissioned by the US Air Force — was the first to discern PLA's ties with Huawei. The monograph explicitly noted that Ren Zhengfei was a former director of the PLA General Staff Department's Information Engineering Academy, which is responsible for telecom research for the Chinese military.[11] It also underscored the brewing relationship among China's commercial companies, the state R&D infrastructure and the military, where the companies are "the public face for, sprang from, or are significantly engaged in joint research with state research institutes."[12]

The possibilities of state influence in Huawei's operations and products also stem out of Ren Zhengfei's close ties with the government, his previous employment with the PLA, and afterwards, with a State-Owned Enterprise. Ren Zhengfei is not an ordinary serviceman; he was invited to the 12th National Congress of the Communist Party of China[13] in 1982. It must also be emphasized here that, in the early years

---

[10] James Mulvenon and Thomas J. Bickford, "The PLA and the Telecommunications Industry in China", in James C. Mulvenon and Richard H. Yang (eds.), *The People's Liberation Army in the Information Age*, RAND Corporation, 1999 (CF-145-CAPP/AF), at https://www.rand.org/pubs/conf_proceedings/CF145.html, p. 248.

[11] Evan S. Medeiros et al., "A New Direction for China's Defense Industry", RAND Corporation – Project Air Force, 2005, at https://www.rand.org/content/dam/rand/pubs/monographs/2005/RAND_MG334.pdf, p. 218.

[12] Ibid., p. 217.

[13] The congress is a high-profile summit of the Communist Party of China convened every five years, where delegates from the party's membership base ponder and approve new policies, and elect the candidates to senior party positions — in other words, the political leadership of China.

of its existence, Huawei managed to bag a key contract to build the first national telecommunications network for the PLA,[14] possibly owing to Ren Zhengfei's personal contacts in the PLA. Followed by think tanks, who were shaping opinion over the alleged links of Chinese companies with the military and the government, the media opened yet another front against Chinese companies.

By 2011–12, the media began drawing public attention to the technology Huawei and ZTE had sold, or agreed to supply, to the Iranian government, aiding it in censorship and surveillance. The Wall Street Journal ran a detailed story in late 2011, describing it as a violation of US sanctions against Iran under the 2010 Comprehensive Iran Sanctions Accountability and Divestment Act.[15] Besides trade sanctions against Iran, the Act also prohibited the US government from entering into, or renewing contracts, with companies that exported sensitive telecommunications technology to Iran. Reuters followed suit with a special report, in early 2012, alleging that ZTE's networking equipment supplied to the Telecommunication Company of Iran was capable of monitoring landlines, mobiles, and internet communications, which could be used to crackdown dissidents.[16] The equipment was reported to be carrying US technology, or parts of US-origin from Oracle, Dell, Cisco, Microsoft and Symantec. The news stories sparked scrutiny by the Federal Bureau of Investigation,[17] and an enquiry was ordered

---

[14] Guan Chong, "Chinese Telecommunications Giant Huawei: Strategies to Success", Nanyang Technopreneurship Center, Singapore, S/N 88-16-013, p. 2.

[15] Steve Stecklow, Farnaz Fassihi and Loretta Chao, "Chinese Tech Giant Aids Iran", *The Wall Street Journal*, October 27, 2011, at https://www.wsj.com/articles/SB10001424052970204644504576651503577823210, accessed July 05, 2019.

[16] Steve Stecklow, "Special Report: Chinese firm helps Iran spy on citizens", *Reuters*, March 22, 2012, at https://www.reuters.com/article/us-iran-telecoms/special-report-chinese-firm-helps-iran-spy-on-citizens-idUSBRE82L0B820120322, accessed July 05, 2019.

[17] Kim Zetter, "FBI Investigating major Chinese Firm for Selling Spy Gear to Iran", *Wired*, December 07, 2012, at https://www.wired.com/2012/07/fbi-zte/, accessed July 05, 2019.

by the US Department of Justice for the violation of the International Emergency Economic Powers Act;[18] exporting US-origin parts from China to Iran without a license from the Department of Treasury's Office of Foreign Assets Control;[19] and evasion of detection by US authorities.[20] In 2017, ZTE admitted these charges, and paid USD 1 billion as a fine for violating these sanctions.[21]

Simultaneously, cyber security concerns arising out of the Chinese hardware as well as unfair trade practices have also compounded the woes of Chinese companies. The backlash against them was not just restricted to the USA: Huawei and ZTE were put under close scrutiny in Europe and Australia as well. In March 2012, the Attorney-General's department of the Australian Government blocked Huawei from tendering for contracts to supply equipment for the National Broadband Network, citing cyber security reasons. The decision was based on advice from the Australian Security Intelligence Organization.[22] At around the same time, the EU Trade Commissioner intended to investigate Huawei and ZTE for anti-dumping and anti-subsidy, on account of subsidies received from the Chinese government. It was

---

18 "It is a crime for a person to willfully commit, willfully attempt to commit, willfully conspire to commit, or willfully cause a violation of any license, order, regulation, or prohibition issued under", see United States District Court for the Northern District of Texas Dallas Division, United States of America v. ZTE Corporation, No. 3-17 CR – 0120K, at https://www.justice.gov/opa/press-release/file/946281/download, p. 4.

19 Ibid., p. 5.

20 Ibid., p. 21.

21 Donna Borak, "ZTE pays $1 billion fine to US over sanctions violations", *CNN Business*, June 22, 2018, at https://money.cnn.com/2018/06/22/news/companies/zte-us-fine-trade-case/index.html, accessed July 07, 2019, and "China's ZTE to pay US $1bn fine in new deal to save company", *The Guardian*, June 07, 2018, at https://www.theguardian.com/business/2018/jun/07/us-china-zte-deal-fine-sanctions, accessed July 07, 2019.

22 Harrison Polites, "Government bans Huawei from NBN tenders", *The Australian Business Review*, March 26, 2012, at https://www.theaustralian.com.au/business/business-spectator/news-story/government-bans-huawei-from-nbn-tenders/84dcd69855af473f4f0d1f32ecb420cf, accessed July 07, 2019.

argued that such preferential low-interest loans and controversial trade practices are helping Chinese companies to undercut prices at global markets and distorting competition. The move drew support from France and Italy;[23] but, surprisingly, it was opposed by Sweden,[24] and even by Ericsson.[25] It also failed to get support either from Nokia Siemens Networks or Alcatel-Lucent. Moreover, by then, the UK and Netherlands, were already procuring heavily from Chinese vendors. The European Commission had made a decision to open an *ex officio*[26] investigation into the matter; but later on, in 2014, it revised its decision and did not pursue it — owing both to the fragmentation within the Commission and to leave space for dialogue and negotiations.[27]

In October 2012, after an 11-month long investigation, the United States House Permanent Select Committee on Intelligence concluded that Huawei and ZTE cannot be trusted to be free of foreign state influence, and the provision of their equipment or services in critical infrastructure could pose a national security threat to the USA.[28] The

---

[23] Ethan Billy, "EU threatens trade duties against China's Huawei, ZTE", *Reuters*, May 15, 2013, at https://www.reuters.com/article/us-eu-china-huawei/exclusive-eu-threatens-trade-duties-against-chinas-huawei-zte-sources-idUSBRE94D0RX20130515, accessed July 05, 2019.

[24] "Swedish official opposes to EU probe into Huawei, ZTE", *China Daily*, May 09, 2013, at http://www.chinadaily.com.cn/business/2013-05/09/content_16487347.htm, accessed July 07, 2019.

[25] Daniel Bases, "EU cites Chinese telecoms Huawei and ZTE for trade violations", *Reuters*, May 18, 2013, at https://uk.reuters.com/article/us-trade-eu/exclusive-eu-cites-chinese-telecoms-huawei-and-zte-for-trade-violations-idUSBRE94H03J20130518, accessed July 07, 2019.

[26] An *ex officio* trade defence action allows the European Commission to launch a trade defence investigation on its own initiative without an official complaint by the EU industry.

[27] "EU not to pursue the anti-dumping investigation against mobile telecommunications networks from China", a European Commission Press Release, March 27, 2014, at http://europa.eu/rapid/press-release_IP-14-339_en.htm, accessed July 05, 2019.

[28] "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE", U.S. House of Representatives – 112th Congress, October 8, 2012, at https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf, p. v.

committee could not ascertain the corporate structure, history, ownership, operations, financial arrangements, or management of Huawei, even as ZTE failed to provide vital pieces of information related to the control of Chinese state-owned enterprises in its business decisions and operations. Both, however, acknowledged the presence of the Party Committee.[29] Reviewing open source and classified information, the committee recommended that the Committee on Foreign Investment in the United States must block acquisitions, takeovers, or mergers involving Huawei and ZTE; and government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including component parts.[30] Acting on the recommendations of the committee, the US forbade sensitive government agencies from buying products from Huawei and ZTE.[31]

At around the same time, Huawei had emerged as one of the major suppliers for the network transformation project of British Telecom in the UK. Huawei and British Telecom have had commercial relations since 2005. Huawei's presence in the telecommunication infrastructure underwent investigation by the Intelligence and Security Committee of the Parliament of UK in 2012–13. Examining the case under the gamut of risks to UK's Critical National Infrastructure (CNI), the committee concluded that the case highlighted weaknesses in the UK's approach to the deployment of equipment within the CNI,[32] and a

---

29 Ibid., p. 23 and p. 40.

30 Ibid., p. 45.

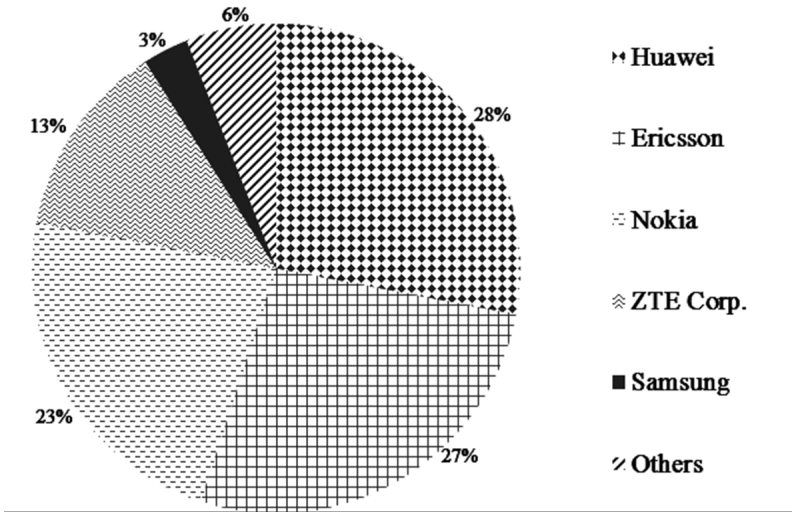
31 The ban also covers video surveillance and telecommunications hardware produced by Hytera Communications, the Hangzhou Hikvision Digital Technology Company, and the Dahua Technology Company. All of them are Chinese firms; see Catherine Shu, "New defense bill bans the U.S. government from using Huawei and ZTE Tech", *TechCrunch*, August 13, 2018, at https://techcrunch.com/2018/08/13/new-defense-bill-bans-the-u-s-government-from-using-huawei-and-zte-tech/, accessed July 09, 2019.

32 "Foreign involvement in the Critical National Infrastructure: The Implications for National Security", the Intelligence and Security Committee of the Parliament of the United Kingdom, June 2013, at https://www.parliament.uk/documents/other-committees/intelligence-security/Critical-National-Infrastructure-Report.pdf, p. 9.

lack of clarity around procedures, responsibility, and powers related to foreign technology in CNI, had risked — and continues to risk — the national security of the UK.[33]

Huawei and ZTE are the poster boys of China's growing technology prowess after its opening up; they are sometimes termed as national champions. Subject to severe criticism and political scrutiny, they have both continued to grow and spread their customer base all across the globe. Huawei, for instance, now supplies products and builds solutions for around 1500 telecom networks in 170 countries, which helps connect one third of the world's population.[34]

Figure 4.1: Mobile Infrastructure Market Share, 2017



Source: IHS Markit

[33] Ibid., p. 20.

[34] "Corporate Introduction", Huawei, at https://www.huawei.com/en/about-huawei/corporate-information, accessed July 07, 2019.

Apparently, the allegations — which began in 2003 — and the subsequent investigations have not derailed Huawei's business prospects, or made a significant dent in Huawei's revenue. By 2017, Huawei held the largest share in global cellular base station market, pegged at 28 per cent[35] (Figure 4.1), with its telecom equipment revenue being as large as Nokia and Ericsson put together.[36] More than technology, cost effectiveness has helped Huawei a great deal; its equipment is said to be 20 to 30 per cent cheaper than the ones Nokia and Ericsson have to offer. Media attention, parliamentary questions, and intelligence led investigations, all have kept Huawei on its toes. In response, Huawei has made many reassurances to its clients and respective governments that its equipment does not pose security threats.

Huawei's Desperate Bid

In order to offset the mounting concerns of the UK government and intelligence agencies, Huawei set up a Cyber Security Evaluation Centre (HCSEC) in 2010. It includes an independent security testing lab made entirely at its own cost, and is headed by an ex-Government Communications Headquarters (GCHQ) Deputy Director, with full executive power over budgets and hiring. When the centre was opened, Huawei described it as "a glasshouse — transparent, readily accessible, and open to regulators and our customers". The Intelligence and Security Committee of the Parliament of UK reviewed HCSEC in its investigation (2012–13), and expressed its discontent regarding whether the centre could provide any protection against the risk of vulnerabilities deliberately created for malicious purposes. It also recommended that GCHQ must have greater oversight of the centre.[37] HCSEC was more of a commercial function for Huawei to prove its trustworthiness to

---

35 Isao Horikoshi, Takashi Kawakami and Kosei Fukao, "Huawei blacklisting bites 5G carriers in the wallet", *Nikkei Asian Review*, February 05, 2019, at https://asia.nikkei.com/Economy/Trade-war/Huawei-blacklisting-bites-5G-carriers-in-the-wallet, accessed July 09, 2019.

36 Dell'Oro Group, "Key Takeaways: The Telecom Equipment Market 3Q 2018", December 7, 2018, at http://www.delloro.com/delloro-group/key-takeaways-telecom-equipment-market-3q-2018, accessed July 09, 2019.

37 n. 32, p. 17.

other foreign countries, and to assure them of the security engineering standards of its telecommunication equipment. However, its effectiveness as an assurance model has always been questioned.

An HCSEC Oversight Board was established in early 2014, comprising members from GCHQ, Huawei, the Cabinet Office, National Cyber Security Centre, and few other departments, to: a) supervise HCSEC's assessment of Huawei's deployed/to be deployed products in the UK; and b) assure independence, competence and, therefore, the overall effectiveness of the HCSEC. The board submits an annual report to the National Security Adviser. The 2018 Annual Report brought technical issues in Huawei's engineering processes to the foreground,[38] acknowledging the risks from a shift in architecture and technology brought about by 5G.[39] The 2019 Annual Report did not find any material progress in the remediation of the issues reported in 2018,[40] and instead, it found serious vulnerabilities in the products provided by Huawei for examination.[41] Over and above this, the report identified poor software engineering and cyber security processes, as well as non-adherence to basic secure coding practices[42] in the underlying software.[43]

---

38 "Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2018", July 2018, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf, pp. 3-4.

39 Ibid., p. 18.

40 "Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2019", March 2019, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf, p. 3.

41 Ibid., p. 17.

42 The specific problems identified with coding practices were: the extensive incorrect use of safe memory manipulation functions; the extensive misuse of signed/unsigned typing and casting to different variable sizes when performing arithmetic operations; the poor management of software component imports; and, the inappropriate suppression of warnings from static analysis tools.

43 n. 40, p. 27.

Keeping an eye on the public opinion and wary of its tarnishing reputation, Huawei often rebuts through white papers and open letters — the allegations on its links with the Chinese government and the PLA. Issuing a clarification over the disapproval of the Committee on Foreign Investment in the United States regarding the acquisition of 3Leaf Systems by Futurewei (Huawei's US subsidiary), Huawei published an open letter addressed to the US Government. The letter denied allegations over security, state support, and Intellectual Property theft, and reassured the US Government that Huawei equipment is not a threat to its national security. It even went on to clarify that it receives tax incentives from the Chinese government, similar to the US companies, as support for some research and development initiatives,[44] and invited investigation by US authorities.[45]

In 2011, Huawei hired John Suffolk as Global Cyber Security & Privacy Officer, who was earlier Chief Information Security Officer in the UK Government.[46] A year later, John Suffolk authored *Cyber Security Perspectives*, a white paper elaborating Huawei's viewpoints regarding cyber security in general, and the steps it is planning to take. The paper called for an open and transparent approach towards cyber security, and invited governments to review Huawei's security capabilities.[47] However, all this has been to little avail, since such tactics have not been able to cut ice with the intelligence community, the security apparatus, and law makers. In the middle of the rising quandaries over Huawei's technology for 5G in early 2019, especially among the members of

---

[44] Ken Hu (Deputy Chairman of Huawei Technologies, Chairman of Huawei USA), "Huawei Open Letter", February 25, 2011, at http://online.wsj.com/public/resources/documents/Huawei20110205.pdf, p. 4.

[45] Ibid., p. 5.

[46] Huawei, "John Suffolk: Senior Vice President, Global Cyber Security & Privacy Officer", at https://www.huawei.eu/profile/john-suffolk, accessed July 12, 2019.

[47] John Suffolk (Global Cyber Security Officer Huawei Technologies), "Cyber Security Perspectives: 21st century technology and security – a difficult marriage", at https://www-file.huawei.com/-/media/corporate/pdf/cyber-security/cyber-security-white-paper-2012-en.pdf, p. 3.

"Five Eyes" alliance, the Science and Technology Committee (of the House of Commons in the Parliament of the UK) asked Huawei to provide reassurances that its products and services pose no threat to the national security of the UK.[48] The committee asked Huawei's plan of action regarding the remediation of the shortcomings underscored in the 2018 report of HCSEC Oversight Board, and the extent to which Huawei could be compelled to assist Chinese intelligence agencies to serve information gathered in the UK through its network. Huawei refuted the concerns through an open letter, and the reply was no different from its previous attempts to douse the fire. Nevertheless, Huawei promised to invest USD 2 billion over the next five years to improve its software engineering capabilities.[49]

Earlier, in June 2018, when the debate arose over the possibilities of excluding Huawei from the upcoming 5G roll-out in Australia, Huawei's open letter to Australian Members of Parliament rejected the security concerns outright.[50] Arguing that Huawei is very well part of the Australian information and communications technology ecosystem, the letter offered the building of an evaluation and testing centre in Australia to ensure an independent verification of its equipment. The European Parliament adopted a resolution in March 2019 in the wake of security risks from Chinese equipment vendors to the EU, originating from a clause in China's National Intelligence Law that imposes

---

48 "Security of the UK's Communications Infrastructure", House of Commons Science and Technology Committee letter to Huawei, January 15, 2019, at https://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/190115-Chair-to-Huawei-re-Communications-Security.pdf.

49 "Security of the UK's Communications Infrastructure", Letter to Chair of the House of Commons Science and Technology Committee, Huawei, January 29, 2019, at https://www-file.huawei.com/-/media/corporate/local-site/uk/pdf/ryan-dings-reply-to-the-uk-science-and-technology-committee.pdf?la=en-gb, accessed July 10, 2019.

50 John Lord AM, John Brumby AO and Lance Hockridge, "Huawei is good & safe for Australia", *Huawei*, at http://huaweihub.com.au/huawei-is-good-safe-for-australia/, accessed July 10, 2019.

obligations on all citizens, enterprises, and other entities to cooperate with the state.[51] It called for a thorough investigation to clarify whether 5G technology in general and technology from foreign vendors in particular, poses security risks to the telecommunication infrastructure of Europe. The insinuations were clearly against Chinese vendors. Europe is the lynchpin of Huawei's global ambitions, both as a mature market for its telecommunication equipment as well as an R&D hub housing high-end skill sets — what Huawei needs the most.

Present State of Affairs: Confrontation, Trade Wars, and Power Play

Of late, 5G has been in the media limelight — not as a technology marvel *per se*, but primarily against the backdrop of brewing controversies as well as the US-China trade war. It began with the US National Defense Authorization Act for the Fiscal Year 2018 (signed in August 2018) which forbade government agencies from procuring equipment or services produced or provided by Huawei and ZTE Corporation.[52] Criminal charges were pressed against Huawei for bank fraud, theft of trade secrets, and breach of American sanctions on Iran, leading to the arrest of Huawei's Chief Financial Officer, Meng Wanzhou, in December 2018. Meng Wanzhou is the daughter of Ren Zhengfei, and she is facing extradition proceedings in Canada where she was arrested at the request of the USA. Later, in January 2019, the US Department of Justice unveiled 23 indictments against Huawei and Meng Wanzhou, which include bank fraud, a theft of trade secrets

---

[51] "Security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them", The European Parliament, March 12, 2019, at http://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_EN.html, accessed July 14, 2019.

[52] "H.R.2810: National Defense Authorization Act for Fiscal Year 2018", U.S. Government Publishing Office, December 12, 2017, at https://www.congress.gov/bill/115th-congress/house-bill/2810/text, accessed July 14, 2019.

conspiracy, and a conspiracy to violate the International Emergency Economic Powers Act (IEEPA).[53]

Another blow to Huawei was the May 2019 Executive Order titled "Securing the Information and Communications Technology and Services Supply Chain". Pursuant to the International Emergency Economic Powers Act and the National Emergencies Act, the Executive Order declares "a national emergency with respect to the threats against information and communications technology and services in the United States".[54] It did not name any country or company per se, but described the threat as "information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries."[55] The Executive Order delegated authority to the Secretary of Commerce (in consultation with heads of other agencies as appropriate) to prohibit transactions involving information and communications technology or services from "adversaries".

This led the Bureau of Industry and Security (BIS) of the US Department of Commerce to designate Huawei Technologies Co. Ltd. and 70 of its affiliates on the "Entity List".[56] US companies

---

53 "Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged with Financial Fraud", The United States Department of Justice, January 28, 2019, at https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial, accessed July 14, 2019.

54 "Statement from the Press Secretary", The White House, May 15, 2019, at https://www.whitehouse.gov/briefings-statements/statement-press-secretary-56/, accessed July 14, 2019.

55 "Executive Order on Securing the Information and Communications Technology and Services Supply Chain", The White House, May 15, 2019, at https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/, accessed July 14, 2019.

56 David Shepardson and Karen Freifeld, "China's Huawei, 70 affiliates placed on U.S. trade blacklist", *Reuters*, May 16, 2019, at https://www.reuters.com/article/us-usa-china-huaweitech/chinas-huawei-70-affiliates-placed-on-us-trade-blacklist-idUSKCN1SL2W4, accessed July 14, 2019.

need a license prior to the export, re-export, or transfer of some, or all, items subject to the Export Administration Regulations for those in the Entity List. Under category 3 (Electronics) and 5 (Telecommunications) of the Commerce Control List, semiconductor integrated circuits, semiconductor technology, equipment, devices or material manufacturing equipment, telecommunications equipment, bridges, gateways, and routers are controlled items. The BIS later issued a 90-day Temporary General License which allows Huawei and its affiliates to engage in transactions in four categories of activity: continued operation of existing networks and equipment; support to existing handsets; cybersecurity research and vulnerability disclosure; and, engagement as necessary for the development of 5G standards by a duly recognized standards body.[57]

As a fall out of the American ban, States both within and outside the "Five Eyes", are reviewing the presence of Huawei and ZTE Corporation in their telecommunications sector, which is not just limited to the telecom equipment segment, but spans R&D, telecom network operations, and business support services. Table 4.1 summarizes the status of Huawei in the 5G roll-out across different countries, both within and out of the "Five Eyes" alliance. The responses are varied, with the USA and Australia leading the charges assertively, while the UK, Germany, and France are being conscientious — possibly to avoid a knee jerk reaction.

---

[57] "Temporary General License" Docket No. 190513445–9459–02, United States Department of Commerce - Bureau of Industry and Security, *Federal Register*, Vol. 84, No. 99, May 22, 2019, at https://www.govinfo.gov/content/pkg/FR-2019-05-22/pdf/2019-10829.pdf, pp. 23468-23471.

Table 4.1: Status of Huawei on 5G.

Country	Status of Huawei on 5G
US	• Recommendations of the House Intelligence Committee in 2012 led to a ban on Huawei and ZTE Corporation from supplying technology and services to sensitive government establishments on account of spying, stealing of intellectual property, and potential ties to the Chinese government and the PLA. • The National Defense Authorization Act (August 2018) forbids all federal agencies from using technology or services supplied by Huawei and ZTE Corporation. • An Executive Order from May 2019 led the US Department of Commerce to designate Huawei and its affiliates from 26 countries to the Entity List.
Australia	• In 2012, Huawei was blocked from bidding for the Australian National Broadband Network on security grounds. • The Australian government blocked Huawei and ZTE from providing 5G equipment in August 2018[58] — the first member amongst the "Five Eyes" to do so.

[58] "Government Provides 5G Security Guidance to Australian Carriers", Ministers for Communications, Cyber Safety and the Arts (Australian Government), August 23, 2018, at https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers, accessed July 14, 2019, also see Arjun Kharpal, "Huawei and ZTE banned from selling 5G equipment to Australia", *CNBC*, August 23, 2018, at https://www.cnbc.com/2018/08/23/huawei-and-zte-banned-from-selling-5g-equipment-to-australia.html, accessed July 14, 2019.

New Zealand	• New Zealand's Government Communications Security Bureau blocked its top telecom firm from using Huawei equipment for its 5G mobile network in November 2018.[59] • In July 2019, Huawei warned the New Zealand government that it may have to pull out of New Zealand if blocked from working on 5G upgrades.[60] • There has been no final decision, and New Zealand still has not completely ruled out Huawei from the 5G network upgrade.[61]
UK	• In December 2018, British Telecom said it would remove Huawei's equipment from its existing 3G/4G mobile operations. • The UK's National Security Council decided in April 2019 to allow Huawei to provide antennas and radio equipment only, and to keep it out of core network deployments.[62] • The UK maintains the stance that any risks posed by Huawei can be mitigated.

[59] Sherisse Pham, "New Zealand prevents mobile carrier from buying Huawei 5G tech over security fears", *CNN Business*, November 28, 2018, at https://edition.cnn.com/2018/11/28/tech/huawei-spark-nz/index.html, accessed July 15, 2019.

[60] "Huawei warns govt it may pull out of New Zealand", *Radio New Zealand*, August 12, 2019, at https://www.rnz.co.nz/news/political/396533/huawei-warns-govt-it-may-pull-out-of-new-zealand, accessed September 15, 2019.

[61] "Huawei never excluded from New Zealand's 5G network construction: NZ PM", *Xinhua*, February 20, 2019, at http://www.xinhuanet.com/english/2019-02/20/c_137836607.htm, accessed July 15, 2019.

[62] "Huawei: UK to make 5G Decision by the Autumn", *BBC*, August 27, 2019, at https://www.bbc.com/news/technology-49481270, accessed September 15, 2019.

Canada	• In January 2019, the Chinese ambassador warned of repercussions if Canada bans Huawei from its 5G networks.[63] • Canada is currently considering whether to block Huawei from providing equipment for 5G networks or not.[64] The decision is likely to be taken after the federal elections, scheduled in October 2019.[65]
Germany	• Germany has been most resistant to US pressure, despite threats of scaling back the sharing of sensitive information. • After a thorough review, Germany's Federal Network Agency, Germany Bundesnetzagentur, took the stance that "no equipment supplier, including Huawei, should, or may, be specifically excluded."[66] • German government has not excluded Huawei from providing networking equipment,[67] but it maintains pressure on Huawei to meet the tightened security criteria.[68]

[63] "Chinese ambassador Lu Shaye warns 'back-stabbing' Canada to stop rallying allies in row over detainees", *South China Morning Post*, January 18, 2019, at https://www.scmp.com/news/china/diplomacy/article/2182612/chinese-ambassador-lu-shaye-warns-back-stabbing-canada-stop, accessed September 15, 2019.

[64] "Huawei likely faces 5G ban in Canada, security experts say – but the trick will be how and when to announce it", *South China Morning Post*, February 07, 2019, at https://www.scmp.com/news/world/united-states-canada/article/2185229/huawei-likely-faces-5g-ban-canada-security-experts, accessed July 15, 2019.

[65] Steven Chase, "Ottawa likely won't make a decision on banning Huawei equipment until after fall election", *The Globe and Mail*, July 30, 2019, at https://www.theglobeandmail.com/politics/article-ottawa-likely-wont-make-a-decision-on-banning-huawei-until-after-fall/, accessed September 15, 2019.

[66] Zak Doffman, "Huawei: U.S. And Europe Divided as Germany Officially Rejects Washington's Demands", *Forbes*, April 14, 2019, at https://www.forbes.com/sites/zakdoffman/2019/04/14/huawei-u-s-and-europe-divided-as-germany-formally-rejects-washingtons-demands/#22dafe5e3bea, accessed September 15, 2019.

[67] Arjun Kharpal, "US allies defy Trump administration's plea to ban Huawei from 5G networks", *CNBC*, March 21, 2019, at https://www.cnbc.com/2019/03/21/future-of-5g-us-allies-defy-washingtons-please-to-ban-huawei.html, accessed July 15, 2019.

[68] "Germany pressures Huawei to meet security requirements", *Deutsche Welle*, June 21, 2019, at https://www.dw.com/en/germany-pressures-huawei-to-meet-security-requirements/a-49294841, accessed September 15, 2019.

France	• In December 2018, Orange confirmed it will not be using Huawei as a 5G equipment supplier in France.[69] • The French Government does not plan to ban Huawei.[70] Instead, it is stepping up controls and safeguards in telecom infrastructure for the next-generation networks in the form of a new amendment to draft business legislation,[71] and keep Huawei away from the user's location data.[72]
Japan	• The Japanese government banned Huawei and ZTE Corporation from official contracts for its upcoming 5G infrastructure, in December 2018. The top three telecom operators followed suit.[73]
India	• Huawei had received an invitation from the government in September 2018 to conduct 5G trials in India, along with Ericsson, Nokia, Samsung, and Cisco.[74] • There is ambiguity over the final decision because, in late February 2019, the Telecom Secretary said that the government is yet to take a decision on whether to allow Chinese equipment makers or not.

[69] "Huawei woes multiply as France risks becoming its next challenge in global 5G fight", *South China Morning Post*, December 14, 2018, at https://www.scmp.com/tech/policy/article/2177975/huawei-woes-multiply-france-risks-becoming-its-next-challenge-global-5g, accessed September 15, 2019.

[70] "France, UK, Germany defy US bid to ban Huawei equipment", *Press TV*, May 18, 2019, at https://www.presstv.com/Detail/2019/05/18/596239/France-UK-Germany-China-Huawei-5G-equipment-US-ban, accessed September 15, 2019.

[71] "France tightens 5G network controls amid Huawei backlash", *Reuters*, January 25, 2019, at https://www.reuters.com/article/us-france-telecom-huawei/france-tightens-5g-network-controls-amid-huawei-backlash-idUSKCN1PJ1T6, accessed July 15, 2019.

[72] Helen Fouquet, "France Aims to Keep Huawei Away From Users' 5G Location Data", *Bloomberg*, June 06, 2019, at https://www.bloomberg.com/news/articles/2019-06-06/france-aims-to-keep-huawei-away-from-users-5g-location-data, accessed September 15, 2019.

[73] "Japan to ban Huawei, ZTE from govt contracts –Yomiuri", *Reuters*, December 07, 2018, at https://www.reuters.com/article/japan-china-huawei/japan-to-ban-huawei-zte-from-govt-contracts-yomiuri-idUSL4N1YB6JJ, accessed July 15, 2019.

[74] "Making India 5G Ready", Report of the 5G High Level Forum, August 23, 2018, at http://dot.gov.in/sites/default/files/5G%20Steering%20Committee%20report%20v%2026.pdf, p. 41.

The global response to Huawei's role in 5G implementation has been mixed. The USA is both persuading and pressurising its allies and members of the "Five Eyes" to get away with Huawei from their 5G deployment plans. Arising out of China's incessant attempts of espionage against both governmental and commercial targets in the USA, the belief that Chinese-made equipment could be used to access or disrupt telecommunication networks is deeply ingrained in the US security establishment. From the podium of the 2019 Munich Security Conference, US Vice President Mike Pence called on the security partners of the USA to reject Huawei and other Chinese telecom companies.[75] Within the "Five Eyes", Australia was quickest to follow the USA. Germany and the UK do not seem to be caving in to American pressure, although the USA has threatened that it will restrict intelligence sharing with allies who do not comply with its call for a ban on the products and services from Chinese telecom majors. China's Ambassador to Canada also warned Ottawa of "repercussions" if Canada drops Huawei from its 5G plans. In the tug of war between China (economic reasons) and US (security reasons), Canada and New Zealand, are playing their cards cautiously — seemingly buying time to take the final call. Nation states are wary of security risks to their telecommunication networks, which are very much a part, and a backbone, of their critical infrastructure.

Nevertheless, on the technical grounds of security, Greg Austin has aptly pointed out that there is no consideration of the numerous vulnerabilities in the Windows operating system which continue to surface and get exploited, causing dire security breaches globally, more than any Huawei products.[76] The EternalBlue exploit in Microsoft's implementation of the Server Message Block protocol was used in

---

[75] Remarks by Vice President Pence at the 2019 Munich Security Conference, February 16, 2019, at https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-2019-munich-security-conference-munich-germany/, accessed July 15, 2019.

[76] Greg Austin, "The campaign against Huawei", *The Strategist – Australian Strategic Policy Institute*, July 06, 2018, at https://www.aspistrategist.org.au/the-campaign-against-huawei/, accessed July 19, 2019.

the WannaCry and NotPetya ransomware attacks, which wreaked havoc across the globe. Cisco has been accused of backdoors on account of critical security vulnerabilities found in its equipment from time to time.[77] The most recent, patched in May 2019, was found in its Nexus 9000 Series Switch which could allow an unauthenticated user to gain root access.[78] Moreover, there has not been any justification or explanation by the USA of its mass surveillance program PRISM run by the National Security Agency (NSA) in collusion with top US technology companies either. China rebuts US accusations with the revelations made by Edward Snowden in 2013, and accuses the USA of large-scale long-term surveillance of foreign governments, enterprises and individuals,[79] and violating the interests and rights of other countries.[80]

The present stand-off between the USA and China — the entire episode of mud-slinging, criminal proceedings, warnings, and prohibition — has unfolded under the shadows of a trade war which began in March 2018 owing to a disagreement over trade deficit, tariffs, foreign direct investment, as well as allegations over espionage and intellectual property theft. It is worthwhile to look at the figures from US-China trade in ICT products and telecommunication equipment over the last decade to assess whether US concerns are grounded in a security conundrum or economic competition.

---

77 Lucian Armasu, "Backdoors Keep Appearing in Cisco's Routers", *Tom's Hardware*, at https://www.tomshardware.com/news/cisco-backdoor-hardcoded-accounts-software,37480.html, accessed September 10, 2019.

78 Michael Heller, "Cisco SSH vulnerability sparks debate over backdoors", *Tech Target*, May 06, 2019, at https://searchsecurity.techtarget.com/news/252462870/Cisco-SSH-vulnerability-sparks-debate-over-backdoors, accessed September 10, 2019.

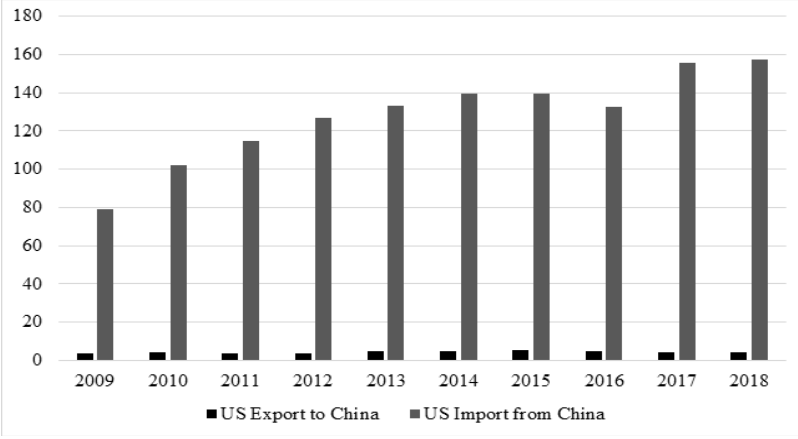
79 Li Xia, "U.S. must stop using "cyber theft" issue to smear China: FM spokesperson", *Xinhua*, October 12, 2018, at http://www.xinhuanet.com/english/2018-10/12/c_137528558.htm, accessed September 10, 2019.

80 Yang Yi, "Commentary: The ulterior motives behind Washington's cyber fear-mongering against China", *Xinhua*, October 15, 2018, at http://www.xinhuanet.com/english/2018-10/15/c_137533091.htm, accessed September 10, 2019.

The US-China Trade War[81]

At around USD 660 billion by 2018, US-China trade has increased by 80 per cent since 2009. However — with a balance of USD 419 billion[82] — China has gained more from this bilateral trade. Of around 22,000 commodities the US trades globally, 500 products from high technology fields, such as biotechnology, Information and Communication Technology (ICT), electronics, aerospace, and advanced materials are classified as Advanced Technology Products (ATP). These products represent the leading edge in technology. Under the ATP category, US imports of ICT products from China have increased by around 50 per cent from USD 79 billion in 2009 to USD 157 billion in 2018. Whereas, the US ICT export to China, from 2009 to 2018, remained miserably between 4.5–2.5 per cent of its total ICT trade with China (Figure 4.2). ICT accounts for majority of the US imports from China under the ATP category.

Figure 4.2: US-China Trade in ICT Products (figures in billion USD)



Source: Created by the author. Data collected from www.census.gov.

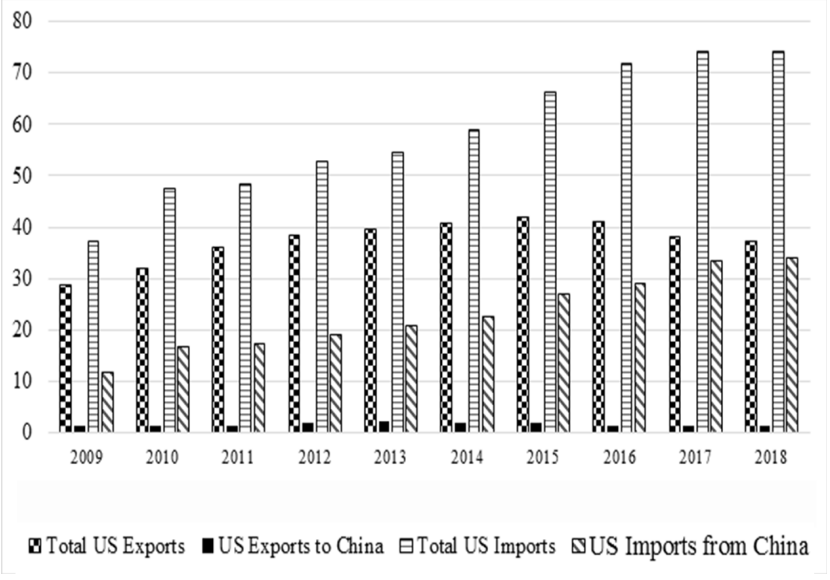
---

[81] This section draws excerpts from a web commentary "US-China Trade War and the High Technology Sector" published by the author, available at https://idsa.in/idsacomments/us-china-trade-war-msharma-220519.

[82] "Trade in Goods with China", United States Census Bureau, at https://www.census.gov/foreign-trade/balance/c5700.html, accessed July 18, 2019.

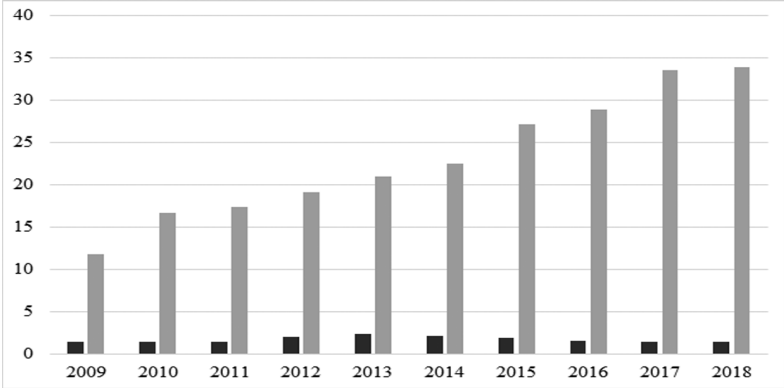
The figures from US-China trade in telecommuincations equipment paint a similar picture. In 2018, US exports of telecommuincations equipment to China were only 4 per cent of total US exports globally. While, for the same year, China had a whopping 45 per cent share in total telecommuincations equipment imported by the USA (Figure 4.3). At USD 34 billion in 2018, imports from China accounted for 96 per cent of their bilateral trade in telecommuincations equipment, where US telecommuincations equipment exports were worth just USD 1.43 billion in 2018. From 2009 to 2018, US telecommuincations equipment imports from China have increased by 188 per cent — from USD 11.7 billion to 33.9 billion (Figure 4.4).

Figure 4.3: US Telecommunications Equipment Trade: World and China (figures in billion USD)



Source: Created by the author. Data collected from www.census.gov.

Figure 4.4: US-China Trade in Telecommunications Equipment (figures in billion USD)



Source: Created by the author. Data collected from www.census.gov.

US telecommuincations equipment exports to China for the same period have grown by just 4.25 percent (Figure 4.4). US-China telecommuincations equipment trade heavily favours China, and an upper hand in the Advanced Technology Products also signifies China's growing technology prowess. Arresting its falling share of exports in ICT and telecommunication equipment trade vis-à-vis China could be one of the driving factors for the US to bring Huawei and ZTE into the fold of trade war.

Chinese telecommunication equipment manufacturers, especially Huawei and ZTE, have had a troubled history ever since they began expanding beyond developing economies. With 3G, China was a new entrant into the elite club of countries setting telecommunication standards. While 5G could be another generation of mobile technology for most of the countries worldwide, it holds great strategic relevance for China. Technology leadership in 5G will mark the arrival of China as a leading technology and economic powerhouse. But this is easier said than done. Leadership in 5G, just like in any other cutting-edge technology domain, demands a vibrating innovation ecosystem, a conducive regulatory environment, ardent support from the government, and active participation in international standard-setting bodies. An early deployment of 5G needs timely allocation of spectrum, an established manufacturing base, and the provisioning of

enabling infrastructure. China is clearly at loggerheads with the USA, and the reasons could be numerous — increasing trade imbalance, as discussed above, is just one of them.

China in 5G: Marching ahead of the Competition?

A 2018 study commissioned by CTIA (the trade association representing the wireless communications industry in the USA) found that 4G leadership created millions of jobs in the USA and it had a profound economic impact.[83] The USA is wary of the fact that losing leadership in 5G means opportunity loss, and the economic benefits will certainly go to the countries who are leading in 5G technology.

A number of reports from US industry, industry associations, enquiry commissions, and the media observe that USA is losing out to the competition from China in 5G. A 2018 report by CTIA concluded that the USA ranked third in 5G readiness — behind China and South Korea.[84] In its 2018 study, Deloitte found that since 2015 China has outspent the USA by USD 24 billion in 5G infrastructure, having built 350,000 new cell sites, while US companies have built 30,000 in the same timeframe.[85] A 2019 Congressional Service Report, titled *5G Telecommunications Technologies: Issues for Congress*, noted that China has made significant strides in positioning itself to dominate in 5G technologies with around USD 400 billion in investments and working closely with Chinese telecom service providers to deploy 5G infrastructure. This, as per the report, is led by a national plan to deploy 5G domestically, capture the revenues from its domestic market, increase the efficiency, productivity, and competitiveness of Chinese technology companies,

---

[83] "How America's 4G Leadership Propelled the U.S. Economy", Recon Analytics, at https://api.ctia.org/wp-content/uploads/2018/04/Recon-Analytics_How-Americas-4G-Leadership-Propelled-US-Economy_2018.pdf, p. 1.

[84] "The Global Race to 5G", CTIA, April 2018, at https://api.ctia.org/wp-content/uploads/2018/04/Race-to-5G-Report.pdf, p. 6.

[85] "5G: The chance to lead for a decade", Deloitte, 2018, at https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-5g-deployment-imperative.pdf, p. 1.

and become a leading supplier of telecommunications equipment to the world.[86] When the Trump administration blocked Singapore based Broadcom's bid to takeover Qualcomm in March 2018, the Committee on Foreign Investment in the United States (CFIU) asserted that the proposed takeover would weaken Qualcomm's position, leaving an opening for China to expand its influence on 5G standard-setting process. CFIU assessed the takeover to have substantial negative national security consequences for the USA.[87]

Companies invest heavily in R&D to invent technology, build intellectual property, and protect it through patents. If an invention is accepted and incorporated into a standard, the underlying patented technology becomes Standard Essential Patents (SEPs). It becomes mandatory for manufacturers to secure license(s) to build equipment based on the standard. Companies have a commercial interest to get the requirements of the standard aligned to their preferred specifications or patented technology, as they can draw benefits from licensing fee or royalty.

This also gives them a first-mover advantage. As discussed in the previous chapter, China played a marginal role in the standard-setting process till 3G; but thereafter, its technology prowess, R&D capacity, and ambitions have grown in leaps and bounds. It also reflects in the increased presence of Chinese companies and their contributions at 3GPP and the ITU. However, its true impact and ability to influence standards is not established. Various estimates from the analysis of patents data, though sometimes conflicting, suggest that China holds the top position for intellectual property in 5G technologies.

The state-run Chinese newspaper *Global Times* reported in March 2019 that China accounted for 10 per cent of the world's 5G-related patents

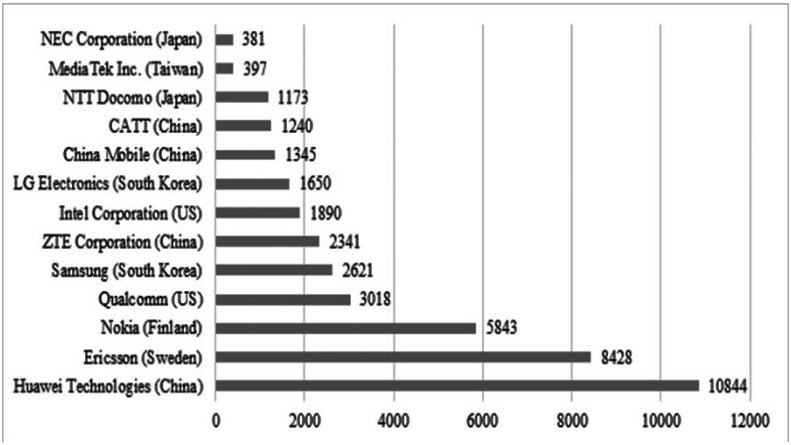
---

[86] "Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress", Congressional Research Service, R45485, January 30, 2019, at https://fas.org/sgp/crs/misc/R45485.pdf, pp. 8-9.

[87] "CFIUS Case 18-036: Broadcom Limited (Singapore)/Qualcomm Incorporated", March 05, 2018, United States Department of the Treasury, at https://www.sec.gov/Archives/edgar/data/804328/000110465918015036/a18-7296_7ex99d1.htm, accessed July 18, 2019.

in 2018.[88] Data from IPlytics — a German company that maintains patent database — shows that Chinese companies account for 34 per cent of worldwide applications for SEPs related to 5G technologies (as of March 2019). This is up by 50 per cent from the 4G era, while the share of Japanese and US entities has fallen down.[89] It ranks Huawei on top for most number of 5G technical contributions, followed by Ericsson, Nokia, Qualcomm, and Samsung (Figure 4.5).[90]

Figure 4.5: Number of 5G Contributions



Source: www.iplytics.com

---

88 Chen Qing, "Huawei tops list of UN patent applications in 2018", *Global Times*, March 19, 2019, at http://www.globaltimes.cn/content/1142621.shtml, accessed July 18, 2019.

89 Akito Tanaka, "China in pole position for 5G era with a third of key patents", *NIKKEI Asian Review*, May 03, 2019, at https://asia.nikkei.com/Spotlight/5G-networks/China-in-pole-position-for-5G-era-with-a-third-of-key-patents, accessed July 18, 2019; and Pan Zhaoyi, "China leads global race in key 5G patents: report", *CGTN*, May 05, 2019, at https://news.cgtn.com/news/3d3d514e7963444e34457a6333566d54/index.html, accessed July 18, 2019.

90 "Who is leading the 5G patent race? A patent landscape analysis on declared SEPs and standards contributions", IPlytics, July 2019, at https://www.iplytics.com/wp-content/uploads/2019/01/Who-Leads-the-5G-Patent-Race_2019.pdf, p. 5.

The accuracy and representation of the data from IPlytics, as well as the methodology have, nevertheless, remained subjective to questioning. Besides, drawing conclusions solely based on the numbers of technical contribution/submissions or the number of employees attending the ITU or 3GPP meetings may be futile. The whole process of standards development is iterative, building upon contributions from other participating entities. The finalised specifications may not necessarily be based on the direct acceptance of a contribution from a single entity; it is rather progressive as entities collaborate for further refinement of the original contribution.[91] Some media reports have even used data from patents filing to insinuate that Chinese companies are dominating 5G standards development, and China may eventually use its strong position to influence standards which may threaten US national security. This may not be a legitimate deduction or correlation. Research suggests that standard-setting bodies have rules to prevent entities from holding-up patents, and the rules often require participants to license essential patents on "Fair, Reasonable and Non-Discriminatory" or "Reasonable and Non-Discriminatory" terms.[92] Moreover, it could not be ascertained whether patents can be leveraged for technological control, as standard-setting bodies limit the total aggregate royalty on a device to a specific quantity to avoid the collection of excessive patent royalties.[93] There are checks and balances in the standard-setting bodies.

History suggests that it was the USA who had urged China to participate in international standards development efforts, both as part of China's

---

[91] Lorenzo Casaccia (Vice President, Technical Standards, Qualcomm Technologies, Inc.), "Why 3GPP Contributions do not indicate 5G Leadership", *Light Reading*, June 30, 2018, at https://www.lightreading.com/mobile/5g/why-3gpp-contributions-do-not-indicate-5g-leadership/a/d-id/744356, accessed July 18, 2019.

[92] Joseph Farrel et al., "Standard Setting, Patents, and Hold-Up", *Antitrust Law Journal*, No. 3, 2007, pp. 624–630.

[93] Eli Greenbaum, "5G, Standard-Setting, and National Security", *Harvard Law School National Security Journal*, July 03, 2018, at https://harvardnsj.org/2018/07/5g-standard-setting-and-national-security/#_ftnref6, accessed July 19, 2019.

obligations under WTO agreements,[94] and to restrict China from developing unilateral or closed standards. For instance, the WTO Agreement on Technical Barriers to Trade aims to ensure that technical regulations are "non-discriminatory", and "do not create unnecessary obstacles to international trade". It also encourages members to use "relevant international standards" as a means to facilitate trade.[95]

On the issue of developing unilateral standards, in 2003, the Chinese government mandated that all wireless devices sold in China must use the WLAN Authentication and Privacy Infrastructure (WAPI) standard[96] — a China-specific encryption standard. The regulation met with a backlash from stakeholders[97] and industry bodies in the wireless market. The US government threatened to hold China liable at the WTO. However, the standard was rejected by the International Organization for Standardization, and the regulation was scrapped.

Based on US-China bilateral trade data in high technology, it could be concluded that the trade heavily favours China. The concerns, therefore, are more economic than security, especially when the Trump administration is striving to correct trade imbalance. From the Obama to the Trump administration, there has been little change in the rhetoric

---

94 "Marrakesh Agreement establishing the World Trade Organization", concluded at Marrakesh on April 15, 1994, No. 31874, at https://treaties.un.org/doc/Publication/UNTS/Volume%201867/volume-1867-A-31874-English.pdf.

95 World Trade Organization, "Technical Barriers to Trade", at https://www.wto.org/english/tratop_e/tbt_e/tbt_e.htm, accessed July 19, 2019.

96 Ping Gao, "WAPI: A Chinese Attempt to Establish Wireless Standards and the International Coalition that Resisted", *Communications of the Association for Information Systems*, Vol. 23, Article 8, 2008, pp. 152-153.

97 "2006 Report to Congress on China's WTO Compliance", The United States Trade Representative, December 11, 2006, at https://ustr.gov/archive/assets/Document_Library/Reports_Publications/2006/asset_upload_file688_10223.pdf, pp. 47–48; and Zeng Peiyan, "Online Extra: Letter from Bush Administration Officials to Beijing Protesting Wi-Fi Encryption Standards", *Bloomberg,* March 15, 2004, at https://www.bloomberg.com/news/articles/2004-03-14/online-extra-letter-from-bush-administration-officials-to-beijing-protesting-wi-fi-encryption-standards, accessed July 19, 2019.

over China's presence in American ICT or telecommunication infrastructure. In fact, with a hard-line approach, hostility towards Chinese companies has increased, on the pretext of security reasons. The probable risk of alienating China any further is that, China may reduce its engagement in the international bodies for standard-setting, and chose to develop alternative standards. It is in the interest of everyone that global technology research, the innovation ecosystem, and supply chains are not disrupted, and that international platforms for technology standardization are not undermined. States have to diligently analyse their respective market conditions, demographics, unique requirements, as well as security situations, and build security assurance frameworks before frantically joining the 5G bandwagon. Cognisant of the vast economic potential of 5G, India is closely watching the developments in this space.

Chapter 5

5G and India: Key Considerations

Housing the second largest mobile phone subscribers globally, India has also joined the race to 5G — notwithstanding the delayed adoption of previous generations of mobile networks. 3G services arrived in India in December 2008, while its first commercial launch was in 2001 in Japan. Likewise, India's first 4G roll-out in 2012 was around 3 years later than the first commercial launch in 2009. India's new National Digital Communications Policy-2018 also envisages a digitally empowered economy and society. This essentially means that the information and communications needs of the citizens and enterprises are met with a ubiquitous, resilient, and affordable digital communications infrastructure and services.[1] With an eye on the economic benefits of 5G, a High Level 5G India 2020 Forum (5G High Level Forum) was constituted in September 2017 to provide vision, mission, and action plan to the "5G India 2020" programme.[2] The Steering Committee of the forum presented its report, *Making India 5G Ready*, in August 2018. The government announced that India is gearing up for its first 5G deployment by 2020, which was followed by a White Paper, *Enabling 5G in India*, from the Telecom Regulatory Authority of India (TRAI) in February 2019. The white paper was

---

1 "National Digital Communications Policy 2018", Department of Telecommunications, Government of India, at http://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf, p. 5.

2 "India Joins Race in 5G Ecosystem, Constitutes High Level Forum on 5G India 2020", Press Information Bureau, Ministry of Communications (Government of India), September 26, 2017, at http://pib.nic.in/newsite/PrintRelease.aspx?relid=171113, accessed July 20, 2019.

intended to initiate a discussion with all the stakeholders to create an enabling environment, and identify regulatory challenges and areas that require investment for a timely rollout of 5G services in India.[3]

The report and the white paper unanimously conclude that the 5G deployment strategy faces conflicting considerations in India, including whether to go for an early or late adoption. The former is more expensive, while the latter will deprive India of the enormous economic benefits. Both of the publications also highlight India's slack participation at standard-setting platforms, and the pressing need to start building capacity in core technology development, product design, and manufacturing, and semiconductor fabrication, etc. for 5G, as a national priority. India is certainly not a key player in technology design, development or the manufacturing of telecommunication equipment.[4] This also means that, like its predecessors, 5G is likely to rest upon either technology imports or equipment manufactured under license in India. Moreover, the technical requirements for 5G call for significant changes in national spectrum allocation and regulatory policies. Other pressing issues pertain to investment, provisioning of enabling infrastructure and, most important, whether to allow Chinese telecommunication equipment manufacturers in 5G deployment, or not. Looking at the priority areas discussed earlier, India has vast grounds to cover before the worldwide commercial launch of 5G in 2020.

Economic Viability

5G is high on capital expenditure, accounting costs for spectrum licensing, infrastructure development, equipment procurement, small cell deployment, and service provisioning. A long-term revenue stream is supposed to offset these initial costs. As a free market economy, the mobile service providers are expected to make these investments, and

---

[3] "TRAI releases White Paper on 'Enabling 5G in India'", Telecom Regulatory Authority of India, Press Release No. 16 /2019, at https://main.trai.gov.in/sites/default/files/PR_No.16of2019.pdf.

[4] Telecom networking equipment includes switches, routers, Base Trans-Receiver Stations, Multiplexers, Antennae, etc.

therefore, their financial health and risk appetite should be one of the key considerations. Surprisingly, despite India being home to over 1 billion mobile subscribers, the Average Revenue per User (ARPU) has nose-dived — from INR 123 in 2015 to a meagre INR 69 by the end of Q2 in 2018.[5] Cut-throat market competition has been driving subscription costs down, cutting down the ARPU. Moreover, this is not the end of woes for the Indian telecommunication industry. With annual revenue under INR 2.5 trillion, the industry has a cumulative debt of INR 7.7 trillion.[6] Close to 30 per cent of the revenues go to the Government as taxes and levies.[7] The industry is under severe financial distress, with falling ARPU, declining revenues, mounting losses, and debt at more than three times the annual revenue. The import duty for equipment such as base stations, optical transport gear, 4G LTE products, gateway controllers, carrier Ethernet switches, etc. has further been increased to 20 per cent.[8] 5G deployments are a costly affair, and debt-ridden mobile service providers have to work their finances out before they can chart out plans for acquiring 5G spectrum or procuring equipment. Over and above these, paltry domestic telecommunication equipment production means that they will have to bear higher costs of equipment.

The case of India is now way different from that of China. Firstly, this is for the simple reason that Chinese telecom service providers are State-Owned Enterprises and their Indian counterparts are primarily

---

5 ARPU Revenue Report Q1 FY 2018-19 – June Quarter, Cellular Operators Association of India, at https://www.coai.com/statistics/arpu-and-revenue-report, accessed July 22, 2019.

6 Cellular Operators Association of India, "Annual Report 2017–18", at https://www.coai.com/sites/default/files/Annual%20Report%20COAI%202017-18.pdf, p. 11.

7 Ibid., p. 23.

8 Kalyan Parbhat, "Telcos may take Rs 6,000 crore knock on import duty hike", *The Economic Times*, October 13, 2018, at //economictimes.indiatimes.com/articleshow/66189887.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppstU, accessed July 20, 2019.

privately owned, with the exception of BSNL and MTNL. State-owned BSNL and MTNL are already under severe financial stress — with a cumulative debt of INR 350 billion. They have not even been allocated 4G spectrum yet.[9] The Chinese government can enforce 5G deployment through its telecom State-Owned Enterprises or even financially support them; but in India the deployment will be market driven. Secondly, China has gained substantial ground in building Intellectual Property in the design and development of telecommunication equipment, and this will lead to reduced costs of equipment acquisition for Chinese mobile service providers. However, beyond capital expenditures, infrastructure has to be in place for the specific requirements of 5G, such as small cell deployment.

Enabling Infrastructure

As discussed in the second chapter, optical fibre connectivity is of utmost importance to support small-cell deployment and increased mobile backhaul traffic. The need for investment in fibre connectivity has been underscored by the TRAI Chairman several times.[10] India will have to make a quantum leap in optical fibre penetration for cost-effective and efficient 5G deployment. India's optical fibre coverage does not fare well. At present, with approximately 1.5 million kilometres of optical fibre cables, only 25 per cent of the cellular network towers have optical fibre backhaul, and the remaining rely on microwave backhaul.[11] By way of comparison, optical fibre kilometre per capita

---

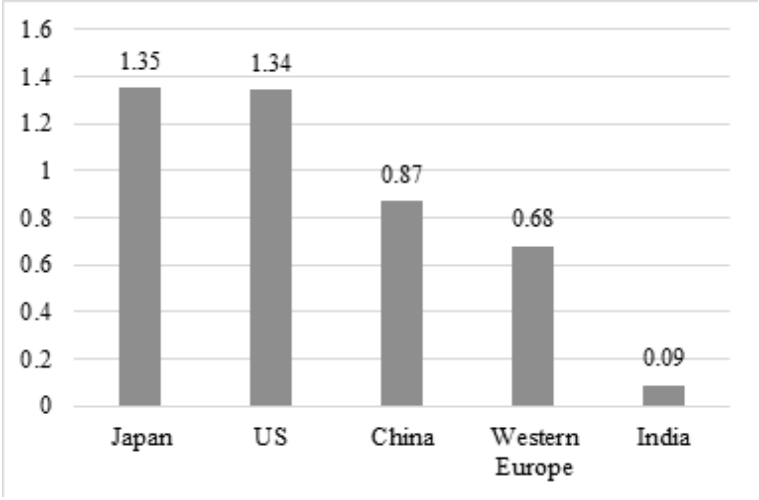
9 Muntazir Abbas, "Trai official: No government reference on 4G airwave for state-run telecom firms", *The Economic Times*, March 24, 2019, at https://economictimes.indiatimes.com/industry/telecom/telecom-news/trai-official-no-government-reference-on-4g-airwave-for-state-run-telecom-firms/articleshow/68531229.cms?from=mdr, accessed July 20, 2019.

10 "India can lead in 5G deployment but investments in fibre infrastructure key: TRAI Chief", ET Bureau, *The Economic Times*, January 17, 2019, at https://economictimes.indiatimes.com/industry/telecom/telecom-news/india-can-lead-in-5g-deployment-but-investments-in-fibre-infrastructure-key-trai-chief/articleshow/67573471.cms?from=mdr, accessed July 20, 2019.

11 n. 1, p. 1.

in India is around one-tenth of China's and one-fifteenth of Japan (Figure 5.1). The Fibre-to-the-Tower programme of the Indian government is supposed to enable at least 60 per cent of telecom towers with optical fibre connectivity, thereby accelerating migration to 4G or 5G services.

Figure 5.1: Fibre Kilometres per Capita



Source: CRU[12]

Moreover, the enabling infrastructure in the case of small cell deployment needs serious rectification in the existing construction and clearance processes. Utility ducts, if built along with roads, highways, and lanes, can drastically reduce the time and costs for laying down new optical fibre cables. Otherwise, laying down new optical fibre cables involves trenching and digging. Utility ducts to carry optical fibre cables should be made mandatory in India in new construction plans. This will pave the way for an efficient infrastructure provisioning process in the long run. Mechanized trenching may further cut down time consumption as compared to the prevailing practice of manual

[12] The figures appeared in ET Telecom, at https://telecom.economictimes.indiatimes.com/tele-talk/fibre-investments-key-to-success-of-5g-in-india/2452, accessed July 22, 2019.

trenching. Small cell deployments will also need to share existing infrastructure, such as buildings, street lighting, and cabinets. On top of this, issues like the Right of Way add to the impediments and delays due to the multiplicity of approvals from different bodies, variable procedures, and non-uniform levies. The Indian Telegraph Right of Way Rules from November 2016 are intended to make this process transparent, uniform and streamlined. The implementation of the rules has, however, been subject to questioning.[13] Along with infrastructure, timely access, availability, and affordability of the spectrum are prerequisite to the time-bound deployment of 5G mobile networks. Harmonizing radio-frequency spectrum for 5G rollout, especially in the 24.5-29.5 GHz band, the L band (1427-1518 MHz), and the C band (3300-3700 MHz), is another uphill task.

Spectrum

The National Digital Communications Policy has recognized spectrum as a key natural resource for public benefit, and called for transparency in its allocation and optimised utilisation. The policy has noted the importance of spectrum availability for Access and Backhaul segments in the timely deployment and growth of 5G mobile networks. The Wireless Planning and Coordination (WPC) wing of the Ministry of Communications is the National Radio Regulatory Authority responsible for Frequency Spectrum Management, including licensing, in India. WPC's Standing Advisory Committee on Radio Frequency Allocation makes recommendations on major frequency allocation

---

[13] "Fibre Future: Government programmes and 5G to drive demand", Tele.net.in, March 23, 2018, at http://www.tele.net.in/index.php?option=com_k2&view=item&id=23318:fibre-future-government-programmes-and-5g-to-drive-demand&Itemid=174, accessed July 22, 2019; and "DoT includes tower cos in right of way rules, industry welcomes move", ET Bureau, *The Economic Times*, May 23, 2018, at https://economictimes.indiatimes.com/industry/telecom/telecom-policy/dot-includes-tower-cos-in-right-of-way-rules-industry-welcomes-move/articleshow/64293364.cms?from=mdr, accessed July 22, 2019; and Navadha Pandey, "Plugging into India's broadband revolution", *Livemint*, June 04, 2019, at https://www.livemint.com/technology/tech-news/plugging-into-india-s-broadband-revolution-1559662971455.html, accessed July 22, 2019.

issues, the formulation of the frequency allocation plan, and making recommendations on the various issues related to ITU.[14] The National Frequency Allocation Plan forms the basis for spectrum utilization in the country, and aims to provide a roadmap for the availability and allocation of spectrum for next generation services.

The 2018 National Frequency Allocation Plan has mentioned that the millimetre bands 24.25, 27.5, 31.8, 37 GHz, and bands below 6 GHz, are under consideration for 5G services in India, though subject to co-existence studies and global deliberations.[15] In its report, the 5G High Level Forum, had recommended significant enhancements in India's spectrum policy in order to realize digital infrastructure as a core utility. For 5G, the report had recommended fresh spectrum of 405 MHz + 137 MHz below 4 GHz range, and 5.25 GHz + 8.3 GHz below 45 GHz range for wireless access, and 14 GHz of unlicensed and 10 GHz of lightly licensed spectrum in the 57 to 86 GHz band[16] for radio backhaul. It had identified three tiers of access spectrum release for 5G, based on availability and readiness:[17]

- Announce Tier: 698-803 MHz, 3300-3600 MHz, 24.25-27.5 GHz, and 27.5 – 29.5 GHz bands to provide certainty to the 5G ecosystem. The recommendation was made to open two mm Bands to be free for two years to support rollout trials as well as indigenous R&D.

---

[14] "About the WPC", Wireless Planning and Coordination Wing, Ministry of Communications (Government of India), at http://wpc.dot.gov.in/content/13_1_AbouttheWPC.aspx, accessed July 20, 2019.

[15] "National Frequency Allocation Plan – 2018", Wireless Planning and Coordination Wing, Ministry of Communications (Government of India), at http://wpc.dot.gov.in/WriteReadData/userfiles/NFAP%202018.pdf, p. 3.

[16] 57–71 GHz as unlicensed spectrum for use in backhaul and access links, and 71-76 GHz and 81-86 GHz under a light touch licensing regime.

[17] "Making India 5G Ready", Report of the 5G High level Forum, August 23, 2018, at http://dot.gov.in/sites/default/files/5G%20Steering%20Committee%20report%20v%2026.pdf, pp. 28-29.

- Identify Tier: 617-698 MHz, 1427-1518 MHz, 29.5 to 31.3 GHz and 37.0 to 43.5 GHz bands for potential 5G use. The recommendation was made to open 37.0 to 43.5 GHz bands to be free for two years to support indigenous R&D.
- Study Tier: 3600-3700 MHz band for the purpose of exploratory studies.

The TRAI white paper noted the availability of 35 MHz spectrum in 700 MHz band (which was put for auction the last time, but was not sold); 100 MHz spectrum from 3300-3400 MHz and 175 MHz in 3400-3600 MHz band (25 MHz spectrum – 3400 MHz to 3425 MHz – is earmarked for Indian Regional Navigation Satellite System); and recognized that 28 GHz is one of the leading and essential bands for early 5G deployments.[18] For spectrum allocation, the TRAI has recommended a block size of 20 MHz to maintain flexibility, and a cap of 100 MHz to avoid the monopolization of the spectrum band.[19]

The identification of spectrum for 5G is more of a technical exercise, and its allocation to 5G services depends entirely on the global developments as it is governed by ITU Radio Regulations. However, further allocation or the assignment of spectrum to specific users or the telecommunication service providers — within the national boundaries — is a policy matter, and is completely under the auspices and control of the government. Spectrum allocation has been a matter of concern in India owing to the lack of transparency earlier in 2G and, of late, to the lack of demand. Expensive spectrum is also attributed to this lack of demand. In a 2018 report, *Spectrum Pricing in Developing Countries*, GMSA Intelligence noted that, since 2010, the Indian government's approach to spectrum management has resulted in inflated spectrum prices and unsold spectrum. Only 41 per cent of the spectrum was sold in the October 2016 auction. Even spectrum from the lucrative

---

[18] "Enabling 5G in India", Telecom Regulatory Authority of India, February 22, 2019, at https://main.trai.gov.in/sites/default/files/White_Paper_22022019.pdf, p. 33.

[19] Ibid., p. 35.

700 MHz band failed to receive bids, reportedly due to high reserve prices.[20] The government could only auction 965 MHz of the total 2,354.44 MHz spectrum across seven bands.[21]

The TRAI white paper explicitly advocated maximizing long-term welfare benefits, and not short term revenue benefits in spectrum pricing and allocations. Surprisingly, for 5G TRAI recommended auctioning 20 MHz blocks in the 3,300-3,600 MHz band at an average reserve price of INR 4.92 billion per megahertz.[22] Mobile service providers in South Korea paid somewhere around INR 1.31 billion per megahertz for the same band[23] — which makes TRAI's recommended price 375 per cent higher than what mobile service providers in South Korea paid. Indian mobile service providers found the prices to be exorbitant, while some of them have even asked for a delayed auction of 5G spectrum.[24] For that matter, the 5G High Level Forum also found the cost of spectrum to be high relative to per capita GDP.[25] The

---

20) "Spectrum pricing in developing countries: Evidence to support better and more affordable mobile services", GSMA Intelligence, July 2018, at https://www.gsma.com/spectrum/wp-content/uploads/2018/12/2018-07-17-5a8f746015d3c1f72e5c8257e4a9829a.pdf, p. 34.

21 "Spotlight on India's 5G rollout roadmap with top panel meeting today", *Livemint*, July 24, 2019, at https://www.livemint.com/industry/telecom/spotlight-on-india-s-5g-rollout-roadmap-with-top-panel-meeting-today-1563950531430.html, accessed July 25, 2019.

22 "Recommendations On Auction of Spectrum in 700 MHz, 800 MHz, 900 MHz, 1800 MHz, 2100 MHz, 2300 MHz, 2500 MHz, 3300-3400 MHz, 3400-3600 MHz Bands", Telecom Regulatory Authority of India, July 08, 2019, at https://main.trai.gov.in/sites/default/files/TRAI_response_08072019_0.pdf, pp. 6-7.

23 n. 21.

24 Navadha Pandey, "Price stalemate expected to prolong India's wait for 5G", *Livemint*, July 09, 2019, at https://www.livemint.com/industry/telecom/price-stalemate-expected-to-prolong-india-s-wait-for-5g-1562694969299.html, accessed July 25, 2019; and "TRAI unlikely to review 5G spectrum prices", *ET Telecom*, June 29, 2019, at https://telecom.economictimes.indiatimes.com/news/trai-unlikely-to-review-5g-spectrum-prices-sources/69994444, accessed July 25, 2019.

25 n. 17, p. 10.

government is targeting the auction of 5G spectrum towards the end of 2019. Since the telecommunications sector is driven by market forces in India, the final prices of spectrum will depend on a number of factors — such as the socio-economic benefits of mobile telephony, expected revenue from spectrum auctioning, business prospects of 5G services, and the ability of the financially-stressed mobile service providers to pay. Besides all these, another capital expenditure for 5G deployment is the equipment which forms the core and radio access network. 5G equipment is an outcome of collaborative, yet highly competitive, multi-national efforts in technology research and development, standard-setting, and manufacturing.

Technology and Standards Development

The 5G High Level Forum had looked into the possibilities to design and manufacture products and solutions in India, and generate intellectual property through innovation and sustained investment in R&D.[26] The report of the Steering Committee had laid out three priority areas for India in 5G:

- Deployment: An early roll out of 5G services to maximise the value proposition of 5G as a technology.
- Technology: To build indigenous industrial and R&D capacity, especially for the design and Intellectual Property.
- Manufacturing: To expand the manufacturing base for 5G technologies, including both semiconductor fabrication and equipment assembly and testing.

At the end of the day, on the ground deployment of 5G networks will be a technical exercise. The companies at the forefront of the technology development lifecycle had begun their R&D efforts probably a decade ago. Moreover, technology development is an incremental and collaborative process, and it is completely globalised now. Huawei, for example, began establishing overseas R&D centres

---

[26] n. 2.

as early as 1999, and it now maintains centres across China, the USA, Europe, and India. Building capacity and competence is a long term endeavour. The report of the 5G High Level Forum had aptly pointed out the dire need of building India's capacity in core technology development (Design and Intellectual Property), as well as the manufacturing of telecommunication equipment and ICT products. It also noted the importance of standards development, product design, and semiconductor manufacturing; and laid strong emphasis on making them a major priority for India.[27]

There have been quite a few initiatives in this direction. The government began setting up Telecom Centres of Excellence (TCOE) way back in 2008 (under Public Private Partnership mode) to promote the development of new technologies, to generate Intellectual Property Rights, and to promote entrepreneurship. The aim was to make India a hub of telecommunication equipment manufacturing, and to position India as a global leader in telecommunication innovation.[28] The Telecom Centres of Excellence have different mandates in the areas of Information Security and Disaster Management of Telecom Infrastructure, Telecom Technology and Management, Telecom Infrastructure, and Next Generation Networks and Technology, to name a few. To spur innovation and research in 5G, the Government had launched "Building an End-to-End 5G Test Bed" program in March 2018. It involves building proof-of-concept 5G prototypes.[29]

At the industry end, companies like HFCL, Coral Telecom, Tejas Networks, and VMC, had ventured into the core telecom space, offering various transmission, access, and core network equipment — such as SDH-based multiplexers Carrier Ethernet solutions, RF & Microwave antennas, Repeaters, Switches, Testing & Measurement equipment, etc.[30]

---

27 n. 17, p. 19.

28 "About TCOE India", Telecom Centres of Excellence, at http://www.tcoe.in/?q=content/about-tcoe-india, accessed July 28, 2019.

29 n. 18, p. 3.

30 "Indian Telecom Equipment Manufacturing: Current State and Potential Future Opportunities", VMC Systems, at http://www.vmcsystems.in/images/gallery_image/1311140938Indian%20Telecom%20Equipment%20Manufacturing.pdf, p. 1.

Unfortunately, it is not a globally competitive industry, and it falls short of even meeting India's technology requirements. As of 2018, imports accounted for a whopping 90 per cent of India's overall telecommunication equipment market.[31] During 2017–18, India's exports of telecom instruments stood at USD 1,201.7 million, against imports worth USD 21,847.92 million.[32] Moreover, none of the companies in India are ready for 5G trials. In a letter written in July 2018, the Department of Telecommunications had invited major Original Equipment Manufacturers (OEMs) to conduct large 5G trials in India. The list included Samsung, Ericsson, Nokia, Cisco, NEC, Qualcomm, and Intel. None of the Indian companies could make it to the list. Given this, a vibrant innovation-led 5G ecosystem appears to be a bridge too far, as 5G technology output and India's contributions to the international standards have been abysmally low. To change this equation, TRAI has recommended measures to bring imports to a 'net zero' by 2022, citing both economic and security reasons for the indigenous production of telecommunication equipment. However, it is widely acknowledged that equipment manufacturing holds a small share in the overall telecom business.

After fabrication, different components are assembled, and thoroughly tested for performance parameters. Beyond this, innovation, R&D, design, and sales and service comprise the major part of the telecom business.[33] Amongst these, the innovation, R&D, and the design segments

---

31 Mehul Pandya, "Indian Telecom Equipment Industry: Will 5G Drive the Future Growth?" *Communications Today*, December 2018, at https://www.communicationstoday.co.in/services/indian-telecom-equipment-industry-will-5g-drive-the-future-growth/, accessed July 28, 2019.

32 "TRAI calls for zero telecom equipment imports by 2022", *The Hindu*, August 03, 2018, at https://www.thehindu.com/business/Industry/trai-calls-for-zero-telecom-equipment-imports-by-2022/article24596076.ece, accessed July 28, 2019.

33 Kalyan Parbhat, "Global telecom gear companies find TRAI's 'Make in India' call unrealistic", *The Economic Times*, August 06, 2018, at //economictimes.indiatimes.com/articleshow/65285703.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst, accessed July 28, 2019.

of the business are more capital and resource intensive. However, they actually build Intellectual Property and generate revenue for the OEMs. Moreover, indigenous manufacturing — on its own — is not a panacea for economic and security concerns either. The entire manufacturing process is now based on global supply chains, as hardware, software, and firmware are sourced from, and assembled and tested in, different countries — depending upon their respective competencies. It may not be economically wise for a single country to manufacture telecom products end-to-end completely on its own.[34] Also, forcing foreign vendors to manufacture in India — as part of the flagship "Make in India" programme — could be counterproductive if it leads to the disruption in the global supply chains of the OEMs. Therefore, indigenous manufacturing should not be the sole aim. Only a globally integrated and globally competitive innovation ecosystem comprising of the private sector, government bodies, and academic and research institutions can bring in true incentives. India may target building core competency in telecom software development, system integration, testing, and operational and business support services. Telecom R&D is another domain where India has substantial availability of human resources and skills-set, since it has a long record of being an R&D hub for global telecom companies like Nokia, Siemens NSN, Ericsson, and Huawei.

Over and above, building an overdue indigenous industrial and R&D capacity has its own set of problems, especially when the global ecosystem for 5G has matured, moved forward and, simultaneously, become extremely competitive. Limited private sector capacity and academic interface leaves industrial and R&D capacity in the lurch. An innovation ecosystem cannot exist unless and until the private sector and academic research moves up the value chain to undertake and execute futuristic R&D projects. The sheer lack of such an ecosystem is partially the reason behind the meagre contribution of Indian companies and academia at international standard-setting bodies, where companies and research institutions from South Korea, the USA, Japan, Sweden, Finland, and China are quite influential, given their rights on patented technologies underpinning 5G mobile standards.

---

[34] Ibid.

India's telecom standards development organization — the Telecommunications Standards Development Society, India (TSDSI) — could get just one use case accepted in the IMT-2020 requirements. Called the Low Mobility Large Cell (LMLC), the use case addresses the requirements of rural settings.[35] It is included in the optional list of 5G standards. The report of the 5G High Level Forum had also made an explicit note of India's low key participation in the standards development process, with implications such as higher equipment costs on account of royalty payments to the Standard Essential Patent holders (around 5 per cent of the unit cost). An application by the author under the Right to Information Act, seeking information regarding number of technical proposals submitted by India at IMT-2020, the status of 5G testbeds, and targets achieved under the IPR and Standardisation Plan (as mentioned in the TCOE report 5G India 2020), is still pending with the Department of Telecommunications at the time of publication.

Building and nourishing an innovation ecosystem for telecommunications and ICT has to be a national priority and executed as a national mission — akin to how China has done it over the last two decades. The Chinese National High-Technology Research and Development Plan and the incessant support of the State Council have gone a long way in elevating scientific and technology research. Moreover, the Chinese telecommunication industry and research have gained immensely from joint ventures with leading foreign companies, and the government's support and preferential treatment in its infancy. The first R&D effort for standards development — the Digital Mobile Communications Technology project — was sponsored by the then State Planning Commission (presently the National Development and Reform Commission). For the development of the 'Chinese indigenous standard' or the TD-SCDMA, the China Academy of Telecommunications Technology received RMB 10 million from the then State Planning Commission in 1995. Research in telecom technology

---

[35] "Telecommunications Standards Development Society, India", Department of Telecommunications, Ministry of Communications, Government of India, at http://dot.gov.in/telecommunications-standards-development-society-india-tsdsi, accessed July 28, 2019.

in China began under the aegis of the government, and the Chinese companies and research institutions continue to receive generous research grants from the government, till today.

For India, if the situation persists, mobile service providers will certainly have to procure equipment from foreign vendors, not just for 5G, but even for the subsequent generations of mobile communication systems. This implies higher procurement costs for Indian mobile service providers and the risk of turning the entire country into a mere market for global telecom technology suppliers. Without massive human and capital investments in this segment, it is just not possible to gain a foothold in product design, Intellectual Property, and standards development aspects of telecom technology.

The domestic industry may not be in a position to compete with the international players in scale or marketing, but a preferential treatment can help them in gaining market share and expanding their presence in the domestic networks. In order to increase their technical competence, technology transfer is also one of the ways as India is in a strong position to demand technology transfer along with the procurement of equipment from leading international players. However, the long-term utility of technology transfer remains questionable, as it has to be leveraged rather than building dependency upon. The role of government is critical in nurturing an innovation culture in the higher education and research institutions. The industrial research and development activities, however, should be driven by the market forces and remain competitive. The government, of course, should extend support, facilitate and set the long-term vision, but refrain from interfering in the direction and administration of R&D processes. For manufacturing, a model based on the lines of Software Technology Parks of India may incentivise the ailing telecommunications and ICT sector. In the meantime, India will also have to deal with the unfolding power play in the technology realm.

INDIA AND THE POWER PLAY

As India prepares for 5G deployment, its quandaries are twofold. The first pertains to the security of imported telecommunication equipment; the second is political in nature: whether to join the anti-China campaign, and block the Chinese telecommunication equipment manufactures

from supplying 5G equipment, especially Huawei and ZTE. There are three camps essentially: one has banned Chinese firms outright from supplying 5G equipment; the second has no reservations over the role of Chinese firms in their telecommunication infrastructure; and, the third camp has allowed Chinese firms to supply non-core equipment after evaluating risks and benefits. There are three key arguments in the support of ban on Chinese firms: the first is their deep linkages with the Chinese government and the PLA; the second is the potential use of their equipment for surveillance at the behest of the Chinese State; and, the third is related to their unfair trade practices (dumping), the infringement of Intellectual Property, and the violation of the US sanctions against Iran. As a matter of fact, Huawei and ZTE are one of the leading players in the global 5G telecommunications technology space. Their rise to the top also marks a shift in technology leadership from the West to the East —which may have perturbed a few. Besides security reasons, banning Huawei and ZTE could possibly serve three purposes: the first is to quell the competition; the second is to protect domestic industry; and, the third is to force the Chinese government to correct trade imbalances.

First and foremost, India will have to tighten a few lose ends at the security front domestically. One is the Indian Telegraph (Amendment) Rules 2017 provision for the mandatory testing and certification[36] of telecom equipment prior to sale or import in India, under the Mandatory Testing and Certification of Telecom Equipment (MTCTE) rules.[37] The deadline for the enforcement of MTCTE procedure was pushed from 01 April 2019 to 01 August 2019,[38] and now to 01 October

---

[36] Performance testing encompasses the safety of the equipment with radio interface, its immunity to electrostatic discharge, operating frequency, output power, and conformance with receiver and transmitter parameters, to name a few; see "Base Station for Cellular Network, Essential Requirements for: Base Station for Cellular Network", Telecommunication Engineering Centre Government of India, TEC4272418.

[37] "About MTCTE (Mandatory Testing & Certification of Telecommunication Equipment)", Telecommunication Engineering Centre, at https://www.mtcte.tec.gov.in/aboutMTCTE, accessed July 30, 2019.

[38] "Notification on Mandatory Certification of Telecom Equipment", Telecommunication Engineering Centre, Ministry of Communications (Government of India), TEC/1-/2018-TC, March 12, 2019, at http://tec.gov.in/pdf/MTCTE/TECNotificationMar19.pdf.

2019. This happens to exclude mobile telephones and equipment.[39] Moreover, there is an acute ambiguity over the status, functioning, capacity, and competence of the Security Lab under the Telecom Engineering Centre (TEC)[40] whose role is critical in the aftermath of allegations against Chinese equipment manufacturers of snooping and backdoors. With such a significant mandate, Security Lab should possess the competence to rip apart a telecom gear, and review the components at both source-code and hardware levels. Any equipment, be it domestically designed and manufactured or imported, has to be mandatorily tested for security aspects. The National Critical Information Infrastructure Protection Centre (NCIIPC) may support the TEC in security evaluation as telecommunications has been identified as a critical infrastructure in India. Once the domestic competence for security assurance is built, India can confidently walk the tight rope on the international political front, especially over the question of Huawei.

It is important to note that Huawei is well integrated in the global technology supply chains. It is a major player with global presence across both developing and developed markets. Huawei's designation to the Entity List of the US Department of Commerce runs the risk of disrupting international markets. For that matter, US companies also gain from Huawei. Out of Huawei's USD 70 billion expenditure on the procurement of components in 2018, close to USD 11 billion went to US firms[41] — Qualcomm, Intel, Microsoft, and Texas

---

[39] Telecom Equipment covered is: 2-Wire Telecom Equipment, Modem, G3 Fax Machine, ISDN CPE, Cordless telephone, and PABX; see Telecommunication Engineering Centre, Ministry of Communications, Government of India, "Mandatory Testing and Certification of Telecommunication Equipment", July 04, 2019, at http://www.tec.gov.in/pdf/MTCTE/notification_mtcte_launch.pdf.

[40] Scope is mentioned as testing the security features of all types of IP and telecom /ICT equipments in access, transport, control and application layers of wireless and wireline domain deployed in the telecom network, e.g. NGN, IMS, LTE etc.; see "Scope of Telecom Security Test Lab", Telecommunication Engineering Centre, at http://www.tec.gov.in/security-lab-sl/, accessed July 30, 2019.

[41] Sijia Jiang and Michael Martina, "Huawei's $105 billion business at stake after U.S. broadside", *Reuters*, May 16, 2019, https://www.reuters.com/article/us-usa-trade-china-huawei-analysis/huaweis-105-billion-business-at-stake-after-us-broadside-idUSKCN1SM123, accessed July 30, 2019.

Instruments, etc. which supply components and technology to Huawei. A deliberate attempt to quell the competition from Huawei is detrimental to the global telecommunications market. Any untoward disruption in global technology research, innovation ecosystem, manufacturing process, or technology supply chains is likely to escalate the costs of 5G deployment for Huawei's clients, or even derail their 5G roll-out plans. Concomitantly, a dogmatic approach can very well inflict damage to the US economy as well as its reputation as a business destination. Since 2012, the USA has kept Huawei and ZTE Corporation at bay; but the two companies are much more integrated in the telecommunications infrastructure in other countries, including India.

Huawei, whose presence in India dates back to 1999 in the form of an R&D facility, was accused of hacking BSNL's mobile base station controller in 2014.[42] Back in 2009, the Intelligence Bureau and the Ministry of Defence had advised that BSNL should not award telecom equipment contracts to Chinese equipment majors Huawei and ZTE in the interest of national security.[43] Despite this, Huawei and ZTE went on to acquire customers in the Indian telecom market, including leading mobile service providers. ZTE and Huawei are amongst the six companies who have submitted proposals for 5G trials in India.[44] India's decision to allow Huawei to bid for India's 5G infrastructure development, and continue its investments in manufacturing and R&D in India should definitely be in line with the national interest, rather than taking sides and constraining options.

---

42 "Chinese telecom equipment maker Huawei allegedly hacked BSNL network: Govt", *The Indian Express*, February 5, 2014, at https://indianexpress.com/article/india/india-others/chinese-telecom-equipment-maker-huawei-allegedly-hacked-bsnl-network-govt/, accessed July 30, 2019.

43 Joji Thomas Philip and Mahima Puri, "Don't award BSNL deal to Huawei: IB, MoD", *The Economic Times*, May 14, 2009, at //economictimes.indiatimes.com/articleshow/4527079.cms?utm_source= contentofinterest&utm_medium= text&utm_campaign=cppst, accessed July 28, 2019.

44 Department Of Telecommunications, Ministry of Communications (Government of India), Lok Sabha Starred Question No.73, June 26, 2019, at http://164.100.47.194/Loksabha/Questions/Qresult15.Aspx?Qref= 628&Lsno=17, accessed July 30, 2019.

For India, whose 90 per cent of telecom equipment is imported, the concerns over foreign surveillance would always loom large, whether it is Huawei (China), Nokia (Finland), Cisco (USA), or Ericsson (Sweden). Given the importance of India for Huawei, an option worth consideration is persuading Huawei to up a security evaluation centre — on the lines of Huawei Cyber Security Evaluation Centre in the UK. A "no back door" pact — what Huawei recently offered India[45] — is a low hanging fruit, but too risky as an option. Backdoors are not one and the only class of threats, cyber security vulnerabilities, pose a major security challenge. So, rather than Huawei or any other vendor certifying its equipment backdoor free, the assurance and the decision to ban or allow any foreign vendor from supplying telecommunication or ICT equipment should be based on a thorough independent security review — which includes backdoors, cyber security vulnerabilities, and geopolitical realities.

---

[45] Surajeet Das Gupta, "Huawei offers to sign 'no back door' pact with India to allay spying fears", *Business Standard*, July 9, 2019, at https://www.business-standard.com/article/companies/huawei-offers-to-sign-no-back-door-pact-with-india-to-allay-spying-fears-119062401409_1.html, accessed July 30, 2019.

Conclusion

5G technologies are going to unleash novel applications, and simultaneously throw open immense business opportunities which will generate jobs and propel economic growth. Technologies underpinning 5G such as Network Function Virtualization, Network Slicing, massive MIMO, Software Defined Networks, and the utilization of millimeter band have made strides over the years, resulting in spectral efficiency, energy efficiency, and better infrastructure utilization. In aggregate, these technologies have brought 5G to the cusp of commercial deployment towards early 2020.

Eyeing the vast economic potential of 5G, and the host of applications it will enable in the near to mid-term, governments are openly supporting 5G efforts despite the challenges in infrastructure provisioning, the harmonization of spectrum, the building of regulatory and policy frameworks, and the raising of capital to meet the costs of 5G deployment. Although building 5G as a technology and setting the standards has been a truly collaborative and an international exercise, the race has already begun for the many firsts as well as for the monetisation of abundant business opportunities. The competition could be termed almost cut-throat, not just among the technology titans, but also among nation states. This is partially because, for the first time in the history of mobile standards, an "outsider" has made inroads into the "elite" club of standard-setting bodies. Apparently, unlike the previous generations of mobile communication standards, more than technology, 5G is about technology leadership. 5G is also one among the basket of emerging technologies — such as Artificial Intelligence and Quantum Information Science — through which China aspires to challenge or alter the existing global technology leadership positions.

Chinese entities have made significant technical contributions to the 5G standard-setting process, and succeeded in getting many standard

essential patents for their inventions. From the very beginning, the telecommunications industry and R&D efforts have received proactive support from the Chinese government in the form of funding, research grants, import substitution policies, cheap credit and preferential treatment. Coming out of an age of low-end manufacturing, Chinese telecommunication equipment manufacturers disrupted global markets with their competitive technology for 3G and 4G mobile networks earlier. Moving another step up the value chain this time, Chinese entities have evolved from technology adopters to technology innovators with 5G. Nevertheless, they have failed to shed the image of copy-cat innovators, and repetitively been accused of intellectual property theft and unfair trade practices. Their close linkages with the government, proximity with the Communist Party of China, and inheritance of the PLA have continuously been sources of scepticism. However, Chinese entities have repeatedly denied these charges and made several desperate bids to gain the confidence of Western governments and their security agencies.

Against the backdrop of these charges, Huawei and ZTE Corporation — the poster boys of China's rise as a technological power — have been subject to numerous reviews, both by intelligence agencies and legislative bodies of other countries. Most recently, the US National Defense Authorization Act for the Fiscal Year 2018 forbade federal agencies from using technology from Huawei and ZTE Corporation. This was followed by a Presidential Executive Order in May 2019, effectively designating Huawei to the Entity List of the US Department of Commerce. The USA is exerting pressure on its allies to ban Huawei from their 5G roll-out plans as well — which is accepted by some, such as Australia, but contested by others, like Germany and the UK. The issue has now acquired a geopolitical flavour, with many a country standing at the cross-roads — to either pay heed to the American warnings or embrace a low-cost upgrade to 5G networks built with Chinese-supplied equipment. The former being a matter of security and the latter being an economic quandary. It is not surprising to see the Chinese government using diplomatic means to offset the American pressure, through both persuasion and coercion. This power play has global ramifications, constraining the options of developed and developing countries alike.

Given the sheer size of the Indian telecommunications market, it may turn out to be one of the battlefields of this unfolding power play. For India, the answer to the question to forbid a foreign vendor from supplying telecommunication or ICT equipment lies in building a strong indigenous competency to test, review, and certify any piece of equipment — both for backdoors as well as for security vulnerabilities. Building strong security assurances is the mainstay of securing the telecommunications sector if India intends to import equipment for the deployment of 5G networks. The final decision over Chinese equipment manufacturers might be political in nature, but it should be grounded in an independent and transparent security assessment of all the equipment vendors, irrespective of their country of origin. India certainly will upgrade to 5G, but there are many obstacles in the road to 5G, which need to be overcome.

First and foremost is the telecom market conditions, where declining ARPU, fierce price wars, and battles for market share have left Indian telecom service providers with weak balance sheets and a pile of debt. Keeping in mind that India is a price sensitive market, affordability of 5G service will depend upon lower spectrum and equipment costs, the efficient usage of the spectrum and network, and infrastructure sharing across operators. Spectrum prices should ideally give due consideration to global prices and per capita GDP or income. The government's role is extremely important — at least for a timely auction of spectrum, and the provisioning of enabling infrastructure and an efficient regulatory framework. Attention has to be drawn to the significant deficiencies in infrastructure, and the wide gaps in domestic innovation and the manufacturing ecosystem for telecommunication systems.

Joining the 5G bandwagon straightaway may not be the best option for India, as some of the astonishing use cases like autonomous cars and connectivity in high-speed trains are yet to find relevance in an Indian scenario. Therefore, mobile broadband (eMBB) and industrial applications (mMTC) are likely to be the key drivers of 5G adoption in India. The domestic telecommunications industry needs to think beyond manufacturing, and start building competency in areas such as R&D, telecom software design and development, system integration, testing, and operational and business support services. As the world's

second largest subscriber base for mobile services, India's telecommunications market should also house a globally competitive innovation ecosystem comprising of the private sector, government bodies, and academic and research institutions. The domestic industry should receive a preferential treatment if it is able to demonstrate technology prowess. Technology transfer is also one of the ways to benefit the domestic industry at this stage, but it is not a long-term solution. The government should continue to build an innovation culture in the higher education and research institutions. However, the industrial research and development activities should be driven by the market forces — without interference, but with the generous support of the government. 5G deployment should not be looked upon as a onetime investment activity. The research for 6G has already begun, which involves harnessing extremely high frequencies of the levels of 300 GHz, or even the terahertz band. 5G should rather be seen as an opportunity to move up the value chain for the forthcoming generations of wireless mobile communication systems.

5G is heralded as a game-changer in mobile telecommunications as it is expected to unleash next-generation technologies such as autonomous vehicles, the Internet of Things and Virtual Reality. It also holds great incentive in terms of economic development, business opportunities, jobs, and a new category of services. This monograph examines the key technologies behind 5G, the requirements of infrastructure and spectrum, and the emerging landscape with the rise of Chinese telecommunication equipment manufactures. It delves into China's rise as a key technology provider in the telecommunications sector, and a prime contributor to standards development. Examining the race among countries to 5G, the monograph looks at technology competition and ambivalent confrontation, with an emphasis on the case of Huawei. It also analyses India's position and underscores the areas which need immediate attention to bridge the gap in both enabling infrastructure and technology development.

Munish Sharma is a Consultant in the Strategic Technologies Centre at the Institute for Defence Studies and Analyses, New Delhi. His research interests include cybersecurity, critical information infrastructure protection, space security and geopolitical aspects of emerging technologies. He is a Chevening Cyber Security Fellow (2018).

idsa
INSTITUTE FOR DEFENCE STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

Institute for Defence Studies and Analyses

No.1, Development Enclave, Rao Tula Ram Marg,
Delhi Cantt., New Delhi - 110 010
Tel.: (91-11) 2671-7983 Fax: (91-11) 2615 4191
E-mail: contactus@idsa.in Website: http://www.idsa.in